

UNIVERSIDAD AUTÓNOMA DE MADRID  
FACULTAD DE CIENCIAS  
DEPARTAMENTO DE MATEMÁTICAS

**Topics in additive  
combinatorics and higher order  
Fourier analysis**

*Tesis presentada por Diego González Sánchez  
y supervisada por Pablo Candela*



# Acknowledgements

First of all, many thanks to my supervisor Pablo Candela, without whom this thesis would have never been possible. Also to my family, especially my parents, my brother, and my girlfriend, who were the (un?)fortunate ones that lived with me for the last four years.

Many thanks to Balázs Szegedy for his hospitality during the period I spent in Budapest at the Alfréd Rényi Institute of Mathematics.

Also, many thanks to Juanjo Rué and Oriol Serra for their reception when I was in Barcelona. And to Moubariz Garaev, Harald Helfgott and Lola Thompson for their kind invitation and the organization of the workshop “Number theory in the Americas”.

Thanks to all colleagues for very useful comments and valuable discussions during these years, especially to my co-authors, who I list in alphabetical order: Daniel di Benedetto, Pierre-Yves Bienvenu, Pablo Candela, Moubariz Garaev, Victor García, David Gryniewicz, Ángel Martínez, Anne de Roton, Igor Shparlinski, Balázs Szegedy, and Carlos Trujillo.

Outside the academic world, I was very lucky to count on a vast cohort of friends that have accompanied me during this period of my life. To all of them, thank you very much. To the marvelous friends that I met at the Pinar Prados primary school, who apart from my family, constitute my earliest memories. To the great ones that I discovered at the Gerardo Diego high school and with whom I grew. To the fantastic friends that I met when I joined the university. To the amazing friends that accompanied me in Cambridge. To my great friends that I met at the ICMAT and the UAM while doing the PhD. To all the salsa people, especially to my salsa team “Los Informales” and to “Salsearte Libre”, with whom I spent uncountable nights of dancing and fun. To my irreplaceable “Mesetarian” friends. To the ones that I met learning contemporary dance and my fellow fencers.

And last but not least, to Ismael and María, my mathematics teachers at school and high school respectively, who spent their free time preparing me for mathematics contests.

Finally, many thanks to La Caixa for the support that they have given me during these years. It has not been only funding, but also easiness, velocity, and willingness to help. Thanks also to the ICMAT, where I found a perfect place to carry out my PhD research.

The project leading to these results has received funding from “la Caixa” Foundation (ID 100010434), under agreement LCF/BQ/SO16/52270027).

# Notation

For the rest of this thesis,  $n, m, i, j, k$ , and  $d$  will always denote integers unless stated otherwise. Similarly,  $p$  will denote always a prime number and  $f, g$ , and  $h$  will denote functions. We will denote by  $\mathbb{Z}_p$  the integers modulo  $p$ , i.e.,  $\mathbb{Z}/p\mathbb{Z}$ . The symbol  $\mathbb{E}$  will denote the average over some set. Typically this set will have a probability measure that can be inferred from the context. For example, given  $f : \mathbb{Z}_p \rightarrow \mathbb{C}$ , we write  $\mathbb{E}f$ ,  $\mathbb{E}_x f$ ,  $\mathbb{E}_{x \in \mathbb{Z}_p} f$ , or  $\mathbb{E}_{x \in \mathbb{Z}_p} f(x)$  for the sum:

$$\frac{1}{p} \sum_{x=0}^{p-1} f(x).$$

Moreover, all functions  $f : X \rightarrow \mathbb{C}$  are assumed to be measurable and integrable; and  $X$  will be a probability space. We will use  $\mathcal{C}$  to denote the conjugate of  $f$ ,  $\mathcal{C}f(x) := \overline{f(x)}$ .

The set  $\{0, 1\}^n$  will be denoted by  $\llbracket n \rrbracket$  for any  $n \geq 1$ , and by definition,  $\llbracket 0 \rrbracket := \{0\}$ . When we want to stress that a variable takes values in some set  $X^n$  ( $n \geq 1$ ), we will denote it by  $\underline{x}$ . Its values will be  $x(i)$  for  $i = 1, \dots, n$ . If we write  $\underline{w} \cdot \underline{x}$ , we mean  $w(1)x(1) + \dots + w(n)x(n)$  (from the context, we will be able to multiply and sum those elements). A typical example will be  $\underline{w} \in \llbracket n \rrbracket$  and  $\underline{x} \in G^n$  where  $G$  is an abelian group. For an element  $v \in \llbracket n \rrbracket$ ,  $|v|$  will stand for  $\sum_{i=1}^n v(i)$ . The element  $\underline{v} \in \llbracket n \rrbracket$  consisting of all coordinates equal to 0 (resp. 1) will be denoted by  $0^n$  (resp.  $1^n$ ).

The symbols  $X$  and  $Y$  will always denote nilspaces, unless stated otherwise, and  $\Theta(X)$  will be the translation group of  $X$ .

We will make use of the well-known asymptotic notation  $f \ll g$  or  $f = O(g)$ . Typically,  $f, g$  will be functions of  $x \in \mathbb{N}$ , and then this notation means that for some constant  $C \geq 0$  we have  $f(x) \leq Cg(x)$  for all  $x$  sufficiently large.

If  $A$  is a finite set, we denote by  $|A|$  its cardinality.

# Contents

<b>1</b>	<b>Introducción</b>	<b>9</b>
1.1	Una desigualdad de Plünnecke-Ruzsa en grupos abelianos compactos . . . . .	10
1.2	Sobre conjuntos con constante aditiva pequeña y conjuntos $m$ -libres en $\mathbb{Z}_p$ . . . . .	11
1.3	Nilespacios y acoplamientos cúbicos . . . . .	13
1.4	Sobre sistemas de nilespacios y sus morfismos . . . . .	16
1.5	Una nota sobre el teorema bilineal de Bogolyubov . . . . .	17
1.6	Apéndice A: Estructuras y resultados auxiliares para nilespacios . . . . .	18
1.7	Resumen y conclusiones . . . . .	19
<b>2</b>	<b>Introduction</b>	<b>20</b>
2.1	A Plünnecke-Ruzsa inequality in compact abelian groups . . . . .	21
2.2	On sets with small sumset and $m$ -sum-free sets in $\mathbb{Z}_p$ . . . . .	22
2.3	Nilspaces and cubic couplings . . . . .	24
2.4	On nilspace systems and their morphisms . . . . .	27
2.5	A note on the bilinear Bogolyubov theorem . . . . .	27
2.6	Appendix A: Auxiliary structures and results for nilspaces . . . . .	29
2.7	Summary and conclusions . . . . .	29
<b>3</b>	<b>On the Plünnecke-Ruzsa inequality</b>	<b>30</b>

<i>CONTENTS</i>	6
3.1 Introduction . . . . .	30
3.2 The case of closed sets in compact abelian Lie groups . . . . .	33
3.3 Extension to closed subsets of compact abelian groups . . . . .	37
3.4 Extension to $K$ -analytic sets . . . . .	41
3.5 On further extensions of the main result . . . . .	43
3.5.1 Generalizing Theorem 3.3 using extensions of the Haar measure . . . . .	44
3.5.2 On extending Theorem 3.3 to larger families of Haar measurable sets . . . . .	46
<b>4 On sets with small sumset</b>	<b>50</b>
4.1 Introduction . . . . .	50
4.2 New bounds toward the $3k - 4$ conjecture in $\mathbb{Z}_p$ . . . . .	54
4.3 Bounds for $m$ -sum-free sets in $\mathbb{Z}_p$ . . . . .	64
4.3.1 Lower bounds for $d_m(\mathbb{Z}_p)$ . . . . .	64
4.3.2 Upper bound for $d_m(\mathbb{Z}_p)$ . . . . .	66
<b>5 Nilspaces and cubic couplings</b>	<b>71</b>
5.1 Introduction . . . . .	71
5.2 Algebraic theory of nilspaces . . . . .	75
5.2.1 Examples of nilspaces . . . . .	78
5.2.2 Characteristic factors and abelian bundles, morphisms and fibrations. . . . .	81
5.2.3 Group of translations . . . . .	85
5.2.4 Extensions and cocycles . . . . .	85
5.2.5 Construction of nilspaces, translation groups and non-coset nilspaces . . . . .	87
5.3 Topological and measure-theoretic aspects of nilspaces . . . . .	91
5.3.1 Haar measure on compact abelian bundles . . . . .	92

5.3.2	Topology of abelian bundles associated with a continuous system of measures . . . . .	95
5.3.3	Finite-rank nilspaces, inverse limit representation and rigidity of morphisms . . . . .	96
5.3.4	Toral nilspaces . . . . .	100
5.4	Cubic couplings . . . . .	102
5.4.1	Results in measure theory . . . . .	102
5.4.2	Couplings . . . . .	105
5.4.3	Idempotent couplings . . . . .	107
5.4.4	Cubic couplings . . . . .	109
5.4.5	Applications of the cubic coupling theory . . . . .	114
<b>6</b>	<b>On nilspace systems</b>	<b>116</b>
6.1	Introduction . . . . .	116
6.2	Some motivating examples . . . . .	121
6.3	Finite-rank valued morphisms factor through fibrations . . . . .	122
6.4	Finite-rank-valued fibrations factor through translation-consistent fibrations . . . . .	126
6.5	An inverse limit theorem for nilspace systems . . . . .	132
<b>7</b>	<b>On the bilinear Bogolyubov theorem</b>	<b>135</b>
7.1	Introduction . . . . .	135
7.2	Proof of proposition 7.4 . . . . .	138
7.3	Proof of proposition 7.5 . . . . .	140
7.4	Proof of proposition 7.3 . . . . .	144
<b>A</b>	<b>Auxiliary structures and results</b>	<b>147</b>
A.1	Algebraic aspects . . . . .	147
A.1.1	Complementary definitions and examples . . . . .	148
A.1.2	Concatenation and tricubes. . . . .	150

A.1.3	More on abelian bundles . . . . .	159
A.2	Topological and measure-theoretic aspects . . . . .	160
A.2.1	Probability spaces of restricted morphisms . . . . .	160

# Chapter 1

## Introducción

En este capítulo vamos a introducir y motivar los resultados que conforman esta tesis doctoral. Además de los dos primeros capítulos, que son introductorios, el resto de la tesis se puede dividir en dos partes: los capítulos tercero y cuarto son resultados en Combinatoria Aditiva *clásica*, mientras que los tres últimos tratan problemas relacionados con el área de Análisis de Fourier de Orden Superior. Los capítulos son autocontenidos, todos cuentan con una introducción propia además de la que suponen los dos primeros capítulos de la tesis, sin perjuicio de que se intente reducir la redundancia entre ellos. Se ha intentado disminuir el número de citas en los dos primeros capítulos para dar una mayor fluidez a su lectura, posponiendo estas a las introducciones de cada capítulo.

Todos los capítulos de esta tesis salvo las introducciones y el capítulo quinto son trabajos que han sido publicados o están siendo revisados para publicación en diferentes revistas ([11, 12, 13, 6]). El capítulo quinto es singular porque contiene una síntesis personal de la teoría de nilespacios y acoplamientos cúbicos. Las razones que justifican un capítulo de esta naturaleza en una tesis doctoral son dos: entender esas teorías fue imprescindible para elaborar los trabajos que han dado lugar a los dos últimos capítulos; y ese capítulo aporta nuevas pruebas, ejemplos y resultados pequeños a la propia teoría. En ese capítulo se pondrá una especial atención a las citas y a que quede claro qué resultados son del autor y cuáles no.

## 1.1 Una desigualdad de Plünnecke-Ruzsa en grupos abelianos compactos

Dado un conjunto  $A \subset Z$  no vacío donde  $Z$  es un grupo abeliano, nos interesa conocer cómo crece el conjunto suma  $nA - mA$ , para  $n, m$  enteros no negativos, definido como

$$nA - mA := \{a_1 + \dots + a_n - a'_1 - \dots - a'_m : a_1, \dots, a_n, a'_1, \dots, a'_m \in A\},$$

en relación con el tamaño de  $A$ . Esta cuestión deja intencionadamente abierta la pregunta de cómo medir el tamaño de los conjuntos  $A$  y  $nA - mA$ . En un principio, supongamos que  $A$  es finito y que la medida es la de contar.

Ahora imaginemos que sabemos de alguna manera que  $|2A| \leq \alpha|A|$  para algún  $\alpha$ . Es razonable pensar que el número de parejas distintas  $a_1, a'_1 \in A$ ,  $a_2, a'_2 \in A$  tal que  $a_1 + a'_1 = a_2 + a'_2$  está relacionado con ese  $\alpha$  (cuanto más pequeño sea  $\alpha$ , más repeticiones habrá). Por tanto sería *de esperar* que cuando miráramos el tamaño de  $3A$ , este también crezca *acorde* con  $\alpha$ , ya que esas mismas repeticiones deberían aparecer de alguna manera. La desigualdad de Plünnecke-Ruzsa es un resultado que nos cuantifica este fenómeno:

**Teorema 1.1** (Plünnecke y Ruzsa). *Sean  $A, B \subset Z$  subconjuntos finitos no vacíos de un grupo abeliano  $Z$ . Supongamos que existe una constante  $\alpha \geq 0$  tal que  $|A + B| \leq \alpha|A|$ . Entonces, para enteros  $n, m \geq 0$  cualesquiera,*

$$|nB - mB| \leq \alpha^{n+m}|A|.$$

Este resultado es posiblemente uno de los más usados en Combinatoria Aditiva. Recientemente, cada vez es más habitual necesitar resultados como esta desigualdad en ámbitos un poco más generales, no sólo para conjuntos finitos. Una de las generalizaciones más naturales consiste en considerar conjuntos *razonables* dentro de grupos abelianos compactos y medirlos con la medida de Haar. En el primer capítulo de esta tesis demostramos esta generalización:

**Teorema 1.2** (Candela, González-Sánchez y de Roton). *Sean  $A, B \subset Z$  subconjuntos  $K$ -analíticos de un grupo abeliano compacto. Sea  $\mu$  la medida*

de Haar de  $Z$  y sea  $\alpha > 0$  tal que  $0 < \mu(A + B) \leq \alpha\mu(A)$ . Entonces, para enteros  $m, n \geq 0$  cualesquiera, tenemos

$$\mu(nB - mB) \leq \alpha^{n+m}\mu(A).$$

En la introducción del Capítulo 3 definiremos con precisión los subconjuntos  $K$ -analíticos. Esta clase de conjuntos son lo suficientemente generales para incluir a los subconjuntos borelianos en el caso de grupos abelianos, compactos y polacos.

## 1.2 Sobre conjuntos con constante aditiva pequeña y conjuntos $m$ -libres en $\mathbb{Z}_p$

El segundo capítulo parte de lo que podríamos considerar un caso particular del capítulo anterior. La pregunta que nos ocupa viene de suponer que  $|2A| \leq \alpha|A|$  donde  $\alpha$  es una constante *muy pequeña*. Entonces, ¿podríamos decir algo más de  $A$ ?

Primero, vamos a dar una idea un poco más precisa de qué significa que  $\alpha$  sea *muy pequeña*. Vamos a suponer para empezar que el grupo ambiente son los enteros, y que tenemos un subconjunto  $A \subset \mathbb{Z}$  finito. Un resultado conocido en el área dice que  $|2A| \geq 2|A| - 1$  y que la igualdad se alcanza si y sólo si  $A$  es una progresión aritmética. Por tanto ya sabemos que de ese mínimo no vamos a poder bajar. Entonces la pregunta es: ¿Qué pasa si suponemos ahora que  $|2A|$  es ligeramente superior a  $2|A| - 1$ ? La primera respuesta *intuitiva* sería decir: *A debería ser muy parecido a una progresión aritmética*. Y como ya pasó en el capítulo anterior, existe un resultado que cuantifica esta intuición, el teorema  $3k - 4$  de Freiman:

**Teorema 1.3** (Freiman). *Sea  $A \subset \mathbb{Z}$  un subconjunto finito no vacío tal que  $|2A| = 2|A| + r \leq 3|A| - 4$ . Entonces existen progresiones aritméticas  $P_A, P_{2A} \subset \mathbb{Z}$  tales que  $A \subset P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subset 2A$  y  $|P_{2A}| \geq 2|A| - 1$ .*

Nótese que esto en particular implica una versión más fuerte de la desigualdad de Plünnecke-Ruzsa en el caso de  $\mathbb{Z}$  cuando el  $\alpha$  es *muy pequeño*. Esta es sólo una de las múltiples aplicaciones de este resultado. El problema está en que de momento este resultado sólo es válido para los enteros, pero

lo que nos gustaría es poder aplicarlo a otros grupos. Sin embargo, esta vez una generalización directa a otros grupos ya no funciona, ya que la desigualdad  $|2A| \geq 2|A| - 1$  no es cierta en general para cualquier subconjunto  $A$  de cualquier grupo abeliano (por ejemplo, si  $A = \mathbb{Z}_p$ , entonces  $2A = \mathbb{Z}_p$ , y la desigualdad es falsa). El primer paso sería ver cuál es el equivalente a ese mínimo en otros grupos.

En el caso particular de  $\mathbb{Z}_p$ , para  $p$  un primo, es conocido como la desigualdad de Cauchy-Davenport, y dice que dado  $A \subset \mathbb{Z}_p$ , se tiene que  $|2A| \geq \min(p, 2|A| - 1)$ . A partir de aquí se puede formular una conjetura de cómo sería el teorema  $3k - 4$  en  $\mathbb{Z}_p$ :

**Conjetura 1.4.** *Sea  $A \subset \mathbb{Z}_p$  un subconjunto finito no vacío tal que  $|2A| = 2|A| + r \leq \min(3|A| - 4, p - r - 3)$ . Entonces existen progresiones aritméticas  $P_A, P_{2A} \subset \mathbb{Z}_p$  tales que  $A \subset P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subset 2A$  y  $|P_{2A}| \geq 2|A| - 1$ .*

Han habido varios resultados parciales que apuntan a que la conjetura es cierta. Uno de los resultados más fuertes de este tipo fue probado por Serra y Zémor en 2009.

En el capítulo cuarto probamos el siguiente resultado parcial que apunta a la veracidad de la Conjetura 1.4, mejorando el resultado de Serra y Zémor para el rango  $|A| \leq \frac{0,75p+3}{2,136861}$ , dando así las mejores cotas actualmente conocidas en esta dirección.

**Teorema 1.5** (Candela, González-Sánchez y Grynkiewicz). *Sea  $A \subset \mathbb{Z}_p$  un subconjunto no vacío tal que*

$$|2A| \leq (2,136861)|A| - 3 \quad \text{y} \quad |2A| \leq \frac{3}{4}p.$$

*Entonces existen progresiones aritméticas  $P_A, P_{2A} \subset \mathbb{Z}_p$  tales que  $A \subset P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subset 2A$  y  $|P_{2A}| \geq 2|A| - 1$ .*

Además, usamos este resultado para obtener nuevas cotas para el problema de los conjuntos  $m$ -libres. Diremos que un conjunto  $A \subset \mathbb{Z}_p$  es  $m$ -libre, para un entero  $m \geq 3$  fijo, si la ecuación  $x + y = mz$  no tiene solución para  $x, y, z \in A$ . Haciendo uso de nuestros resultados del Capítulo 4, si definimos

$$d_m(\mathbb{Z}_p) = \max \left\{ \frac{|A|}{p} : A \subseteq \mathbb{Z}_p \text{ es } m\text{-libre} \right\},$$

tenemos que

$$\lim_{p \rightarrow \infty} d_m(\mathbb{Z}_p) \leq \frac{1}{3,1955}.$$

Esta es a día de hoy la mejor cota conocida para esta cantidad. Usando el resultado clásico de Cauchy-Davenport es sencillo ver la cota trivial de  $1/3$ . La única cota no trivial que había hasta el momento de esta cantidad era  $1/3,0001$ , dada por Candela y de Roton usando el resultado de Serra y Zémor.

### 1.3 Nilespaceos y acoplamiento cúbico

Hay al menos dos importantes motivaciones que conducen al concepto de nilspace (y acoplamiento cúbico): como objeto que permite extender la noción de nilsecuencia en Combinatoria Aditiva, y como objeto que describe los factores característicos de ciertos sistemas ergódicos. De hecho, este concepto trata de unificar varios resultados en las áreas anteriormente mencionadas que, al menos desde el trabajo de Furstenberg sobre el teorema de Szemerédi en 1977, se sabe que están relacionadas. El teorema de Szemerédi es uno de los resultados más importantes en combinatoria:

**Teorema 1.6** (Szemerédi). *Sea  $k \geq 3$  un entero y  $A \subset \mathbb{N}$  un subconjunto cualquiera. Si  $A$  no contiene progresiones aritméticas de longitud  $k$  no triviales<sup>1</sup>, entonces  $|A \cap [1, N]| = o_k(N)$ .*

Desde la perspectiva de Combinatoria Aditiva, imaginemos que queremos estudiar los subconjuntos de los naturales que no contienen progresiones aritméticas no triviales (en lo sucesivo, omitiremos ese último adjetivo). En 1953 Roth dio una demostración del teorema de Szemerédi para el caso de progresiones de longitud 3. Uno de los puntos clave de esta es, dado un conjunto  $A \subset \mathbb{Z}_p$  que no tiene progresiones de tamaño 3, estudiar el funcional

---

<sup>1</sup>Dado un entero  $k \geq 3$ , un grupo abeliano  $G$  y elementos  $x, r \in G$ , diremos que  $x, x + r, \dots, x + (k - 1)r$  forman una progresión aritmética de longitud  $k$ . Si  $r \neq 0$  diremos que la progresión es *no trivial*.

$$\Lambda_3(1_A, 1_A, 1_A) := \mathbb{E}_{x,r \in \mathbb{Z}_p} 1_A(x) 1_A(x+r) 1_A(x+2r), \quad (1.1)$$

que cuenta precisamente el número de progresiones de longitud 3 en  $A$ . El truco está ahora en dividir  $1_A = f_U + f_{U^\perp}$ , donde  $f_U$  será la parte que llamaremos pseudoaleatoria y  $f_{U^\perp}$  la parte que llamaremos estructurada. Para cierta elección de  $f_U$  y  $f_{U^\perp}$ , se prueba que existe un carácter de Fourier  $\chi$  tal que  $\mathbb{E}(f_{U^\perp} \chi)$  es grande (mayor a una cantidad que depende sólo de la densidad de  $A$ ). Y por último, mediante un argumento conocido como *aumento de densidad*, se demuestra que si  $A \subset [1, N]$  no tiene progresiones de tamaño 3, entonces  $|A| \ll N/\log \log N$ .

En el caso de progresiones de longitud  $k \geq 4$ , podemos proceder de manera análoga estudiando el funcional:

$$\Lambda_k(f_1, \dots, f_k) = \mathbb{E}_{x,r \in \mathbb{Z}_p} f_1(x) f_2(x+r) \cdots f_k(x+(k-1)r).$$

El problema es que a partir de aquí ya no vamos a ser capaces de hacer lo mismo que antes (en general) y encontrar un carácter de Fourier tal que  $\mathbb{E}(f_{U^\perp} \chi)$  sea grande (haciendo la misma división de antes). La generalización correcta en este escenario la dio Gowers con la introducción de las ahora llamadas normas de Gowers. Con ellas consiguió demostrar el teorema de Szemerédi usando un argumento análogo al de Roth. Después, usando nilsecuencias, Green y Tao dieron una noción análoga a los caracteres de Fourier para cada norma de Gowers. En particular, probaron un importante resultado en el área, conocido como teorema inverso, el cual dice (de manera informal) que si  $f$  es una función sobre  $\mathbb{Z}_p$  con  $p$  un primo grande, y  $0 < \varepsilon \leq \|f\|_{U^{k-1}}$  ( $\|\cdot\|_{U^{k-1}}$  es la norma  $k-1$  de Gowers), entonces existe una función  $g$  muy estructurada (más precisamente, una nilsecuencia de orden  $k-2$  y complejidad acotada en términos de  $\varepsilon$ ) tal que

$$c(\varepsilon) \leq \mathbb{E}(fg).$$

Szegedy desarrolló un enfoque novedoso sobre el teorema inverso, distinto del de Green y Tao, introduciendo en particular la noción de nilespacios junto con Antolín Camarena, y usándola con análisis en ultraproductos para demostrar una versión más general del teorema inverso [86]. Basándose en estos avances, Candela y Szegedy recientemente demostraron la versión cualitativa más general conocida actualmente del teorema inverso, válida para grupos abelianos compactos e incluso para nilvariedades (que son un ejemplo particular de nilespacio) [18], y Manners demostró una versión cuantitativa

del teorema inverso para  $\mathbb{Z}_p$  en [63]. En estos resultados, los nilespacios juegan un papel central. El teorema de Candela y Szegedy dice que dadas las hipótesis del teorema inverso sobre un grupo compacto abeliano  $G$ , existe un nilespacio  $X$  tal que se puede tomar  $g = F \circ \varphi$ , donde  $\varphi : G \rightarrow X$  es lo que se conoce como un morfismo de nilespacios compactos (una función que respeta la estructura algebraica y topológica de los nilespacios compactos) y  $F : X \rightarrow \mathbb{C}$  una función continua.

Por otra parte, desde el punto de vista de Teoría Ergódica, empecemos recordando el teorema de recurrencia múltiple de Furstenberg:

**Teorema 1.7** (Furstenberg). *Sea  $(\Omega, \mathcal{A}, \mu, T)$  un sistema de probabilidad que preserva la medida y  $A \in \mathcal{A}$  un conjunto de probabilidad positiva. Entonces para todo entero  $k \geq 1$  tenemos que*

$$\liminf_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mu(A \cap T^{-n}A \cap T^{-2n}A \cap \dots \cap T^{-kn}A) > 0.$$

Este fue el resultado en el que Furstenberg se apoyó para probar el teorema de Szemerédi en 1977. Una generalización natural de este resultado consiste en estudiar la convergencia en  $L^2(\mu)$  de medias de productos de funciones acotadas sobre progresiones aritméticas de longitud  $k \geq 1$ . En 2005 Host y Kra probaron el siguiente resultado:

**Teorema 1.8** (Host y Kra). *Sea  $(\Omega, \mathcal{A}, \mu, T)$  un sistema de probabilidad invertible que preserva la medida. Entonces para todo entero  $k \geq 1$  y funciones medibles  $f_j$  sobre  $\Omega$  acotadas para  $1 \leq j \leq k$ , tenemos que*

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N f_1(T^n \omega) f_2(T^{2n} \omega) \dots f_k(T^{kn} \omega)$$

*existe en  $L^2(\Omega)$ .*

Destaquemos que con anterioridad a que Host y Kra probaran este teorema, otros autores ya habían demostrado resultados parciales. El caso  $k = 1$  es un resultado clásico de Von Neumann, y Furstenberg probó el caso  $k = 2$ . Para  $k = 3$ , Conze y Lesigne probaron casos particulares, hasta que Host y Kra probaron el caso general para cualquier  $k \geq 1$  (otra prueba fue dada independientemente por Ziegler). Nótese la similitud de estas medias con los funcionales  $\Lambda_k(f_1, \dots, f_k)$  definidos anteriormente.

Para probar el Teorema 1.8, Host y Kra demostraron que bastaba estudiar la convergencia de ciertos sistemas, llamados *factores característicos* del sistema original. También demostraron que estos factores tienen una estructura que se puede describir con (límites inversos de) nilvariedades. Una generalización de este resultado es gracias a Candela y Szegedy usando el resultado de Candela, González-Sánchez y Szegedy que constituye el Capítulo 6 de esta tesis. Para generalizar los resultados de Host y Kra, Candela y Szegedy introdujeron el concepto de acoplamiento cúbico. Esto es esencialmente una familia de medidas tales que sus factores característicos son nilespacios.

Todos estos resultados indican que los nilespacios y los acoplamientos cúbicos son conceptos adecuados para describir numerosos fenómenos tanto en combinatoria como en teoría ergódica. Es por esto que pensamos que merecen un capítulo a parte en esta tesis. En él, presentaremos de forma resumida las teorías que se han desarrollado sobre nilespacios a partir del trabajo inicial de Antolín Camarena y Szegedy, a través de trabajos de varios autores, en particular Candela y también Gutman, Manners y Varjú. Presentaremos además nuevas pruebas de hechos conocidos y pequeños resultados que de por sí no son suficientes para una publicación propia, pero que son también de interés.

## 1.4 Sobre sistemas de nilespacios y sus morfismos

Como mencionábamos en la sección anterior, este trabajo se hizo como herramienta para generalizar el resultado de Host y Kra sobre factores característicos. Para empezar, muestra cómo si nos hacemos una pregunta sobre ciertos sistemas ergódicos podemos reducirla a una pregunta de nilespacios, mediante los resultados sobre acoplamientos cúbicos. Por tanto en este capítulo no encontraremos (hasta el final, donde viene explicada la aplicación) nada de teoría de la medida ni de sistemas ergódicos, tan sólo resultados sobre nilespacios. Para el lector no familiarizado con la teoría de nilespacios, recomendamos leer el Capítulo 5 de esta tesis.

La pregunta que nos hacemos es la siguiente. Sea  $X$  un nilespacio compacto y sea  $\{\alpha_j \in \Theta(X): j = 1, \dots, n\}$  un conjunto finito de traslaciones. ¿Existe una representación de  $X$  como  $\varprojlim X_i$  donde  $X_i$  son de rango

finito y para cada  $i \in \mathbb{N}$  y cada  $j = 1, \dots, n$  existe  $\beta_{i,j} \in \Theta(X_i)$  tal que  $\pi_i \circ \alpha_j = \beta_{i,j} \circ \pi_i$ ? Un primer intento sería utilizar el teorema del límite inverso (no confundir con el teorema inverso) para nilespacios y ver si los factores  $X_i$  que se obtienen tienen la propiedad buscada. Esto reduce la pregunta a comprobar si dadas una fibración  $\varphi : X \rightarrow Y$ , donde  $Y$  es de rango finito, y  $\alpha \in \Theta(X)$ , entonces  $\varphi \circ \alpha = \beta \circ \varphi$  para cierta  $\beta \in \Theta(Y)$ .

La respuesta a esta última pregunta es negativa en general, como probaremos con un ejemplo explícito. Sin embargo, lo que haremos es demostrar que existe un nilespacio  $Y'$  de rango finito y fibraciones  $\phi : X \rightarrow Y'$  y  $\psi : Y' \rightarrow Y$  con  $\psi \circ \phi = \varphi$ , de modo que exista  $\beta' \in \Theta(Y')$  tal que  $\phi \circ \alpha = \beta' \circ \phi$ . Usando este resultado, representaremos  $X$  como límite inverso de nilespacios  $X'_i$  que sí tengan la propiedad deseada.

## 1.5 Una nota sobre el teorema bilineal de Bogolyubov

Dado un subconjunto  $A \subset \mathbb{F}_p^n$  no vacío y enteros  $\ell, m \geq 0$  cualesquiera, el conjunto  $\ell A - mA$  está incluido en  $\text{span}(A)$ , el subespacio generado por  $A$ . De hecho, si  $\ell$  o  $m$  son lo suficientemente grandes y  $0 \in A$ , tenemos que  $\ell A - mA = \text{span}(A)$  (un argumento sencillo muestra que para que se dé esta igualdad basta que  $\max(\ell, m) \geq n(p-1)$ ). Sin embargo, el siguiente resultado demuestra que ya  $2A - 2A$  contiene un subespacio vectorial grande (comparado con el tamaño de  $A$ ):

**Teorema 1.9** (Bogolyubov). *Sea  $A \subset \mathbb{F}_p^n$  un subconjunto de densidad  $\alpha := |A|/p^n > 0$ . Entonces  $2A - 2A$  contiene un subespacio vectorial de codimensión  $O(\alpha^{-2})$ .*

Este resultado tiene múltiples aplicaciones en combinatoria aditiva. Por ejemplo, Gowers lo usó en su prueba del teorema de Szemerédi para progresiones de longitud 4 en  $\mathbb{F}_p^n$ . Para estudiar progresiones de longitud 5, Gowers y Milićević usaron una versión bilineal del mismo. Antes de formular un teorema bilineal de Bogolyubov definimos las sumas verticales (resp. horizontales) como

$$A \overset{V}{\pm} A := \{(x, y_1 \pm y_2) : (x, y_1), (x, y_2) \in A\}.$$

A partir de esta definición, sea  $\phi_V$  (resp.  $\phi_H$ ) el funcional

$$A \mapsto (A \overset{V}{+} A) \overset{V}{-} (A \overset{V}{+} A).$$

Bienvenu y Lê probaron la siguiente versión de Bogolyubov bilineal:

**Teorema 1.10** (Bienvenu y Lê). *Sea  $\delta > 0$ , entonces existe  $c(\delta) > 0$  de modo que se cumple lo siguiente. Si  $A \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  tiene densidad  $\delta$ , entonces existen subespacios  $W_1, W_2 \subseteq \mathbb{F}_p^n$  de codimensiones  $r_1$  y  $r_2$  respectivamente y formas bilineales  $Q_1, \dots, Q_{r_3}$  en  $W_1 \times W_2$  tales que  $\phi_H \phi_V \phi_H(A)$  contiene*

$$\{(x, y) \in W_1 \times W_2 : Q_1(x, y) = \dots = Q_{r_3}(x, y) = 0\} \quad (1.2)$$

y  $\max\{r_1, r_2, r_3\} \leq c(\delta)$ .

La pregunta que nos hacemos proviene de observar que si en el teorema de Bogolyubov tomamos un conjunto  $A \subset \mathbb{F}_p^n$  invariante por sumas,  $A + A = A$ , entonces ese conjunto es directamente un subespacio vectorial. Parecería natural pensar que en el caso bilineal esto se repite, i.e., si tomamos un conjunto  $A \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  tal que  $A \overset{V}{+} A = A$  y  $A \overset{H}{+} A = A$  (a estos conjuntos los llamaremos *transversos*), entonces  $A$  debería ser un conjunto de la forma (1.2) (a los cuales llamaremos *bilineales*). Esto es sin embargo falso, y en el Capítulo 7 lo probaremos con ejemplos explícitos, otros no constructivos pero que probarán que hay *muchos* conjuntos transversos no bilineales, y también resultados positivos en algunos casos particulares (si sabemos algo más del conjunto  $A$ ).

## 1.6 Apéndice A: Estructuras y resultados auxiliares para nilespacios

Este apéndice contiene herramientas que se usan para probar algunos de los resultados del Capítulo 5. Para no hacer este demasiado largo, se tomó la decisión de dividir el resumen de la extensa teoría de nilespacios entre un capítulo y un apéndice. Aquí encontraremos conceptos auxiliares como espacio de cubos, nilespacio no ergódico y tricubo, además de diversas pruebas y explicaciones. Cabe destacar el concepto de tricubo y composición de un tricubo, que presenta una manera alternativa de describir estos objetos a como se explica en los artículos originales de Antolín-Camarena y Szegedy, y en los trabajos posteriores de Candela y Szegedy.

## 1.7 Resumen y conclusiones

Los diferentes resultados expuestos tienen varias aplicaciones además de las ya mencionadas anteriormente. La versión continua de la desigualdad de Plünnecke-Ruzsa no sólo nos permite usarla en contextos más generales, sino que la prueba de este resultado puede servir de modelo a pruebas de multitud de resultados que se conocen de momento sólo para grupos finitos. El proceso de cómo discretizar un conjunto en un grupo abeliano de Lie y luego usar análisis de Fourier para extenderlo a grupos abelianos compactos es de interés propio, aunque en esta tesis nos hemos centrado en aplicarlo a la desigualdad de Plünnecke-Ruzsa.

Los avances hacia la conjetura  $3k - 4$  en  $\mathbb{Z}_p$  y su aplicación al estudio de conjuntos  $m$ -libres, aunque no resuelven completamente los problemas, son necesarios para poder ir avanzando en la teoría.

En cuanto a la teoría de nilespacios y acoplamientos cúbicos, parte de esta tesis puede verse como un ejemplo de cómo puede ser muy útil para resolver ciertos problemas. El Capítulo 5 por otro lado supone un resumen y ciertos complementos a la teoría de nilespacios, y su lectura debería complementarse con las referencias dadas en ese capítulo.

El Capítulo 6 desarrolla un resultado a priori teórico pero con una aplicación muy clara en mente, y amplía el conocimiento que tenemos sobre nilespacios, lo cual posiblemente será muy útil en un futuro próximo.

El Capítulo 7 es por otro lado un ejemplo de los problemas típicos que nos encontramos al estudiar problemas de Análisis de Fourier de Orden Superior, y de cómo muchas veces la generalización a estos casos no es *trivial*.

# Chapter 2

## Introduction

In this chapter, we are going to introduce and motivate the results that form this doctoral thesis. In addition to the first two chapters, the rest of the thesis can be divided into two parts: the third and fourth chapters are results in *classical* additive combinatorics, while the last three deal with problems related to the area of higher order Fourier analysis. The chapters are self-contained, all of them have their own introduction in addition to the one present in the first two chapters of the thesis. Redundancy between chapters has been narrowed to the minimum possible. The number of citations has been reduced in the first two chapters to ease the reading, postponing citations to the introductions of each chapter.

All chapters in this thesis, except the introductions and Chapter 5, are works that have already been published, or are being refereed in different journals ([11, 12, 13, 6]). Chapter 5 is different in nature because it contains a personal synthesis of the theory of nilspaces and cubic couplings. The reasons that justify such a chapter in a doctoral thesis are the following: understanding such a theory was essential to develop the last two chapters of the thesis; we have included new proofs, examples, and small results to the theory of nilspaces. We will be especially careful with citing references, clearly stating which results are original and which are not.

## 2.1 A Plünnecke-Ruzsa inequality in compact abelian groups

Let  $A \subset Z$  be a non-empty set where  $Z$  is an abelian group. We are interested in the growth rate of the set  $nA - mA$ , for any  $n, m$  non-negative integers, defined as

$$nA - mA := \{a_1 + \dots + a_n - a'_1 - \dots - a'_m : a_1, \dots, a_n, a'_1, \dots, a'_m \in A\},$$

in relation to the size of  $A$ . This question leaves intentionally open the question of how to measure the size of  $A$  and  $nA - mA$ . In principle, assume that  $A$  is finite and that the measure is the counting measure.

Now imagine that we know somehow that  $|2A| \leq \alpha|A|$  for some  $\alpha$ . It is reasonable to think that the number of distinct pairs  $a_1, a'_1 \in A$ ,  $a_2, a'_2 \in A$  such that  $a_1 + a'_1 = a_2 + a'_2$  is related to the value of  $\alpha$  (if  $\alpha$  is small then there will be *many* repetitions). Therefore, it is sensible to think that if we look at the size of  $3A$ , it would also grow according to  $\alpha$ , because those repetitions should appear as well. The Plünnecke-Ruzsa inequality is a result that quantifies this phenomenon:

**Theorem 2.1** (Plünnecke and Ruzsa). *Let  $A, B \subset Z$  be finite non-empty subsets of an abelian group  $Z$ . Suppose that there exists a number  $\alpha \geq 0$  such that  $|A + B| \leq \alpha|A|$ . Then, for any integers  $n, m \geq 0$  we have*

$$|nB - mB| \leq \alpha^{n+m}|A|.$$

This result is possibly one of the most used in additive combinatorics. In the last years, such results have often been needed in more general settings, not only for finite sets. One of the most natural generalizations consists in considering *reasonable* sets inside compact abelian groups, and measure them using the Haar measure. The first chapter of this thesis is devoted to such a generalization:

**Theorem 2.2** (Candela, González-Sánchez, and de Roton). *Let  $A, B \subset Z$  be  $K$ -analytic subsets of a compact abelian group. Let  $\mu$  be the Haar measure of  $Z$ , and let  $\alpha > 0$  be such that  $0 < \mu(A + B) \leq \alpha\mu(A)$ . Then for any integers  $m, n \geq 0$ , we have*

$$\mu(nB - mB) \leq \alpha^{n+m}\mu(A).$$

In the introduction of Chapter 3 we will give the precise definition of  $K$ -analytic sets. This class of sets is general enough to include the class of Borel sets if the ambient group is a compact Polish abelian group.

## 2.2 On sets with small sumset and $m$ -sum-free sets in $\mathbb{Z}_p$

The second chapter treats a problem that can be seen as a special case of the previous result. The question we are interested in is the following: suppose that  $|2A| \leq \alpha|A|$  where  $\alpha$  is a *very small* constant. Could we then say something more about  $A$ ?

First of all, let us give an idea of what is meant here by  $\alpha$  being *very small*. Suppose that the ambient group is  $\mathbb{Z}$ , and that we have a finite set  $A \subset \mathbb{Z}$ . A classical result in the area says that  $|2A| \geq 2|A| - 1$ , and that equality is attained if and only if  $A$  is an arithmetic progression. Thus, we already know that this value imposes a lower bound on  $\alpha$ . The question now is: what happens if we suppose that  $|2A|$  is slightly larger than  $2|A| - 1$ ? The intuitive answer would be:  $A$  should be very similar to an arithmetic progression. And, just like in the previous chapter, there exists a theorem that quantifies this intuition, namely Freiman's  $3k - 4$  theorem:

**Theorem 2.3** (Freiman). *Let  $A \subset \mathbb{Z}$  be a non-empty finite subset such that  $|2A| = 2|A| + r \leq 3|A| - 4$ . Then there exist arithmetic progressions  $P_A, P_{2A} \subset \mathbb{Z}$  such that  $A \subset P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subset 2A$  and  $|P_{2A}| \geq 2|A| - 1$ .*

Note that this implies, in particular, a stronger version of the Plünnecke-Ruzsa inequality in the case of  $\mathbb{Z}$  when  $\alpha$  is *very small*. This is one of the multiple applications of this result. The problem with this result is that so far it is only valid for the integers, but we would like to apply it to other groups. However, this time the generalization is not that obvious, because the inequality  $|2A| \geq 2|A| - 1$  no longer holds for every subset  $A$  of every abelian group (for instance, if  $A = \mathbb{Z}_p$ , then  $2A = \mathbb{Z}_p$ , and the inequality is false). The first step would be to find what is the equivalent of that minimum in other groups.

The particular case of  $\mathbb{Z}_p$  for  $p$  a prime is known as the Cauchy-Davenport inequality. It states that for any  $A \subset \mathbb{Z}_p$  we have that  $|2A| \geq \min(p, 2|A| -$

1). Hence, we can formulate a sensible conjecture on what the  $3k-4$  theorem in  $\mathbb{Z}_p$  could look like:

**Conjecture 2.4.** *Let  $A \subset \mathbb{Z}_p$  be a non-empty subset such that  $|2A| = 2|A| + r \leq \min(3|A| - 4, p - r - 3)$ . Then there exist arithmetic progressions  $P_A, P_{2A} \subset \mathbb{Z}_p$  such that  $A \subset P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subset 2A$  and  $|P_{2A}| \geq 2|A| - 1$ .*

There have been many partial results that point to the validity of this conjecture. One of the strongest of this kind was proved by Serra and Zémor in 2009.

In the fourth chapter of this thesis we prove a partial result towards Conjecture 2.4, which improves the result of Serra and Zémor for the range  $|A| \leq \frac{0.75p+3}{2.136861}$ , thus giving the best bounds currently known in this setting.

**Theorem 2.5** (Candela, González-Sánchez, and Grynkiewicz). *Let  $A \subset \mathbb{Z}_p$  be a non-empty subset such that*

$$|2A| \leq (2.136861)|A| - 3 \quad \text{and} \quad |2A| \leq \frac{3}{4}p.$$

*Then there exist arithmetic progressions  $P_A, P_{2A} \subset \mathbb{Z}_p$  such that  $A \subset P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subset 2A$  and  $|P_{2A}| \geq 2|A| - 1$ .*

In addition, we use this result to obtain new bounds for the problem of  $m$ -sum-free sets. We say that  $A \subset \mathbb{Z}_p$  is  $m$ -sum-free, for a fixed integer  $m \geq 3$ , if the equation  $x + y = mz$  does not have a solution for  $x, y, z \in A$ . Using our advances towards the  $3k - 4$  conjecture, if we define

$$d_m(\mathbb{Z}_p) = \max \left\{ \frac{|A|}{p} : A \subseteq \mathbb{Z}_p \text{ is } m\text{-sum-free} \right\},$$

we prove that

$$\lim_{p \rightarrow \infty} d_m(\mathbb{Z}_p) \leq \frac{1}{3.1955}.$$

This is the best known bound for this quantity currently. Using the Cauchy-Davenport inequality, the bound we obtain is  $1/3$ . The only non-trivial bound previous to ours was  $1/3.0001$  given by Candela and de Roton using the result of Serra and Zémor.

## 2.3 Nilspaces and cubic couplings

There are at least two important motivations for the concept of nilspaces (and cubic couplings): as an object that enables an extension of the notion of nilsequence in additive combinatorics, and as an object that describes certain characteristic factors of ergodic measure-preserving systems. Indeed, this concept enables a unification of many results in the aforementioned areas which, at least since the work of Furstenberg on Szemerédi's Theorem in 1977, are known to be related. Let us recall the statement of Szemerédi's theorem, one of the most important results in combinatorics.

**Theorem 2.6** (Szemerédi). *Let  $k \geq 3$  be an integer and  $A \subset \mathbb{N}$ . If  $A$  does not contain non-trivial arithmetic progressions<sup>1</sup> of length  $k$ , then  $|A \cap [1, N]| = o_k(N)$ .*

Imagine that we would like to study the subsets of the natural numbers that do not contain non-trivial arithmetic progressions (in the sequel, we will omit “non-trivial”). In 1953 Roth presented a proof of Szemerédi's theorem for the case of progressions of length 3. One of the key points of his argument was, given a set  $A \subset \mathbb{Z}_p$  with no arithmetic progression of length 3, to study the functional

$$\Lambda_3(1_A, 1_A, 1_A) := \mathbb{E}_{x,r \in \mathbb{Z}_p} 1_A(x)1_A(x+r)1_A(x+2r), \quad (2.1)$$

that counts the number of progressions of length 3 in  $A$ . The idea now is to use a decomposition of the form  $1_A = f_U + f_{U^\perp}$ , where  $f_U$  is the part we will call pseudorandom, and  $f_{U^\perp}$  the part we will call structured. For a certain choice of  $f_U$  and  $f_{U^\perp}$ , it is proved that there exists a Fourier character  $\chi$  such that  $\mathbb{E}(f_{U^\perp}\chi)$  is a large quantity (larger than a quantity that only depends on the density of  $A$ ). It is then proved, using an argument known as *density increment*, that if  $A \subset [1, N]$  does not contain arithmetic progressions of length 3, then  $|A| \ll N/\log \log N$ .

To study the case of progressions of length  $k \geq 4$ , we could study analogously the functional

$$\Lambda_k(f_1, \dots, f_k) = \mathbb{E}_{x,r \in \mathbb{Z}_p} f_1(x)f_2(x+r) \cdots f_k(x+(k-1)r).$$

---

<sup>1</sup>Let  $k \geq 3$  be an integer,  $G$  an abelian group, and  $x, r \in G$ . We say that  $x, x+r, x+2r, \dots, x+(k-1)r$  form an arithmetic progression of length  $k$ . If  $r \neq 0$ , we say that the progression is non-trivial.

The problem now is that we will not be able to do the same as before (in general), and find a Fourier character  $\chi$  such that  $\mathbb{E}(f_{U^\perp}\chi)$  is a large quantity (making the same decomposition as before). The correct generalization of this scenario was given by Gowers with the introduction of the now-called Gowers norms. With these norms, Gowers managed to prove Szemerédi's Theorem using an argument analogous to Roth's proof. Later, Green and Tao used nilsequences as analogues of Fourier characters for each Gowers norm. In particular, they proved an important result in this area, known as the inverse theorem, which says (informally) that if  $f$  is a function on  $\mathbb{Z}_p$  with  $p$  a large prime and  $0 < \varepsilon \leq \|f\|_{U^{k-1}}$  (where  $\|\cdot\|_{U^{k-1}}$  is the  $(k-1)$ -Gowers norm), then there exists a *very structured function*  $g$  (more precisely, a  $(k-2)$ -step nilsequence of complexity bounded in terms of  $\varepsilon$ ) such that

$$c(\varepsilon) \leq \mathbb{E}(fg).$$

Szegedy developed a novel approach to the inverse theorem, different from that of Green and Tao, introducing in particular the notion of nilspace in joint work with Antolín Camarena, and using it together with analysis on ultraproducts to prove a more general version of the inverse theorem [86]. Based on these advances, Candela and Szegedy recently proved the most general qualitative version of the inverse theorem known so far, valid for compact abelian groups and even nilmanifolds (which are special cases of nilspaces) [18], while Manners proved a quantitative version for  $\mathbb{Z}_p$  in [63]. In these results, nilspaces play a central role. The result of Candela and Szegedy says (roughly speaking) that assuming the largeness of the  $(k-1)$ -Gowers norm (as above) on some compact abelian group  $G$ , there exists a compact nilspace  $X$  such that we can take  $g = F \circ \varphi$  where  $\varphi : G \rightarrow X$  is a morphism of compact nilspaces (a function that respects the algebraic and topological structure of nilspaces), and  $F : X \rightarrow \mathbb{C}$  is a continuous function.

Concerning ergodic theory, let us recall Furstenberg's multiple recurrence theorem:

**Theorem 2.7** (Furstenberg). *Let  $(\Omega, \mathcal{A}, \mu, T)$  be a measure-preserving probability system and  $A \in \mathcal{A}$  a set of positive measure. Then for every integer  $k \geq 1$  we have*

$$\liminf_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mu(A \cap T^{-n}A \cap T^{-2n}A \cap \dots \cap T^{-kn}A) > 0.$$

Furstenberg used this result in his proof of Szemerédi's theorem in 1977. It is natural to try to generalize this result to study the convergence in  $L^2(\mu)$  of averages of products of bounded functions along an arithmetic progression of length  $k \geq 1$ . In 2005, Host and Kra proved the following result:

**Theorem 2.8** (Host and Kra). *Let  $(\Omega, \mathcal{A}, \mu, T)$  be an invertible measure-preserving probability system. Then for every integer  $k \geq 1$ , and bounded measurable functions  $f_j$  over  $\Omega$  for  $1 \leq j \leq k$ , we have that*

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N f_1(T^n \omega) f_2(T^{2n} \omega) \cdots f_k(T^{kn} \omega)$$

*exists in  $L^2(\Omega)$ .*

Let us remark that some particular cases of this theorem had been proved before. The case  $k = 1$  is a classical result by Von Neumann, and Furstenberg proved the case  $k = 2$ . For  $k = 3$ , Conze and Lesigne proved some particular cases, until the full proof for any  $k \geq 1$  was given by Host and Kra (and later independently by Ziegler). Note the similarities between these averages and the functionals  $\Lambda(f_1, \dots, f_k)$  defined previously.

To prove Theorem 2.8, Host and Kra proved that it was enough to study the convergence for certain special systems, called *characteristic factors* of the original system. They also proved that these factors have a structure that can be described with (inverse limits of) nilmanifolds. Candela and Szegedy generalized this result using another result of Candela, González-Sánchez and Szegedy which constitutes Chapter 6 of this thesis. To generalize the result of Host and Kra, Candela and Szegedy introduced the concept of cubic couplings. This is essentially a family of measures such that its characteristic factors are nilspaces.

All these results indicate that nilspaces and cubic couplings are adequate concepts to describe many phenomena in ergodic theory and combinatorics. This is the reason why we have included a chapter about them in this thesis. In that chapter, we will present in summarized form the theory of nilspaces that has developed since the original work of Antolín Camarena and Szegedy, through the subsequent work of several authors, including Candela and also Gutman, Manners and Varjú. We shall also present new proofs of known facts and small results that are not enough for a publication, but which are also interesting in themselves.

## 2.4 On nilspace systems and their morphisms

As we mentioned in the previous section, this work was a tool to generalize the result of Host and Kra on characteristic factors. First of all, it shows how certain natural questions about certain ergodic systems can be reduced to questions about nilspaces, using cubic couplings. Hence, in this chapter we will not find (until the very end, where the application is explained) anything about measure theory, nor ergodic theory, only results about nilspaces. For the reader not familiarized with the theory of nilspaces, we recommend Chapter 5 of this thesis.

The question we ask ourselves is the following. Let  $X$  be a compact nilspace and let  $\{\alpha_j \in \Theta(X) : j = 1, \dots, n\}$  be a finite set of translations. Is there a representation of  $X$  as an inverse limit  $\varprojlim X_i$  where  $X_i$  are compact finite-rank nilspaces, and for every  $i \in \mathbb{N}$  and every  $j = 1, \dots, n$  there exists  $\beta_{i,j} \in \Theta(X_i)$  such that  $\pi_i \circ \alpha_j = \beta_{i,j} \circ \pi_i$ ? A first attempt would be to use the inverse limit theorem (not to be confused with the inverse theorem) for nilspaces and check whether the factors  $X_i$  obtained have the desired properties. This reduces the question to seeing if, given a fibration  $\varphi : X \rightarrow Y$ , where  $Y$  is a compact finite-rank nilspace, and any  $\alpha \in \Theta(X)$ , we always have  $\varphi \circ \alpha = \beta \circ \varphi$  for some  $\beta \in \Theta(Y)$ .

The answer to this question is negative in general, as we will show with an explicit example. However, what we can do is prove that there exists a compact finite-rank nilspace  $Y'$  and fibrations  $\phi : X \rightarrow Y'$  and  $\psi : Y' \rightarrow Y$  such that  $\psi \circ \phi = \varphi$ , and such that there exists  $\beta' \in \Theta(Y')$  with  $\phi \circ \alpha = \beta' \circ \phi$ . Using this result, we represent  $X$  as the inverse limit of nilspaces  $X'_i$  with the desired property.

## 2.5 A note on the bilinear Bogolyubov theorem

Given a non-empty subset  $A \subset \mathbb{F}_p^n$  and any integers  $\ell, m \geq 0$ , the set  $\ell A - mA$  is included in  $\text{span}(A)$ , the subspace generated by  $A$ . A simple argument shows that if  $0 \in A$  and  $\max(\ell, m) \geq (p-1)n$ , then  $\ell A - mA = \text{span}(A)$ . However, the following result proves that already  $2A - 2A$  contains a *large* subspace (compared to the size of  $A$ ):

**Theorem 2.9** (Bogolyubov). *Let  $A \subset \mathbb{F}_p^n$  a subset of density  $\alpha := |A|/p^n > 0$ . Then  $2A - 2A$  contains a linear subspace of codimension  $O(\alpha^{-2})$ .*

This result has multiple applications in additive combinatorics. For example, Gowers used it in his proof of Szemerédi's theorem for progressions of length 4 in  $\mathbb{F}_p^n$ . To study progressions of length 5, Gowers and Milićević used a bilinear version of the result. To formulate a bilinear Bogolyubov theorem let us first define the vertical (resp. horizontal) sums as

$$A \overset{V}{\pm} A := \{(x, y_1 \pm y_2) : (x, y_1), (x, y_2) \in A\}.$$

Using that definition, let  $\phi_V$  (resp.  $\phi_H$ ) the functional

$$A \mapsto (A \overset{V}{+} A) \overset{V}{-} (A \overset{V}{+} A).$$

Bienvenu and Lê proved the following version of the bilinear Bogolyubov theorem:

**Theorem 2.10** (Bienvenu and Lê). *Let  $\delta > 0$ . Then there exists  $c(\delta) > 0$  such that the following holds. If  $A \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  is of density  $\delta$ , then there exist linear subspaces  $W_1, W_2 \subseteq \mathbb{F}_p^n$  of codimension  $r_1$  and  $r_2$  respectively, and bilinear forms  $Q_1, \dots, Q_{r_3}$  in  $W_1 \times W_2$  such that  $\phi_H \phi_V \phi_H(A)$  contains*

$$\{(x, y) \in W_1 \times W_2 : Q_1(x, y) = \dots = Q_{r_3}(x, y) = 0\} \quad (2.2)$$

where  $\max\{r_1, r_2, r_3\} \leq c(\delta)$ .

The question we posed comes from the following observation. In Bogolyubov's Theorem, if a set  $A \subset \mathbb{F}_p^n$  is invariant under sums  $A + A = A$ , then this set is a linear subspace. It could be natural to infer that in the bilinear case we have a similar behaviour, i.e., if we take a set  $A \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  such that  $A \overset{V}{+} A = A$  and  $A \overset{H}{+} A = A$  (these will be called *transverse sets*), then  $A$  should be a set of the form (2.2) (these will be called *bilinear sets*). However, this assertion is false, and in Chapter 7 we show it with explicit examples, a large amount of non-constructive examples, but also some positive results (when we know extra information about  $A$ ).

## 2.6 Appendix A: Auxiliary structures and results for nilspaces

This appendix contains many tools used to prove results in Chapter 5. In order not to make Chapter 5 too large, we split the summary about the theory of nilspaces between a chapter and an appendix. Auxiliary concepts such as cubespace, non-ergodic nilspace, tricube, and many proofs and explanations constitute this appendix. It is worth highlighting the concept of tricube and tricube composition, which is presented here in an alternative way from that in the original papers of Antolín-Camarena and Szegedy, and later works of Candela and Szegedy.

## 2.7 Summary and conclusions

The different results presented in this thesis have diverse applications in addition to the ones already mentioned. The proof of the Plünnecke-Ruzsa inequality in compact abelian groups can be used as a model for similar results. For instance, it can be used to extend theorems in additive combinatorics that currently deal with finite groups. The discretization process of a set in a compact abelian Lie group, with the use of Fourier analysis to extend it to compact abelian groups, is interesting in itself, although we have used it only to prove the Plünnecke-Ruzsa inequality.

The advances towards the  $3k - 4$  conjecture in  $\mathbb{Z}_p$  and its application to the study of  $m$ -sum-free sets are necessary to further the theory, although we do not prove the full conjecture.

About the theory of nilspaces and cubic couplings, some parts in this thesis are devoted to showing how it can be very useful to solve certain problems. Chapter 5 constitutes a summary of the theory of nilspaces, and its reading should be complemented with the references given in that chapter.

Chapter 6 develops an a priori theoretical result but with a very clear application in mind. It also furthers the knowledge about nilspaces, a theory likely to find further uses in the future.

Chapter 7 shows a typical problem that appears naturally in higher order Fourier analysis, and how on many occasions the generalization is not trivial.

# Chapter 3

## A Plünnecke-Ruzsa inequality in compact abelian groups

First published in *Revista Matemática Iberoamericana* in Volume 35, Issue 7, 2019, published by the European Mathematical Society. This chapter was written in collaboration with Pablo Candela and Anne de Roton. For the original publication see [11].

### 3.1 Introduction

The Plünnecke-Ruzsa inequality is a central result in additive combinatorics, providing useful upper bounds for the cardinality of iterated sums and differences of a finite subset of an abelian group. The version of the result that is used most often is the following.

**Theorem 3.1.** *Let  $A, B$  be finite non-empty subsets of an abelian group and suppose that  $|A + B| \leq \alpha|A|$ . Then for all non-negative integers  $m, n$  we have  $|mB - nB| \leq \alpha^{m+n}|A|$ .*

A first version of this result (for iterated sums only) was proved by Plünnecke in the late 1960s [70]. The proof was simplified and the result extended to sums and differences by Ruzsa in the late 1980s [76]. Both of these treatments of the result used nontrivial tools from graph theory. In 2011, a much shorter and elementary proof was given by Petridis [67]. We refer the reader to the latter paper and also to the survey [68] of the same author for more background on this result and its numerous applications.

Theorem 3.1 is applicable in the discrete setting of *finite* subsets of abelian groups. Other central tools to handle sumsets have gained much applicability by being extended from the discrete setting to more general settings including continuous groups. This is the case for instance for the Cauchy-Davenport inequality, which was extended to the circle group in [71], to tori in [61], and to compact connected abelian groups in [57]. This motivates extending Theorem 3.1 to more general subsets of more general abelian groups. Here we focus on Haar-measurable subsets of compact abelian groups, aiming for an extension of Theorem 3.1 with the cardinality replaced by the Haar probability measure. This leads us to seek a suitable class of Haar-measurable sets for which to prove such an extension. Such a class should be sufficiently general, but it is also natural to require it to be stable under addition, meaning that if  $A, B$  are sets in this class then so is their sumset  $A + B$ . Questions related to this stability were already of interest to Erdős and Stone, who showed in [25] that the sum of two Borel sets can fail to be Borel. It is also known since Sierpiński's work [83] that the sum of Lebesgue measurable sets need not be Lebesgue measurable (see also [23]). However, the class of *analytic sets* is stable under addition (as was already noted in [25, 83]), and in a Polish space (a separable topological space metrizable by a complete metric) this class is general enough to contain all Borel sets; see Proposition 8.2.3 of [24]. In this chapter we extend the Plünnecke-Ruzsa inequality to analytic sets in compact Polish abelian groups, and thus to all Borel sets in such groups. In fact, our main result holds for the more general class of *K-analytic sets*, which can be defined in any compact (Hausdorff) abelian group, as we recall below.

There are also extensions of additive combinatorial tools to the non-abelian setting, for instance in [55] and more recently in [88]. The latter paper includes a variant of the Plünnecke-Ruzsa inequality (with weaker bounds) for non-abelian groups (see Lemma 3.4 in [88]), and also related results for open sets in some continuous groups. The extensions in this chapter go in a different direction, their aim being to make the Plünnecke-Ruzsa inequality applicable to as large a class of sets as possible in the compact abelian setting.

Before we state our main result, let us recall some definitions. All compact abelian groups in the sequel are assumed to be Hausdorff. In the setting of general Hausdorff topological spaces, Choquet defined the useful notion of a *K-analytic set*; see Definition 3.1 in [20]. This extended the classical notion of analytic set defined by Lusin and Souslin [60, 85], the latter notion

pertaining to Polish spaces. To state Choquet's definition, let us first recall that a subset  $B$  of a topological space  $X$  is a  $K_{\sigma\delta}$  set if  $B = \bigcap_{i \in \mathbb{N}} \bigcup_{j \in \mathbb{N}} K_{i,j}$ , for compact sets  $K_{i,j} \subset X$ .

**Definition 3.2** (Choquet). Let  $X$  be a Hausdorff topological space. A set  $A \subset X$  is a  $K$ -analytic set if there is a  $K_{\sigma\delta}$  set  $B$  in a compact Hausdorff space and a continuous map  $f : B \rightarrow X$  such that  $A = f(B)$ .

We recall more background on  $K$ -analytic sets in Section 3.4 below. Let us note for now that the sum or difference of two  $K$ -analytic sets in a compact abelian group  $G$  is  $K$ -analytic (this follows from the definition, and is detailed in Section 3.4), and that  $K$ -analytic subsets of  $G$  are Haar-measurable; see Theorem 4.3 in [84]. Let  $\mu$  denote the Haar probability measure on  $G$ . We can now state our main result.

**Theorem 3.3.** *Let  $G$  be a compact abelian group and let  $A, B$  be  $K$ -analytic subsets of  $G$  satisfying  $0 < \mu(A+B) \leq \alpha \mu(A)$ . Then we have  $\mu(mB - nB) \leq \alpha^{m+n} \mu(A)$  for all non-negative integers  $m, n$ .*

As mentioned above, if  $G$  is also Polish then the theorem holds in particular for any Borel sets  $A, B \subset G$ . We also prove the following variant, which can be useful in cases where the constant  $\alpha \geq 1$  is close to 1.

**Theorem 3.4.** *Let  $G$  be a connected compact abelian group and let  $A, B$  be  $K$ -analytic subsets of  $G$  satisfying  $0 < \mu(A+B) \leq \alpha \mu(A)$ . Then for all  $n \in \mathbb{N}$  such that  $\alpha^n < 1/\mu(A)$ , we have  $\mu(nB) \leq (\alpha^n - 1) \mu(A)$ .*

This result also holds in finite groups in which an analogue of the Cauchy-Davenport inequality is available, as we shall explain in the sequel.

The condition  $0 < \mu(A+B)$  in the theorems above is necessary. Indeed, let  $C$  be the Cantor middle-third set in  $[0, 1]$ , and let  $B$  denote  $C$  viewed as a subset of the circle group  $\mathbb{T} = \mathbb{R}/\mathbb{Z}$  (identifying this group as a set with  $[0, 1)$  the usual way). Since in  $\mathbb{R}$  we have  $C+C = [0, 2]$  (as can be seen using ternary expansions), in  $\mathbb{T}$  we have  $\mu(mB - nB) = 1$  whenever  $m+n \geq 2$ . If we now let  $A$  be a singleton in  $\mathbb{T}$ , then  $\mu(A+B) = \mu(B) = 0$ . In particular, for every  $\alpha > 0$  we have  $\mu(A+B) \leq \alpha \mu(A)$ , but the conclusion of Theorem 3.3 fails for all  $m, n \in \mathbb{N}$ .

The chapter is laid out as follows. In Section 3.2 we establish the special case of Theorem 3.3 for closed subsets of an arbitrary compact abelian

Lie group. In Section 3.3, we prove an approximation result for closed subsets of general compact abelian groups by subsets of compact abelian Lie groups, which refines a similar result from [19]. This is then combined in Section 3.4 with measure-theoretic results concerning  $K$ -analytic subsets of Hausdorff spaces, and using this we complete the proofs of Theorems 3.3 and 3.4. In Section 3.5 we discuss further extensions of Theorem 3.3. In particular we prove a version of Theorem 3.3 involving the inner Haar measure, which allows the set  $A$  to be arbitrary; see Theorem 3.20. We then discuss further possible extensions of Theorem 3.3 to more general classes of Haar measurable sets, a direction which leads to basic questions in descriptive topology concerning generalizations of  $K$ -analytic sets (see for instance Question 3.27).

**Acknowledgements.** We are very grateful to Petr Holický for providing the example in Proposition 3.26 and for very useful comments. We also thank the anonymous referee for useful remarks.

## 3.2 The case of closed sets in compact abelian Lie groups

Every compact abelian Lie group is isomorphic to  $\mathbb{T}^d \times Z$  for some non-negative integer  $d$  and some finite abelian group  $Z$ ; see Proposition 2.42 in [44]. In this section we prove the following special case of Theorem 3.3.

**Theorem 3.5.** *Let  $A, B$  be closed subsets of  $\mathbb{T}^d \times Z$  satisfying  $0 < \mu(A + B) \leq \alpha \mu(A)$ . Then for all non-negative integers  $\ell, m$  we have  $\mu(\ell B - mB) \leq \alpha^{\ell+m} \mu(A)$ .*

*Remark 3.6.* The sum or difference of any finite number of closed sets in a compact abelian group is closed. Indeed, in a compact Hausdorff space a set is closed if and only if it is compact. Therefore, the sum of any (finite) number of closed sets is the image of a compact set through a continuous map, so it is compact, whence it is also closed.

Given a set  $A \subset \mathbb{T}^d \times Z$ , and a positive integer  $n$ , we define the set

$$A_n = A + \left[ -\frac{1}{n}, \frac{1}{n} \right]^d \times \{0_Z\} \subset \mathbb{T}^d \times Z. \quad (3.1)$$

*Remark 3.7.* The sequence of sets  $(A_n)_{n \in \mathbb{N}}$  is decreasing and  $\bigcap_{n \in \mathbb{N}} A_n = \overline{A}$ . In particular, for a closed set  $A$ , by continuity of  $\mu$  we have  $\mu(A_n) \rightarrow \mu(A)$ .

Theorem 3.1 is usually deduced from the following result (see Theorem 3.1 in [67]).

**Theorem 3.8.** *Let  $A$  and  $B$  be finite non-empty subsets of an abelian group satisfying  $|A + B| \leq \alpha|A|$ . Then there exists a non-empty subset  $X \subset A$  such that for every positive integer  $m$  we have  $|X + mB| \leq \alpha^m|X|$ .*

In the same spirit, we shall first establish the following analogue of Theorem 3.8 for closed subsets of compact abelian Lie groups.

**Theorem 3.9.** *Let  $A, B$  be closed subsets of  $\mathbb{T}^d \times Z$  satisfying  $0 < \mu(A + B) \leq \alpha \mu(A)$ . Then for every  $\varepsilon > 0$ , for every sufficiently large  $n \in \mathbb{N}$  there exists a non-empty closed subset  $A'_n \subset A_n$  such that for every  $m \in \mathbb{N}$  we have  $\mu(A'_n + mB) \leq (1 + \varepsilon)^m \alpha^m \mu(A'_n)$ .*

Let us record a consequence that we shall use later to obtain Theorem 3.4.

**Corollary 3.10.** *Let  $A, B$  be closed subsets of  $\mathbb{T}^d$  satisfying  $0 < \mu(A + B) \leq \alpha \mu(A)$ . Then for every positive integer  $m$  such that  $\alpha^m < 1/\mu(A)$ , we have  $\mu(mB) \leq (\alpha^m - 1)\mu(A)$ .*

The condition  $\alpha^m < 1/\mu(A)$  is seen to be necessary by letting  $A = B$  with  $\mu(A) > 1/2$ ,  $m = 1$ , and  $\alpha = \frac{1}{\mu(A)} < 2$ . We then have  $\mu(A + B) = 1 = \alpha \mu(A)$ , yet  $\mu(B) > (\alpha - 1)\mu(A)$ .

*Proof.* Let  $(\varepsilon_j)_{j \in \mathbb{N}}$  be a decreasing sequence of positive numbers tending to 0, and let  $(n_j)_{j \in \mathbb{N}}$  be a strictly increasing sequence of positive integers such that for every  $j$  there exists a closed set  $A'_{n_j} \subset A_{n_j}$  satisfying  $\mu(A'_{n_j} + mB) \leq (1 + \varepsilon_j)^m \alpha^m \mu(A'_{n_j})$ . From the assumption  $\alpha^m < 1/\mu(A)$  it follows that  $\mu(A'_{n_j} + mB) \leq (1 + \varepsilon_j)^m \alpha^m \mu(A'_{n_j}) < 1$  for  $j$  sufficiently large, so we may apply Macbeath's analogue for  $\mathbb{T}^d$  of the Cauchy-Davenport inequality, see Theorem 1 in [61], to deduce that  $\mu(A'_{n_j} + mB) \geq \mu(A'_{n_j}) + \mu(mB)$ , whence  $\mu(mB) \leq ((1 + \varepsilon_j)^m \alpha^m - 1) \mu(A'_{n_j}) \leq ((1 + \varepsilon_j)^m \alpha^m - 1) \mu(A_{n_j})$ . Letting  $j \rightarrow \infty$  and using the continuity of the Haar measure, the result follows.  $\square$

To prove Theorem 3.9 we begin with the following basic fact.

**Lemma 3.11.** *Let  $A, B \subset \mathbb{T}^d \times Z$  be closed sets. Then  $\mu(A_n + B_n) \rightarrow \mu(A + B)$  as  $n \rightarrow \infty$ .*

*Proof.* It suffices to prove that  $\bigcap_{n \in \mathbb{N}} (A_n + B_n) = A + B$ . Indeed, since for each  $n$  we have  $A_n + B_n = A + B + \left([- \frac{2}{n}, \frac{2}{n}]^d \times \{0_Z\}\right)$ , the sequence of sets  $(A_n + B_n)_{n \in \mathbb{N}}$  is decreasing, so the result would then follow by continuity of  $\mu$ . Clearly  $\bigcap_{n \in \mathbb{N}} (A_n + B_n) \supset A + B$ . To see the opposite inclusion, let  $x \in \bigcap_{n \in \mathbb{N}} (A_n + B_n)$ . For every  $n$  let  $a_n \in A_n, b_n \in B_n$  such that  $x = a_n + b_n$ . There is a convergent subsequence  $(a_k)$  of  $(a_n)$  and, within the resulting set of integers  $k$ , there is an infinite subset of integers  $\ell$  such that  $(b_\ell)$  converges as well. We thus have  $a, b \in \mathbb{T}^d \times Z$  such that  $a_\ell \rightarrow a$  and  $b_\ell \rightarrow b$  as  $\ell \rightarrow \infty$ , and  $a_\ell + b_\ell = x$  for every  $\ell$ . Since  $a_\ell \in A_\ell$  and  $b_\ell \in B_\ell$ , by definition of these sets there exist  $a'_\ell \in A, b'_\ell \in B$  such that  $a_\ell - a'_\ell$  and  $b_\ell - b'_\ell$  both converge to 0 as  $\ell \rightarrow \infty$ . Hence  $a'_\ell \rightarrow a$  and  $b'_\ell \rightarrow b$  as  $\ell \rightarrow \infty$ . Since  $A, B$  are closed, we have  $a \in A$  and  $b \in B$ . Hence  $x = \lim_{\ell \rightarrow \infty} (a_\ell + b_\ell) = \lim_{\ell \rightarrow \infty} a_\ell + \lim_{\ell \rightarrow \infty} b_\ell = a + b \in A + B$ , as required.  $\square$

*Proof of Theorem 3.9.* Fix any  $\varepsilon > 0$ . Since  $\mu(A + B) > 0$ , by Lemma 3.11 there exists  $n$  such that  $\mu(A_n + B_n) \leq (1 + \varepsilon) \mu(A + B)$ . We also have  $\mu(A) > 0$  so, since  $\bigcap_n A_n = A$ , we can also suppose that  $\mu(A_n) \leq (1 + \varepsilon) \mu(A)$ , by taking  $n$  even larger if necessary.

Consider now  $A_{2n}, B_{2n}$ , which also satisfy  $\mu(A_{2n} + B_{2n}) \leq (1 + \varepsilon) \mu(A + B)$ . Let  $N = 2n$ , and consider the following discrete subgroup of  $\mathbb{T}^d \times Z$  (where we identify  $\mathbb{T}^d$  as a set with  $[0, 1)^d$ , and  $\mathbb{Z}_N$  denotes the integers in  $[0, N - 1]$  with addition mod  $N$ ):

$$\left(\frac{1}{N} \mathbb{Z}_N^d\right) \times Z := \left\{ \left(\frac{j}{N}, z\right) : j \in \{0, \dots, N - 1\}^d, z \in Z \right\}.$$

We denote the small cube  $[0, \frac{1}{N})^d \times \{0_Z\}$  by  $Q$ , and define the following subsets of  $\mathbb{T}^d \times Z$ :

$$D_A := \left\{ \left(\frac{j}{N}, z\right) \in \left(\frac{1}{N} \mathbb{Z}_N^d\right) \times Z : \left(\left(\frac{j}{N}, z\right) + Q\right) \cap A_{2n} \neq \emptyset \right\},$$

$$D_B := \left\{ \left(\frac{j}{N}, z\right) \in \left(\frac{1}{N} \mathbb{Z}_N^d\right) \times Z : \left(\left(\frac{j}{N}, z\right) + Q\right) \cap B_{2n} \neq \emptyset \right\}.$$

We claim that

$$A_{2n} \subset D_A + Q \subset A_n. \tag{3.2}$$

To see the first inclusion, note that for every  $x \in A_{2n}$  there exists a unique  $j \in [0, N)^d$  and  $z \in Z$  such that  $x \in \left(\frac{j}{N}, z\right) + Q$ , and then by definition

we have  $(\frac{j}{N}, z) \in D_A$ . To see the second inclusion, note that for every  $x \in D_A + Q$  there is  $(\frac{j}{N}, z) \in D_A$  such that  $(\frac{j}{N}, z) + Q$  contains both  $x$  (by assumption) and also some  $a \in A_{2n}$  (by definition of  $D_A$ ). Therefore  $x \in a + ((-\frac{1}{N}, \frac{1}{N})^d \times \{0_Z\}) \subset A_{2n} + ((-\frac{1}{N}, \frac{1}{N})^d \times \{0_Z\})$ . Since this holds for every such  $x$ , it follows that  $D_A + Q \subset A_{2n} + ((-\frac{1}{N}, \frac{1}{N})^d \times \{0_Z\}) \subset A_n$ .

In exactly the same way, we obtain that

$$B_{2n} \subset D_B + Q \subset B_n. \quad (3.3)$$

We now claim that

$$|D_A + D_B + (\{0, \frac{1}{N}\}^d \times \{0_Z\})| \leq (1 + \varepsilon) \alpha |D_A|. \quad (3.4)$$

Indeed, the left side equals  $N^d |Z| \mu(D_A + D_B + (\{0, \frac{1}{N}\}^d \times \{0_Z\}) + Q)$ , which is

$$N^d |Z| \mu(D_A + D_B + ([0, \frac{2}{N}]^d \times \{0_Z\})) = N^d |Z| \mu(D_A + Q + D_B + Q).$$

By (3.2) and (3.3), this is at most  $N^d |Z| \mu(A_n + B_n)$ . By our choice of  $n$  and our assumptions, this is at most  $N^d |Z| (1 + \varepsilon) \mu(A + B) \leq N^d |Z| (1 + \varepsilon) \alpha \mu(A) \leq N^d |Z| (1 + \varepsilon) \alpha \mu(A_{2n})$ . By (3.2) this is at most  $N^d |Z| (1 + \varepsilon) \alpha \mu(D_A + Q) = (1 + \varepsilon) \alpha |D_A|$ , and (3.4) follows.

Now, given (3.4), we apply Theorem 3.8 to  $D_A$  and  $D_B + (\{0, \frac{1}{N}\}^d \times \{0_Z\})$  in the finite group  $\frac{1}{N} \mathbb{Z}_N^d \times Z$ , and we obtain a set  $D_{A'} = D_{A',n} \subset D_A$  such that for every  $m \geq 1$

$$|D_{A'} + m(D_B + (\{0, \frac{1}{N}\}^d \times \{0_Z\}))| \leq (1 + \varepsilon)^m \alpha^m |D_{A'}|.$$

Let  $A'_n = D_{A'} + \overline{Q} = D_{A'} + ([0, \frac{1}{N}]^d \times \{0_Z\})$ , which is a closed subset of  $A_n$ . Using (3.3) we have  $A'_n + mB_{2n} \subset D_{A'} + \overline{Q} + m(D_B + Q) = D_{A'} + mD_B + ([0, \frac{m+1}{N}]^d \times \{0_Z\})$ , and this last set in turn is  $D_{A'} + mD_B + (\{0, \frac{1}{N}, \dots, \frac{m}{N}\}^d \times \{0_Z\}) + Q$ , which equals  $D_{A'} + m(D_B + \{0, \frac{1}{N}\}^d \times \{0_Z\}) + Q$ . Note that this last set has measure equal to  $N^{-d} |Z|^{-1} |D_{A'} + m(D_B + \{0, \frac{1}{N}\}^d \times \{0_Z\})|$ . Hence

$$\begin{aligned} \mu(A'_n + mB) &\leq \mu(A'_n + mB_{2n}) \\ &\leq N^{-d} |Z|^{-1} |D_{A'} + m(D_B + \{0, \frac{1}{N}\}^d \times \{0_Z\})| \\ &\leq (1 + \varepsilon)^m \alpha^m N^{-d} |Z|^{-1} |D_{A'}| = (1 + \varepsilon)^m \alpha^m \mu(A'_n). \end{aligned}$$

□

To deduce Theorem 3.5, we emulate the argument from the discrete setting, which uses Ruzsa's triangle inequality. To do so we use the following generalization of this inequality, which follows directly from the proof of a more general version by Tao (valid also in the non-commutative setting), namely Lemma 3.2 in [88].

**Lemma 3.12.** *Let  $A_1, A_2, A_3$  be closed subsets of a compact abelian group with Haar measure  $\mu$ . Then  $\mu(A_1 - A_3) \mu(A_2) \leq \mu(A_1 - A_2) \mu(A_2 - A_3)$ .*

The main result of this section can now be obtained.

*Proof of Theorem 3.5.* We apply Theorem 3.9 to  $A$  and  $B$  with any fixed  $\varepsilon > 0$ , and obtain that for all  $n$  sufficiently large  $\mu(A'_n + mB) \leq (1 + \varepsilon)^m \alpha^m \mu(A'_n)$ , for some  $A'_n \subset A_n$  closed and any integer  $m \geq 0$ . If one of  $\ell$  or  $m$  is 0, say  $\ell = 0$ , then we have immediately  $\mu(mB) \leq \mu(A'_n + mB) \leq (1 + \varepsilon)^m \alpha^m \mu(A_n)$ , and so letting  $n \rightarrow \infty$ , using that  $\bigcap_{n \geq 1} A_n = A$ , and then letting  $\varepsilon \rightarrow 0$ , we deduce that  $\mu(mB) \leq \alpha^m \mu(A)$  as required. If  $\ell, m$  are both positive, then by Lemma 3.12 applied with  $A_1 = \ell B$ ,  $A_2 = -A'_n$ ,  $A_3 = mB$ , we have

$$\begin{aligned} \mu(\ell B - mB) \mu(A'_n) &\leq \mu(\ell B + A'_n) \mu(A'_n + mB) \\ &\leq (1 + \varepsilon)^{\ell+m} \alpha^{\ell+m} \mu(A'_n)^2 \\ &\leq (1 + \varepsilon)^{\ell+m} \alpha^{\ell+m} \mu(A'_n) \mu(A_n). \end{aligned}$$

From the proof of Theorem 3.9 we have  $\mu(A'_n) > 0$ . Dividing by this and letting  $n \rightarrow \infty$ , we obtain  $\mu(\ell B - mB) \leq (1 + \varepsilon)^{\ell+m} \alpha^{\ell+m} \mu(A)$ . Letting  $\varepsilon \rightarrow 0$ , the result follows.  $\square$

To complete the proof of Theorem 3.3, firstly, in the next section we approximate any compact abelian group by a Lie group in such a way that Theorem 3.5 can be used to deduce the case of Theorem 3.3 for *closed* sets. Then in Section 3.4, using approximation results for  $K$ -analytic sets in Hausdorff spaces, we deduce Theorem 3.3 in full generality.

### 3.3 Extension to closed subsets of compact abelian groups

Approximating compact groups by compact Lie groups is a standard technique, and it has been used already in arithmetic combinatorics (e.g. in

[19]). However, here we shall need such approximations with the added guarantee that they behave well with respect to addition. We ensure this by working with closed sets, obtaining the following result.

**Lemma 3.13.** *Let  $G$  be a compact abelian group with Haar probability measure  $\mu$ , let  $A, B$  be closed subsets of  $G$ , and let  $\delta > 0$ . Then there exists a compact abelian Lie group  $G_0$ , a continuous surjective homomorphism  $q : G \rightarrow G_0$ , and closed sets  $A', B' \subset G_0$ , such that  $A \subset q^{-1}(A')$ ,  $B \subset q^{-1}(B')$ ,  $\mu(q^{-1}(A') \setminus A) < \delta$ , and  $\mu(q^{-1}(A' + B') \setminus (A + B)) < \delta$ .*

*Remark 3.14.* The proof of this lemma will make it clear that we would be able to approximate simultaneously any finite number of sets, as well as combinations of them using sum and difference. For example, given closed sets  $A_1, A_2, A_3$  we could obtain sets  $A'_i$  in  $G_0$  such that  $A_i \subset q^{-1}(A'_i)$ ,  $\mu(q^{-1}(A'_i) \setminus A_i) < \delta$  for  $i = 1, 2, 3$ , and also  $\mu(q^{-1}(A'_1 + A'_2) \setminus (A_1 + A_2)) < \delta$  and  $\mu(q^{-1}(A'_1 + A'_2 - 2A'_3) \setminus (A_1 + A_2 - 2A_3)) < \delta$ .

To prove Lemma 3.13, we first prove the following modification of Lemma A.2 in [19].

**Lemma 3.15.** *Let  $G$  be a compact abelian group, let  $A$  be a closed subset of  $G$ , and let  $0 < \delta < 1/2$ . Then there exists a compact abelian Lie group  $G_0$  and a continuous surjective homomorphism  $q : G \rightarrow G_0$  such that, letting  $A' = q(A)$ , we have  $\mu(q^{-1}(A') \setminus A) < \delta$ .*

*Proof.* By regularity of  $\mu$ , there is an open set  $U \supset A$  such that  $\mu(U \setminus A) < \delta^3/2^{10}$ . By Urysohn's lemma (see Theorem 32.3 and Theorem 33.1 in [65]) there is a continuous function  $h : G \rightarrow [0, 1]$  such that  $h(x) = 1$  for all  $x \in A$  and  $h(x) = 0$  for all  $x \notin U$ . Then

$$\|1_A - h\|_{L^1(G)} = \int_A |1_A - h| \, d\mu + \int_{U \setminus A} |1_A - h| \, d\mu + \int_{U^c} |1_A - h| \, d\mu.$$

The first and last integrals are 0, and the second one is at most  $\mu(U \setminus A) < \delta^3/2^{10}$ .

By the Stone-Weierstrass theorem, there is a trigonometric polynomial  $P(x)$  such that  $\|h - P\|_{L^\infty(G)} < \delta^3/2^{10}$  (see p. 24 in [75]), whence  $\|P - 1_A\|_{L^1(G)} < \delta^3/2^9$ . By the triangle inequality we also have  $\|P\|_{L^\infty(G)} < 2$ . Here the proof differs from that of Lemma A.2 in [19]: here  $|P(a) - 1| < \delta^3/2^{10}$  holds for all  $a \in A$  (we use this at the end of the proof).

Let  $\widehat{G}$  be the dual group of  $G$  and let  $\widehat{G}_0$  be the subgroup of  $\widehat{G}$  generated by the spectrum of  $P$ , i.e., by the finite set  $\{\gamma \in \widehat{G} : \widehat{P}(\gamma) \neq 0\}$ . Then  $\widehat{G}_0$  is a finitely generated discrete abelian group, therefore it is the dual of a compact abelian Lie group  $G_0$ . Letting  $\Lambda$  be the annihilator of  $\widehat{G}_0$  ( $\Lambda$  a closed subgroup of  $G$ ), we have that  $G_0$  is isomorphic as a compact abelian group to  $G/\Lambda$  (see [75] section 2.1), so the map  $G \rightarrow G/\Lambda$  gives a continuous surjective homomorphism  $q : G \rightarrow G_0$ . Then there exists a trigonometric polynomial  $P_0$  on  $G_0$  with  $P = P_0 \circ q$ , whence  $\|P_0\|_{L^\infty(G_0)} \leq 2$ . Moreover, writing  $P - P^2 = P - 1_A + 1_A^2 - P^2$ , we have

$$\begin{aligned} \|P_0 - P_0^2\|_{L^1(G_0)} &= \|P - P^2\|_{L^1(G)} \\ &\leq \int_G |1_A - P| \, d\mu_G + \int_G |1_A - P| |1_A + P| \, d\mu_G < \delta^3/2^7. \end{aligned}$$

Therefore, the set  $D := \{x \in G_0 : |P_0(x) - P_0^2(x)| > \delta^2/2^4\}$  has measure at most  $\delta/8$ . For every  $x$  in the complement  $D^c = G_0 \setminus D$ , we must have  $|P_0(x)| \leq \delta/4$  or  $|1 - P_0(x)| \leq \delta/4$ .

Now let  $A_0 := \{x \in G_0 : |P_0(x) - 1| \leq \delta/4\}$ . We have that  $\|1_{A_0} - P_0\|_{L^1(G_0)}$  is at most

$$3 \int_D d\mu_{G_0} + \int_{A_0 \cap D^c} |1 - P_0(x)| \, d\mu_{G_0} + \int_{A_0^c \cap D^c} |P_0(x)| \, d\mu_{G_0} < 7\delta/8,$$

so  $\mu_G(A \Delta q^{-1}(A_0)) \leq \|1_A - P\|_{L^1} + \|P - 1_{A_0} \circ q\|_{L^1} = \|1_A - P\|_{L^1(G)} + \|1_{A_0} - P_0\|_{L^1(G_0)} < \delta$ .

Now note that by definition of  $A_0$  it is clear that  $A' := q(A)$  is included in  $A_0$ , because  $|1 - P(a)| < \delta^3/2^{10}$  for all  $a \in A$ . So indeed, we have that  $\mu_G(q^{-1}(A_0) \setminus A) < \delta$ . Moreover, instead of taking  $A_0$  as our approximating set, we can just take  $A'$ , since  $A \subset q^{-1}(A') \subset q^{-1}(A_0)$ .  $\square$

*Proof of Lemma 3.13.* By the same argument as in the proof of Lemma 3.15 applied to the sets  $A$  and  $A + B$ , we find polynomials  $P_1$  and  $P_2$  that yield the approximations for  $A$  and  $A + B$  respectively. Then, to define  $\widehat{G}_0$ , instead of the spectrum of  $P$  as in the previous proof, now we take  $\widehat{G}_0$  to be the subgroup generated by the union of the spectra of  $P_1$  and  $P_2$ , that is  $\{\gamma \in \widehat{G} : \widehat{P}_i(\gamma) \neq 0 \text{ for } i = 1 \text{ or } 2\}$ . This is again a finite set, so  $G_0$  is finitely generated as required. We then obtain the desired approximation simultaneously for  $A$  and  $A+B$ , namely that  $\mu((q^{-1}q(A)) \setminus A)$  and  $\mu((q^{-1}q(A+B)) \setminus (A+B))$  are both less than  $\delta$ . Then letting  $A' =$

$q(A)$  and  $B' = q(B)$  and using that  $q$  commutes with addition, the result follows.  $\square$

We can now obtain the claimed special case of Theorem 3.3.

*Proof of Theorem 3.3 for closed sets.* Let  $A, B$  be closed sets in the compact abelian group  $G$  such that  $0 < \mu(A + B) \leq \alpha \mu(A)$ ; in particular  $\mu(A) > 0$ . Fix an arbitrary small  $\delta > 0$ , and apply Lemma 3.13 to obtain the corresponding approximating sets  $A', B' \subset G_0$ . Then we have

$$0 < \mu(A + B) \leq \mu(q^{-1}(A') + q^{-1}(B')) = \mu(q^{-1}(A' + B')) < \mu(A + B) + \delta,$$

and  $\mu(A + B) \leq \alpha \mu(A) \leq \alpha \mu(q^{-1}(A'))$ . Letting  $\mu_0$  denote the Haar measure on  $G_0$ , by the basic fact that the continuous surjective homomorphism  $q$  preserves the Haar measures (i.e.  $\mu \circ q^{-1} = \mu_0$ ), we have

$$0 < \mu_0(A' + B') \leq \left( \alpha + \frac{\delta}{\mu(A)} \right) \mu_0(A'),$$

where in the last inequality we used that  $\mu_0(A') \geq \mu(A)$ .

Applying Theorem 3.5, we obtain  $\mu_0(mB' - nB')$  is less or equal than  $(\alpha + \delta/\mu(A))^{m+n} \mu_0(A')$ , which implies that  $\mu(q^{-1}(mB' - nB')) \leq (\alpha + \delta/\mu(A))^{m+n} \mu(q^{-1}(A'))$ . By Lemma 3.13 and the fact that  $mB - nB \subset q^{-1}(mB' - nB')$  we conclude that

$$\mu(mB - nB) \leq (\alpha + \delta/\mu(A))^{m+n} (\mu(A) + \delta).$$

Letting  $\delta \rightarrow 0$ , the result follows.  $\square$

A similar argument yields the following extension of Corollary 3.10.

**Corollary 3.16.** *Let  $A, B$  be closed subsets of a connected compact abelian group satisfying  $0 < \mu(A + B) \leq \alpha \mu(A)$ . Then for every  $m \in \mathbb{N}$  such that  $\alpha^m < 1/\mu(A)$ , we have*

$$\mu(mB) \leq (\alpha^m - 1)\mu(A).$$

*Proof.* We take  $\delta > 0$  so small that  $\delta < \mu(A)$  and  $(\alpha + \delta/\mu(A))^m < 1/(\mu(A) + \delta)$ . We can then argue as in the last proof, using the additional fact that the group  $G_0$ , being here a *connected* compact abelian Lie group (by continuity of  $q$  and connectedness of  $G$ ), must be a torus  $\mathbb{T}^d$ , so that we can apply Corollary 3.10.  $\square$

### 3.4 Extension to $K$ -analytic sets

The classical definition of analytic sets, originating in work of Lusin and Souslin from 1917 [60, 85], essentially concerned the type of spaces now known as Polish spaces. Let us recall the classical definition in this setting (see [24]): a subset  $A$  of a Polish space  $X$  is said to be an *analytic set* if there is a Polish space  $Y$  and a continuous function  $f : Y \rightarrow X$  such that  $f(Y) = A$ .

In the more general setting of Hausdorff spaces, as we recalled in the introduction, Choquet gave a fruitful definition of analytic sets that extends the classical one. For convenience we recall this definition here, but in a slightly different form due to Sion, see Definition 2.1 in [84]. In Hausdorff spaces, the definitions of Choquet and Sion are in fact equivalent, as was shown by Jayne in [52]. Recall that a subset  $B$  of a topological space  $X$  is a  $K_{\sigma\delta}$  set if we have  $B = \bigcap_{i \in \mathbb{N}} \bigcup_{j \in \mathbb{N}} K_{i,j}$ , for compact sets  $K_{i,j} \subset X$ .

**Definition 3.17** ( $K$ -analytic set). Let  $X$  be a Hausdorff space. A set  $A \subset X$  is a  $K$ -analytic set if there is a  $K_{\sigma\delta}$  set  $B$  in a Hausdorff space and a continuous map  $f : B \rightarrow X$  such that  $A = f(B)$ .

The reference [73] provides a detailed introduction to analytic sets, including historical background on the evolution of this notion.

In this section we extend the main result of the previous section to all  $K$ -analytic sets in a compact abelian group, thus completing the proof of Theorem 3.3. Before we do so, let us briefly illustrate some consequences of this extension.

When  $X$  is a Polish space, Definitions 3.2 and 3.17 are equivalent to the classical definition of analytic sets. Indeed, it is a basic fact that analytic sets in Polish spaces are continuous images of the set  $\mathcal{I} = (0, 1) \setminus \mathbb{Q}$  (see Proposition 8.2.7 and Example 6, p. 255 in [24]), and it is not hard to see that  $\mathcal{I}$  is a  $K_{\sigma\delta}$  set. As mentioned in the introduction, we also have that in a Polish space all Borel sets are analytic (see Proposition 8.2.3 in [24]). The extension of the Plünnecke-Ruzsa inequality that we obtain in this section thus applies in particular to all Borel sets in any Polish compact abelian group. The family of Polish compact abelian groups contains every metrizable compact abelian group, see Corollary D.40 in [24] (this includes for instance the Lie groups from Section 3.2, but also more general groups, for example  $\mathbb{T}^{\mathbb{N}}$ ).

We now turn to the proof of Theorem 3.3. Note first that it follows in a straightforward way from the distributivity of Cartesian products across unions and intersections that the Cartesian product of two  $K$ -analytic sets is  $K$ -analytic. From this it then follows, by continuity of addition, that if  $A, B$  are  $K$ -analytic sets in  $G$  then so is  $A + B$ .

To complete the proof of the theorem, we shall use the following measure-theoretic property of  $K$ -analytic sets, which is a small modification (and follows from the proof) of Theorem 4.2 in [84].

**Theorem 3.18.** *Let  $X$  be a Hausdorff space, let  $A_0$  be a  $K_{\sigma\delta}$  set in some Hausdorff space, let  $f : A_0 \rightarrow X$  be a continuous map, let  $A$  be the  $K$ -analytic set  $f(A_0)$  in  $X$ , and let  $\mu$  be an outer measure on  $X$ . Then for every  $\delta > 0$  there is a compact set  $C \subset A_0$  such that  $\mu(f(C)) > \mu(A) - \delta$ .*

The standard definition of an outer measure (or Carathéodory measure) can be recalled from the same paper; see Definition 4.1 in [84]. We shall use the fact that the Haar measure  $\mu$  on a compact abelian group is a restriction of an outer measure (namely the outer Haar measure) to the Haar-measurable sets, and the fact that  $K$ -analytic subsets of  $G$  are Haar measurable (which follows from Theorem 4.3 of [84]). With these facts we can prove the following lemma, which plays a key role in the proof of Theorem 3.3.

**Lemma 3.19.** *Let  $G$  be a compact abelian group, and let  $B$  be a  $K$ -analytic subset of  $G$ . Then for all non-negative integers  $m, n$  we have*

$$\mu(mB - nB) = \sup_{D \subset B, D \text{ compact}} \mu(mD - nD). \quad (3.5)$$

*Proof.* The left side of (3.5) is at least the right side since, on one hand, by the Haar measure's inner regularity we have  $\mu(mB - nB)$  equal to  $\sup_{C \subset mB - nB, C \text{ compact}} \mu(C)$ , and on the other hand for every compact set  $D \subset B$  the set  $C = mD - nD$  is a compact subset of  $mB - nB$ .

To see that the left side of (3.5) is at most the right side, note that since  $B^{m+n}$  is  $K$ -analytic there is a  $K_{\sigma\delta}$  set  $T$  in some Hausdorff space and a continuous function  $f : T \rightarrow G^{m+n}$  such that  $B^{m+n} = f(T)$ . Let  $\pm$  denote the continuous function  $G^{m+n} \rightarrow G$ ,  $(x_1, \dots, x_{m+n}) \mapsto x_1 + \dots + x_m - x_{m+1} - \dots - x_{m+n}$ . Fix any  $\delta > 0$ , and note that by Theorem 3.18 there exists a compact set  $C \subset T$  such that  $\mu(\pm(f(T))) - \delta < \mu(\pm(f(C)))$ .

Let  $D$  be the compact set  $\pi_1(f(C)) \cup \cdots \cup \pi_{m+n}(f(C))$ , where  $\pi_i : G^{m+n} \rightarrow G$  is the projection to the  $i$ -th component. Since  $f(C) \subset B^{m+n}$ , it is clear that  $D \subset B$ . Moreover, we also have

$$\begin{aligned} \pm(f(C)) &\subset \pi_1(f(C)) + \cdots + \pi_m(f(C)) - \pi_{m+1}(f(C)) - \cdots - \pi_{m+n}(f(C)) \\ &\subset mD - nD. \end{aligned}$$

Hence  $\mu(mB - nB) - \delta = \mu(\pm(f(T))) - \delta < \mu(mD - nD)$ . Since  $\delta$  was arbitrary, the desired inequality follows, and the proof is complete.  $\square$

With these ingredients, we can now obtain our main result.

*Proof of Theorem 3.3.* We assume that  $A, B$  are  $K$ -analytic subsets of  $G$  that satisfy  $0 < \mu(A + B) \leq \alpha \mu(A)$ , so in particular  $\mu(A) > 0$ . Fix an arbitrary  $\delta \in (0, \mu(A))$ .

By Theorem 3.18 there exists a compact set  $E \subset A$  such that  $\mu(E) > \mu(A) - \delta > 0$ , and by Lemma 3.19 there exists a compact set  $D \subset B$  such that  $\mu(mD - nD) > \mu(mB - nB) - \delta$ . We then have

$$0 < \mu(E + D) \leq \mu(A + B) \leq \alpha \mu(A) \leq \alpha(\mu(E) + \delta) \leq \alpha\left(1 + \frac{\delta}{\mu(A) - \delta}\right)\mu(E).$$

For subsets of the compact Hausdorff space  $G$  the closure property is equivalent to compactness, so we can apply to  $D, E$  the case of Theorem 3.3 for closed sets, obtaining

$$\mu(mB - nB) - \delta \leq \mu(mD - nD) \leq \alpha^{m+n} \left(1 + \frac{\delta}{\mu(A) - \delta}\right)^{m+n} \mu(E).$$

Letting  $\delta \rightarrow 0$  and using that  $E \subset A$ , we deduce that  $\mu(mB - nB) \leq \alpha^{m+n} \mu(A)$ .  $\square$

Theorem 3.4 can be obtained with a similar argument, replacing the use of Theorem 3.3 for closed sets by that of Corollary 3.16.

## 3.5 On further extensions of the main result

In this last section we discuss further generalizations of Theorem 3.3. In particular, in Subsection 3.5.1 we prove a version of the theorem that allows the Haar measure of one of the two sets to be replaced by the inner Haar measure, thus allowing this set to be arbitrary. Then, in Subsection 3.5.2 we stick to using only the Haar measure and we discuss the problem of extending Theorem 3.3 to more general families of Haar measurable sets.

### 3.5.1 Generalizing Theorem 3.3 using extensions of the Haar measure

Theorem 3.3 yields the following more general version easily.

**Theorem 3.20.** *Let  $G$  be a compact abelian group, with Haar measure  $\mu$  and inner Haar measure  $\mu_*$ . Let  $A$  be any subset of  $G$ , let  $B$  a  $K$ -analytic subset of  $G$ , and suppose that  $0 < \mu_*(A + B) \leq \alpha \mu_*(A)$ . Then for all non-negative integers  $m, n$  we have*

$$\mu(mB - nB) \leq \alpha^{m+n} \mu_*(A).$$

To prove this, first we note that Theorem 3.3 can be rephrased as follows.

**Theorem 3.21.** *Let  $G$  be a compact abelian group, let  $A, B$  be  $K$ -analytic subsets of  $G$ , with  $\mu(A) > 0$  and  $B \neq \emptyset$ . Then  $\mu(mB - nB) \mu(A)^{n+m-1} \leq \mu(A + B)^{n+m}$  for all non-negative integers  $m, n$ .*

The assumption  $\mu(A) > 0$  and  $B \neq \emptyset$  here is indeed equivalent to  $0 < \mu(A + B) \leq \alpha \mu(A)$ , where we can always take the optimal constant, i.e.  $\alpha = \frac{\mu(A+B)}{\mu(A)}$ .

*Proof of Theorem 3.20.* The assumption  $0 < \mu_*(A + B) \leq \alpha \mu_*(A)$  implies that  $\mu_*(A) > 0$ . We then have  $\frac{\mu_*(A+B)}{\mu_*(A)} \leq \alpha$ , and so it suffices to prove that for all  $m, n \geq 0$  we have

$$\mu(mB - nB) \mu_*(A)^{m+n-1} \leq \mu_*(A + B)^{m+n}. \quad (3.6)$$

Let  $E, F$  be compact subsets of  $A, B$  respectively, with  $\mu(E) > 0$  and  $F \neq \emptyset$ . Then, by Theorem 3.21 we have  $\mu(mF - nF) \mu(E)^{n+m-1} \leq \mu(E + F)^{n+m}$ . Taking the supremum of both sides of this inequality over compact sets  $E \subset A$  and  $F \subset B$ , we have

$$\begin{aligned} \sup_{F \subset B, F \text{ compact}} \mu(mF - nF) & \sup_{E \subset A, E \text{ compact}} \mu(E)^{m+n-1} \\ & \leq \sup_{\substack{E \subset A, E \text{ compact} \\ F \subset B, F \text{ compact}}} \mu(E + F)^{m+n}. \end{aligned}$$

As  $E + F$  is a compact subset of  $A + B$ , the right side here is at most  $\mu_*(A + B)^{m+n}$ . We also have  $\sup_{E \subset A, E \text{ compact}} \mu(E)^{m+n-1} = \mu_*(A)^{m+n-1}$ . Hence

$$\sup_{F \subset B, F \text{ compact}} \mu(mF - nF) \mu_*(A)^{m+n-1} \leq \mu_*(A + B)^{m+n}.$$

Since  $B$  is  $K$ -analytic, applying (3.5) we have  $\sup_{F \subset B, F \text{ compact}} \mu(mF - nF) = \mu(mB - nB)$ . This proves (3.6), and the result follows.  $\square$

We do not know whether an even more general version of Theorem 3.20 holds in which both sets  $A, B$  can be arbitrary. One difficulty is that to complete the above proof we relied on the property of  $K$ -analytic sets given in (3.5), and we are not able to use such a property for more general sets. More precisely, to prove a more general version of Theorem 3.20 in which  $B$  could also be arbitrary, it would be helpful to have an analogue of equality (3.5) of the following kind holding for *any* subset  $B \subset G$ :

$$\sup_{F \subset B, F \text{ compact}} \mu(mF - nF) = \mu_*(mB - nB). \quad (3.7)$$

However, this equality can fail. Indeed, we shall discuss a counterexample below that can be constructed using Bernstein sets. Bernstein sets in  $\mathbb{R}$  are classical examples of non-measurable sets. Let us recall the definition of these sets in a Polish space.

**Definition 3.22.** A subset  $B$  of a Polish space  $X$  is a *Bernstein set* if for every uncountable closed set  $C \subset X$  we have  $C \cap B \neq \emptyset$  and  $C \setminus B \neq \emptyset$ .

Recall that a subset of a topological space is *perfect* if it is closed and contains no isolated point. An equivalent definition of Bernstein sets in a Polish space  $X$  is that  $B$  is a Bernstein set in  $X$  if it meets every nonempty perfect subset of  $X$  but contains none of them (the equivalence can be seen using Corollary 6.3 and Theorem 6.4 of [54]).

**Proposition 3.23.** *There exists a set  $B \subset \mathbb{T}$  for which equality (3.7) fails for all  $m, n \in \mathbb{N}$ .*

*Proof.* We can take  $B$  to be a certain Bernstein subset of  $\mathbb{T}$  that can be found using methods from [58]. The paper [58] provides constructions of Bernstein subsets of  $\mathbb{R}$  with additional algebraic properties. Using Method 3.2 and Application 3.3 from [58], we can construct a Bernstein subset  $B \subset \mathbb{R}$  such

that  $B - B = \mathbb{R}$ , and such that  $B + \mathbb{Z} = B$  (for the latter property, which is not included in [58] explicitly, we can first ensure that  $1 \in B$ , and since  $B$  is a subgroup we obtain the desired property; we omit the details). Thus, we obtain a Bernstein set  $B \subset \mathbb{T}$  with the property that  $B - B = \mathbb{T}$ . For this set we then have that (3.7) fails for all  $m, n \in \mathbb{N}$ . Indeed, we have on one hand  $\mu_*(mB - nB) = \sup_{F \subset mB - nB, F \text{ compact}} \mu(F) = 1$ , since  $mB - nB \supset B - B = \mathbb{T}$ , yet on the other hand  $\sup_{F \subset B, F \text{ compact}} \mu(mF - nF) = 0$ , since any such  $F \subset B$  must be countable, so that  $mF - nF$  is also countable and hence  $\mu(mF - nF) = 0$ .  $\square$

Using Bernstein sets we can actually rule out at least one candidate of a version of Theorem 3.3 for arbitrary sets  $A, B$ , namely the version with assumption  $0 < \mu^*(A + B) \leq \alpha \mu^*(A)$  and conclusion  $\mu_*(mB - nB) \leq \alpha^{m+n} \mu_*(A)$  for all  $m, n \in \mathbb{Z}_{\geq 0}$ . Indeed, we have the following example.

**Proposition 3.24.** *There exist subsets  $A, B \subset \mathbb{T}$  such that  $A + B$  is Haar measurable and satisfies  $0 < \mu(A + B) \leq \alpha \mu^*(A)$ , and yet for all positive integers  $m, n$  the set  $mB - nB$  is Haar measurable and satisfies  $\mu(mB - nB) > \alpha^{m+n} \mu_*(A)$ .*

*Proof.* Let  $B \subset \mathbb{T}$  be the Bernstein set that we constructed above, satisfying  $B - B = \mathbb{T}$ , let  $I = (-\frac{\varepsilon}{2}, \frac{\varepsilon}{2}) \subset [-\frac{1}{2}, \frac{1}{2}) = \mathbb{T}$  for some  $\varepsilon < 1$ , and let  $A = B \cup I$ . Since  $B$  is dense in  $\mathbb{T}$ , we have  $A + B \supset I + B = \mathbb{T}$ , hence  $\mu(A + B) = 1$ . We also have  $\mu^*(A) \geq \mu^*(B) = 1$ , so  $\mu(A + B) \leq \alpha \mu^*(A)$  with  $\alpha = 1$ . However, for  $m, n \geq 1$  we have  $mB - nB \supset B - B = \mathbb{T}$ , so  $\mu(mB - nB) = 1$ , and since  $\mu_*(A) = \varepsilon < 1$ , we have  $\mu(mB - nB) > \alpha^{m+n} \mu_*(A)$ .  $\square$

### 3.5.2 On extending Theorem 3.3 to larger families of Haar measurable sets

As mentioned in the introduction, for non-Polish compact abelian groups one could desire a more general version of Theorem 3.3, in particular because of the issue that the family of  $K$ -analytic sets does not necessarily contain all Borel subsets of such a group (see §5 in [43]). There are more recent, more general notions of analytic sets that do include all Borel sets in this setting. A notable example is the family of Čech-analytic sets.

**Definition 3.25.** Let  $X$  be a compact Hausdorff topological space. A set  $A$  in  $X$  is a *Čech-analytic set* if  $A$  is the projection on  $X$  of a set in  $X \times \mathbb{N}^{\mathbb{N}}$  that is the intersection of a closed set with a  $G_{\delta}$ -set.

This notion was introduced by Fremlin in the unpublished note [28] (see also the appendix in [53]). The family of Čech-analytic subsets of a compact Hausdorff space contains all Borel subsets of this space, as shown in Theorem 4 (c) of [28].

There is an even more general notion, namely that of a *scattered- $K$ -analytic set*. We shall mention this notion again below but we shall not recall its much more technical definition here (for more information on this notion we refer to [43, 45, 46]).

The families of Čech-analytic and scattered- $K$ -analytic sets address several shortcomings, while conserving several main advantages, of the family of  $K$ -analytic sets in descriptive topology; this is discussed in Sections 5 and 6 of [73]. It may therefore seem natural to wonder whether Theorem 3.3 holds for these families of sets. However, there is a property of  $K$ -analytic sets that fails for these more general families, namely the stability under addition in a compact abelian group. Because of this failure, we were unable to adapt the methods in this chapter to extend Theorem 3.3 to these families.

The main aim of this subsection is to illustrate this failure of stability under addition with an example, which was shown to us by Petr Holický, and which we present below with his kind permission.

Recall that a subset  $A$  of a topological space is *isolated* if  $A$  together with its relative topology is a discrete space (equivalently, the set contains no limit-point of itself).

**Proposition 3.26** (P. Holický). *There exists a compact abelian group  $G$  and Čech-analytic sets  $A, B \subset G$  such that  $A + B$  is not Čech-analytic.*

*Proof.* Let  $G = \mathbb{T}^{\mathbb{R}} = \{f : \mathbb{R} \rightarrow \mathbb{T}\}$  equipped with pointwise addition. The pointwise topology on  $G$  is compact (it is equivalent to the product topology and compactness follows from Tychonoff's theorem). Thus  $G$  is a compact abelian group.

Let  $\{x_r : r \in \mathbb{R} \setminus \{0\}\}$  be a non-analytic set in the Polish compact space

$\mathbb{T}$ . Viewing  $\mathbb{T}$  as  $[-\frac{1}{2}, \frac{1}{2})$  with addition mod 1, we define

$$\begin{aligned} A &= \{f_r \in G : r \in \mathbb{R} \setminus \{0\}, f_r(r) = \frac{1}{4}, f_r(s) = 0 \text{ for } s \neq r\}, \\ B &= \{g_r \in G : r \in \mathbb{R} \setminus \{0\}, g_r(0) = x_r, g_r(r) = -\frac{1}{4}, g_r(s) = 0 \text{ for } s \neq 0, r\}. \end{aligned} \quad (3.8)$$

In these definitions we are taking for each real number  $r \in \mathbb{R} \setminus \{0\}$  an element of  $G$ . For example in the case of  $A$ , the function  $f_r(s) \in G$  takes the value  $1/4$  when  $s = r$  and 0 otherwise.

We claim that  $A$  and  $B$  are both Čech-analytic subsets of  $G$ . To see this, recall that the compact Hausdorff space  $G$  is completely regular, and that complete regularity is a hereditary property. It then follows from Theorem 6.14 (c) of [43] that a subset of  $G$  is Čech-analytic if it is *isolated- $K$ -analytic* (in the sense of Definition 6.7 in [43]), so it suffices to show that  $A$  and  $B$  are both isolated- $K$ -analytic. It can be seen that  $A$  is isolated- $K$ -analytic by noting that  $A = \bigcup_{r \in \mathbb{R} \setminus \{0\}} \{f_r\}$ , that each singleton  $\{f_r\}$  is isolated, and that  $\mathcal{E} = \{\{f_r\} : r \in \mathbb{R} \setminus \{0\}\}$  is an isolated collection (in the sense of Definition 6.1 of [43]); hence, by Theorem 6.13 (b) of [43], the union  $A$  is indeed isolated- $K$ -analytic. Similarly  $B$  is isolated- $K$ -analytic, and our claim is thus proved.

For  $\theta \in \mathbb{T}$  let  $\|\theta\|_{\mathbb{T}}$  denote the absolute value of the representative of  $\theta$  in  $[-\frac{1}{2}, \frac{1}{2})$ . Let

$$U = \{h \in G : \|h(r)\|_{\mathbb{T}} \leq \frac{1}{8} \text{ for } r \neq 0\}.$$

This is a compact subset of  $G$  so it is Čech-analytic (as a Borel set; see Theorem 4 in [28]).

The family of Čech-analytic sets is closed under finite intersections (even countable ones, see Theorem 5.6 in [43]), so if  $A + B$  were Čech-analytic, then  $(A + B) \cap U$  would also be. However, we have  $(A + B) \cap U = \{h \in G : h(0) = x_r \text{ for some } r \neq 0, h(s) = 0 \text{ for } s \neq 0\}$ . Hence  $(A + B) \cap U$  is homeomorphic to a subset of  $\mathbb{T}$  that is not analytic and therefore not Čech-analytic (in the Polish space  $\mathbb{T}$  the classes of analytic and Čech-analytic sets are equal). Hence  $(A + B) \cap U$  is not Čech-analytic, and then neither is  $A + B$ .  $\square$

Proposition 3.26 can be strengthened if we use the terminology of scattered- $K$ -analytic sets. Indeed, the family of scattered- $K$ -analytic sets is larger than the family of Čech-analytic sets and it can be shown that the set

$A + B$  in Proposition 3.26 is not even scattered- $K$ -analytic. The proof is actually almost the same, except that it uses the more technical definitions and properties of scattered- $K$ -analytic sets given in [43, 45, 46].

The extension of Theorem 3.3 mentioned at the beginning of this section, and Proposition 3.26, together lead to the question of what would be a suitable class of Haar measurable sets, larger than the class of  $K$ -analytic sets, for which such an extension can be proved.

**Question 3.27.** *Is there a class  $\mathcal{C}$  of Haar measurable subsets of a general compact abelian group  $G$  such that  $\mathcal{C}$  is stable under addition and  $\mathcal{C}$  contains every Borel subset of  $G$ ?*

If a generalization of Theorem 3.3 going beyond Theorem 3.20 is proved, in which  $A$  and  $B$  can both be arbitrary, then naturally Question 3.27 will be less relevant to the Plünnecke-Ruzsa inequality. However the question seems of interest in itself.

# Chapter 4

## On sets with small sumset and $m$ -sum-free sets in $\mathbb{Z}_p$

The content of this chapter is the result of joint work with Pablo Candela and David J. Grynkiewicz. It is currently being refereed. A short version of this work was published in *Acta Mathematica Universitatis Comenianae*, Volume 88, Issue 3, and presented at EUROCOMB 2019 in August 2019 [12].

### 4.1 Introduction

Given a subset  $A$  of an abelian group  $G$ , we often denote the sumset  $A+A = \{x+y : x, y \in A\}$  by  $2A$ , and we denote the complement  $G \setminus A$  by  $\overline{A}$ .

One of the central topics in additive number theory is the study of the structure of a finite subset  $A$  of an abelian group under the assumption that the sumset  $2A$  is small. In this chapter, we focus on groups  $\mathbb{Z}_p$  of integers modulo a prime  $p$ , and on the regime in which the *doubling constant*  $|2A|/|A|$  is within a small additive constant of the minimum possible value.

To put this in context, let us recall the basic fact that a finite set  $A$  of integers always satisfies  $|2A| \geq 2|A| - 1$  and that this minimum is attained only if  $A$  is an arithmetic progression (see [39, Theorem 3.1]). This description of extremal sets is extended by a result of Freiman, known as the  $3k-4$  Theorem, which tells us that  $A$  is still efficiently covered by an arithmetic progression even when  $|2A|$  is as large as  $3|A| - 4$ .

**Theorem 4.1** (Freiman’s  $3k - 4$  Theorem). *Let  $A \subseteq \mathbb{Z}$  be a finite set satisfying  $|2A| \leq 3|A| - 4$ . Then there is an arithmetic progression  $P \subseteq \mathbb{Z}$  such that  $A \subseteq P$  and  $|P| \leq |2A| - |A| + 1$ .*

For sets  $A$  in  $\mathbb{Z}_p$  with  $2A \neq \mathbb{Z}_p$ , the Cauchy-Davenport Theorem [39, Theorem 6.2] gives the lower bound analogous to the one for  $\mathbb{Z}$  mentioned above, namely  $|2A| \geq 2|A| - 1$ , and the description of extremal sets as arithmetic progressions (when  $|2A| < p - 1$ ) is given by Vosper’s Theorem [39, Theorem 8.1].

It is widely believed that an analogue of Freiman’s  $3k - 4$  Theorem holds for subsets of  $\mathbb{Z}_p$  under some mild additional upper bound on  $|2A|$  (or on  $|A|$ ). More precisely, the following conjecture is believed to be true (see [39, Conjecture 19.2]), describing efficiently not just  $A$ , but also  $2A$ , in terms of progressions.

**Conjecture 4.2.** *Let  $p$  be a prime and let  $A \subset \mathbb{Z}_p$  be a nonempty subset satisfying  $2A \neq \mathbb{Z}_p$  and  $|2A| = 2|A| + r \leq \min\{3|A| - 4, p - r - 3\}$ . Then there exist arithmetic progressions  $P_A, P_{2A} \subseteq \mathbb{Z}_p$  with the same difference such that  $A \subseteq P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subseteq 2A$ , and  $|P_{2A}| \geq 2|A| - 1$ .*

Progress toward this conjecture was initiated by Freiman himself, who proved in [27] that the conclusion concerning  $P_A$  holds provided that  $|2A| \leq 2.4|A| - 3$  and  $|A| < p/35$ . Since then, there has been much work improving Freiman’s result in various ways. For instance, Rødseth showed in [72] that the constraint  $|A| < p/35$  can be weakened to  $|A| < p/10.7$  while maintaining the doubling constant 2.4. In [35], Green and Ruzsa pushed the doubling constant up to 3, at the cost of a stronger constraint  $|A| < p/10^{215}$ . In [81], Serra and Zémor obtained a result with no constraint on  $|A|$  other than the bounds on  $|2A|$  in the conjecture, with the same conclusion concerning  $P_A$ , but at the cost of reducing the doubling constant, namely, assuming that  $|2A| \leq (2 + \alpha)|A|$  with  $\alpha < 0.0001$ . See also [15], where the doubling constant 2.4 in Freiman’s result is improved to 2.48 while keeping the hypothesis on  $|A|$  markedly less constraining than the one from [35]. The book [39] presents various other results towards Conjecture 4.2, in a treatment covering many of the methods from the works mentioned above.

In this chapter, we establish the following new result regarding Conjecture 4.2, which noticeably improves the doubling constant obtained by Serra and Zémor in [81] at the cost of only adding the mild constraint  $|2A| \leq \frac{3}{4}p$ .

**Theorem 4.3.** *Let  $p$  be prime, let  $A \subseteq \mathbb{Z}_p$  be a nonempty subset with  $|2A| = 2|A| + r$ , and let  $\alpha \approx 0.136861$  be the unique real root of the cubic  $4x^3 + 9x^2 + 6x - 1$ . Suppose*

$$|2A| \leq (2 + \alpha)|A| - 3 \quad \text{and} \quad |2A| \leq \frac{3}{4}p.$$

*Then there exist arithmetic progressions  $P_A, P_{2A} \subseteq \mathbb{Z}_p$  with the same difference such that  $A \subseteq P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subseteq 2A$ , and  $|P_{2A}| \geq 2|A| - 1$ .*

Unlike in [81], here we do have a constraint on  $|A|$  in the form of the upper bound  $|2A| \leq \frac{3}{4}p$ . However, this upper bound is still optimal in the following weak sense. The conjectured upper bound on  $|2A|$  (given by Conjecture 4.2) is  $p - r - 3$ . However, in the extremal case where  $r = |A| - 4$  (the largest value of  $r$  allowed in Conjecture 4.2), the conjectured bound implies  $3|A| - 4 = |2A| \leq p - |A| + 1$ , whence  $|A| \leq \frac{p+5}{4}$  and  $|2A| = 3|A| - 4 \leq \frac{3p-1}{4}$ . Thus, the bound  $p - r - 3$  becomes as small as  $\frac{3p-1}{4}$  as we range over all allowed values for  $\alpha$  and  $|A|$ , making  $\frac{3}{4}p$  the optimal bound independent of  $\alpha$  and  $r$ .

We also prove the following variant of Theorem 4.3, which is optimized for sets  $A$  whose density is large but at most  $1/3$ . This optimization is designed for an application concerning  $m$ -sum-free sets, which we discuss below.

**Theorem 4.4.** *Let  $p$  be prime, let  $\eta \in (0, 1)$ , let  $A \subseteq \mathbb{Z}_p$  be a set with  $|A| \geq \eta p > 0$  and  $|2A| = 2|A| + r < p$ , and let*

$$\alpha = -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\eta p \sin(\pi/p) / \sin(\pi\eta/3)}.$$

*Suppose*

$$|2A| \leq (2 + \alpha)|A| - 3 \quad \text{and} \quad |A| \leq \frac{p-r}{3}.$$

*Then there exist arithmetic progressions  $P_A, P_{2A} \subseteq \mathbb{Z}_p$  with the same difference such that  $A \subseteq P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subseteq 2A$ , and  $|P_{2A}| \geq 2|A| - 1$ .*

We apply this result to obtain new upper bounds for the size of  $m$ -sum-free sets in  $\mathbb{Z}_p$ . For a positive integer  $m$ , a subset  $A$  of an abelian group is said to be  $m$ -sum-free if there is no triple  $(x, y, z) \in A^3$  satisfying  $x + y = mz$ .

These sets have been studied in numerous works in arithmetic combinatorics, including various types of abelian group settings [3, 21, 22, 69, 64] (see also [14, Section 3] for an overview of this topic). In  $\mathbb{Z}_p$ , a central goal concerning these sets is to estimate the quantity

$$d_m(\mathbb{Z}_p) = \max \left\{ \frac{|A|}{p} : A \subseteq \mathbb{Z}_p \text{ } m\text{-sum-free} \right\}.$$

This goal splits naturally into two problems of different nature. On the one hand, we have the case  $m = 2$ , which is the only one in which the solutions of the linear equation in question (i.e., 3-term arithmetic progressions) form a translation invariant set. Roth's Theorem [74] tells us that  $d_2(\mathbb{Z}_p) \rightarrow 0$  as  $p \rightarrow \infty$ , and the problem in this case is then the well-known one of determining the optimal bounds for Roth's theorem, i.e., how fast  $d_2(\mathbb{Z}_p)$  vanishes as  $p$  increases (recent developments in this direction include [7, 78]). On the other hand, we have the cases  $m \geq 3$ . For each of these, the above-mentioned translation-invariance fails, and it is known that  $d_m(\mathbb{Z}_p)$  converges, as  $p \rightarrow \infty$  through primes, to a positive constant  $d_m$  which can be modeled on the circle group (see [16]), the problem then being to determine this constant. Our application of Theorem 4.4 makes progress on the latter problem.

Note that, if  $A$  is  $m$ -sum-free, then the *dilate*  $m \cdot A = \{mx : x \in A\} \subseteq \mathbb{Z}_p$  satisfies  $2A \cap m \cdot A = \emptyset$ , whence, if  $m$  and  $p$  are coprime, we have  $|2A| + |m \cdot A| = |2A| + |A| \leq p$ . Combining this with the bound  $|2A| \geq 2|A| - 1$  given by the Cauchy-Davenport Theorem, we deduce the simple bound  $|A| \leq \frac{p+1}{3}$ , which implies in particular that  $d_m \leq 1/3$ . It was noted in [14] that partial versions of Conjecture 4.2 can be used to improve on this bound, provided these versions are applicable to sets of density up to  $1/3$ . The best version available for that purpose in [14] was given by the theorem of Serra and Zémor mentioned above, and this resulted in the first upper bound for  $d_m$  below  $1/3$ , namely  $1/3.0001$  (see [14, Theorem 3.1]). In this chapter, using Theorem 4.4 we obtain the following improvement.

**Theorem 4.5.** *Let  $p \geq 5$  be a prime, let  $m$  be an integer in  $[2, p - 2]$ , and let  $c = c(p)$  be the solution to the equation*

$$\left( 7 + \sqrt{8cp \sin(\pi/p) / \sin(\pi c/3) + 9} \right) c = 4 + \frac{12}{p}.$$

*Then  $d_m(\mathbb{Z}_p) < c$ . In particular,  $d_m \leq \frac{1}{3.1955}$ .*

Regarding lower bounds for  $d_m(\mathbb{Z}_p)$ , note that, identifying  $\mathbb{Z}_p$  with the integers  $[0, p-1]$ , the interval  $(\frac{2}{m^2-4}p, \frac{m}{m^2-4}p)$  is an  $m$ -sum-free set. This set has asymptotic density  $\frac{1}{m+2}$ , and is still the greatest known example for  $m \leq 7$ . However, for larger values of  $m$ , a construction of Tomasz Schoen (personal communication), presented in this chapter in Lemma 4.11 with his kind permission, yields an improved lower bound of the form  $d_m \geq \frac{1}{8} - o_{m \rightarrow \infty}(1)$ . We summarize these results as follows.

**Theorem 4.6.** *For  $m \leq 7$ , we have  $d_m \geq \frac{1}{m+2}$ . For  $m \geq 8$ , we have  $d_m \geq \frac{1}{2m} \lfloor \frac{m}{4} \rfloor$ .*

The chapter is laid out as follows. In Section 4.2, we prove Theorems 4.3 and 4.4. Our results on  $m$ -sum-free sets are proved in Section 4.3. There, in Subsection 4.3.1, we present Schoen's construction and deduce Theorem 4.6. Then, in Subsection 4.3.2, we apply Theorem 4.4 to obtain Theorem 4.5.

## 4.2 New bounds toward the $3k-4$ conjecture in $\mathbb{Z}_p$

Our first task in this section is to prove Theorem 4.3. We shall obtain this result as the special case  $\varepsilon = 3/4$  of the following theorem.

**Theorem 4.7.** *Let  $p$  be prime, let  $0 < \varepsilon \leq \frac{3}{4}$  be a real number, let  $\alpha$  be the unique positive root of the cubic  $4x^3 + (12 - 4\varepsilon)x^2 + (9 - 4\varepsilon)x + (8\varepsilon - 7)$ , and let  $A \subseteq \mathbb{Z}_p$  be a nonempty subset with  $|2A| = 2|A| + r$ . Suppose*

$$|2A| \leq (2 + \alpha)|A| - 3 \quad \text{and} \quad |2A| \leq \varepsilon p.$$

*Then there exist arithmetic progressions  $P_A, P_{2A} \subseteq \mathbb{Z}_p$  with the same difference such that  $A \subseteq P_A$ ,  $|P_A| \leq |A| + r + 1$ ,  $P_{2A} \subseteq 2A$ , and  $|P_{2A}| \geq 2|A| - 1$ .*

The proof is a modification of the argument used to prove [39, Theorem 19.3], itself based on the original work of Freiman [27] and incorporating improvements to the calculations noted by Rødseth [72]. The main new contribution is an argument to allow the restriction  $|2A| \leq \frac{1}{2}(p+3)$  from [39, Theorem 19.3] to be replaced by the above condition  $|2A| \leq \varepsilon p$ . For  $\varepsilon = 3/4$ , this is optimal in the sense explained in the introduction.

In the proof of Theorem 4.7, we use the following version of the  $3k - 4$  Theorem for  $\mathbb{Z}$ . Here, for  $X \subseteq \mathbb{Z}$ , we denote the greatest common divisor  $\gcd(X - X)$  by  $\gcd^*(X)$ . Note, for  $|X| \geq 2$ , that  $d = \gcd^*(X)$  is the minimal  $d \geq 1$  such that  $X$  is contained in an arithmetic progression with difference  $d$ .

**Theorem 4.8.** *Let  $A, B \subseteq \mathbb{Z}$  be finite, nonempty subsets with  $\gcd^*(A + B) = 1$  and*

$$|A + B| = |A| + |B| + r \leq |A| + |B| + \min\{|A|, |B|\} - 3 - \delta,$$

where  $\delta = 1$  if  $x + A = B$  for some  $x \in \mathbb{Z}$ , and otherwise  $\delta = 0$ . Then there are arithmetic progressions  $P_A, P_B, P_{A+B} \subseteq \mathbb{Z}$  with common difference 1 such that  $A \subseteq P_A, B \subseteq P_B, P_{A+B} \subseteq A + B, |P_A| \leq |A| + r + 1, |P_B| \leq |B| + r + 1$  and  $|P_{A+B}| \geq |A| + |B| - 1$ .

For a prime  $p$ , nonzero  $g \in \mathbb{Z}_p$  (which is then a generator of  $\mathbb{Z}_p$ ), and integers  $m \leq n$ , let

$$[m, n]_g = \{mg, (m + 1)g, \dots, ng\}$$

denote the corresponding interval in  $\mathbb{Z}_p$ . If  $m > n$ , then  $[m, n]_g = \emptyset$ . For  $X \subseteq \mathbb{Z}_p$ , we let  $\ell_g(X)$  denote the length of the shortest arithmetic progression with difference  $g$  which contains  $X$ , and we let  $\overline{X} = (\mathbb{Z}_p) \setminus X$  denote the complement of  $X$  in  $\mathbb{Z}_p$ . We say that a sumset  $A + B \subseteq \mathbb{Z}_p$  *rectifies* if  $\ell_g(A) + \ell_g(B) \leq p + 1$  for some nonzero  $g \in \mathbb{Z}_p$ . In such case,  $A \subseteq a_0 + [0, m]_g$  and  $B \subseteq b_0 + [0, n]_g$  with  $m + n = \ell_g(A) + \ell_g(B) - 2 \leq p - 1$ , for some  $a_0, b_0 \in \mathbb{Z}_p$ , in which case the maps  $a_0 + sg \mapsto s$  and  $b_0 + tg \mapsto t$ , for  $s, t \in \mathbb{Z}$ , when restricted to  $A$  and  $B$  respectively, show that the sumset  $A + B$  is *Freiman isomorphic* (see [39, Section 2.8]) to an integer sumset. This allows us to canonically apply results from  $\mathbb{Z}$  to the sumset  $A + B$ .

If  $G$  is an abelian group and  $A, B \subseteq G$  are subsets, then we say that  $A$  is *saturated* with respect to  $B$  if  $(A \cup \{x\}) + B \neq A + B$  for all  $x \in \overline{A}$ . In the proof of Theorem 4.7, we shall also use the following basic result regarding saturation [39, Lemma 7.2], whose earlier form dates back to Vosper [89]. We include the short proof for completeness.

**Lemma 4.9.** *Let  $G$  be an abelian group and let  $A, B \subseteq G$  be subsets. Then*

$$-B + \overline{A + B} \subseteq \overline{A}$$

with equality holding if and only if  $A$  is saturated with respect to  $B$ .

*Proof.* First observe that  $-B + \overline{A + B} \subseteq \overline{A}$ , for if  $b \in B$ ,  $z \in \overline{A + B}$  and by contradiction  $-b + z = a$  for some  $a \in A$ , then  $z = a + b \in A + B$ , contrary to its definition. If  $A$  is saturated with respect to  $B$ , then given any  $x \in \overline{A}$ , there exists some  $b \in B$  and  $z \in \overline{A + B}$  with  $x + b = z$ , whence  $x = -b + z \in -B + \overline{A + B}$ . This shows that  $\overline{A} \subseteq -B + \overline{A + B}$ , and as the reverse inclusion always holds (as just shown), it follows that  $\overline{A} = -B + \overline{A + B}$ . Conversely, if  $\overline{A} = -B + \overline{A + B}$ , then given any  $x \in \overline{A}$ , there exists some  $b \in B$  and  $z \in \overline{A + B}$  with  $x = -b + z$ , implying  $x + b = z \notin A + B$ . Since  $x \in \overline{A}$  is arbitrary, this shows that  $A$  is saturated with respect to  $B$ .  $\square$

*Proof of Theorem 4.7.* Let  $f(x) = 4x^3 + (12 - 4\varepsilon)x^2 + (9 - 4\varepsilon)x + (8\varepsilon - 7)$ , so that  $f'(x) = 12x^2 + (24 - 8\varepsilon)x + (9 - 4\varepsilon)$ . Then  $f'(x) > 0$  for  $x \geq 0$  (in view of  $\varepsilon \leq 3/4$ ), meaning  $f(x)$  is an increasing function for  $x \geq 0$  with  $f(0) = 8\varepsilon - 7 < 0$  and  $f(1/2) = 1 + 5\varepsilon > 0$ . Consequently,  $f(x)$  has a unique positive root  $0 < \alpha < \frac{1}{2}$ .

Since  $|2A| \leq \varepsilon p < p$ , the Cauchy-Davenport Theorem implies  $r \geq -1$ . Let

$$\beta = \frac{r + 3}{|A|} > 0, \quad (4.1)$$

so that

$$r = \beta|A| - 3, \quad |2A| = 2|A| + r = (2 + \beta)|A| - 3 \quad \text{and} \quad \beta \leq \alpha < \frac{1}{2}. \quad (4.2)$$

Since  $2|A| + r = |2A| \leq \varepsilon p \leq \frac{3}{4}p$ , it follows that  $|A| \leq \frac{3}{8}p - \frac{1}{2}r = \frac{3}{8}p - \frac{1}{2}\beta|A| + \frac{3}{2}$ , which implies (in view of  $\beta > 0$ ) that

$$|A| \leq \frac{3p + 12}{4(2 + \beta)} < \frac{3p + 12}{8}. \quad (4.3)$$

The proof naturally breaks into two parts: a first case where there is a large rectifiable sub-sumset, and a second case where there is not.

**Case 1:** Suppose there exist subsets  $A' \subseteq A$  and  $B' \subseteq A$  with  $|B'| \leq |A'|$  and

$$|A'| + 2|B'| - 4 \geq |2A| \quad (4.4)$$

such that  $A' + B'$  is rectifiable. Furthermore, choose a pair of subsets  $A' \subseteq A$  and  $B' \subseteq A$  with these properties such that  $|A'| + |B'|$  is maximal, and for these subsets  $A'$  and  $B'$ , let  $g \in \mathbb{Z}_p$  be a nonzero difference with  $\ell_g(A') +$

$\ell_g(B') \leq p + 1$  minimal. Note  $|A'| \geq |B'| \geq 2$ ; indeed, if  $|B'| \leq 1$ , then combining this with the hypotheses  $|B'| \leq |A'| \leq |A|$  and (4.4) yields the contradiction  $|A| - 2 \geq |2A| \geq |A|$ . Since  $A' + B'$  rectifies, the Cauchy-Davenport Theorem for  $\mathbb{Z}$  [39, Theorem 3.1] ensures

$$|A' + B'| = |A'| + |B'| + r' \text{ with } r' \geq -1.$$

Moreover, we have

$$\begin{aligned} A' \subseteq P_A := a_0 + [0, m]_g, \quad B' \subseteq P_B := b_0 + [0, n]_g \\ \text{and } A' + B' \subseteq a_0 + b_0 + [0, m + n]_g \end{aligned} \quad (4.5)$$

with  $a_0, a_0 + mg \in A'$ ,  $b_0, b_0 + ng \in B'$  and  $m + n \leq p - 1$ , for some  $a_0, b_0 \in \mathbb{Z}_p$ . Then, since  $A' + B'$  rectifies, it follows that the map  $\psi : \mathbb{Z}_p \rightarrow [0, p - 1] \subseteq \mathbb{Z}$  defined by  $\psi(sg) = s$  for  $s \in [0, p - 1]$ , gives a Freiman isomorphism of  $A' + B'$  with the integer sumset  $\psi(-a_0 + A') + \psi(-b_0 + B') \subseteq \mathbb{Z}$ . Observe that

$$\gcd^*(\psi(-a_0 + A') + \psi(-b_0 + B')) = 1,$$

since if  $\psi(-a_0 + A') + \psi(-b_0 + B')$  were contained in an arithmetic progression with difference  $d \geq 2$ , then this would also be the case for  $\psi(-a_0 + A')$  and  $\psi(-b_0 + B')$ , and then  $\ell_{dg}(A') + \ell_{dg}(B') < \ell_g(A') + \ell_g(B')$  would follow in view of  $|A'| \geq |B'| \geq 2$ , contradicting the minimality of  $\ell_g(A') + \ell_g(B')$  for  $g$ .

In view of (4.4) and  $|B'| \leq |A'|$ , we have  $|A' + B'| \leq |2A| \leq |A'| + |B'| + \min\{|A'|, |B'|\} - 4$ . Thus, since  $\gcd^*(\psi(-a_0 + A') + \psi(-b_0 + B')) = 1$ , we can apply the  $3k - 4$  Theorem (Theorem 4.8) to the isomorphic sumset  $\psi(-a_0 + A') + \psi(-b_0 + B')$ . Then, letting  $P_A = a_0 + [0, m]_g$ ,  $P_B = b_0 + [0, n]_g$  and  $P_{A+B} \subseteq A' + B'$  be the resulting arithmetic progressions with common difference  $g$ , we conclude that

$$|P_A \setminus A'| \leq r' + 1 \quad \text{and} \quad |P_B \setminus B'| \leq r' + 1. \quad (4.6)$$

If  $A' = A$  and  $B' = A$ , then the original sumset  $2A$  rectifies, we have  $r' = r$ , and the theorem follows with  $P_A = P_B$  and  $P_{2A} = P_{A+B}$  as just defined. Therefore we can assume otherwise, which in view of  $|B'| \leq |A'|$  means

$$A \setminus B' \neq \emptyset. \quad (4.7)$$

Let  $\Delta = |2A| - |A' + B'| \geq 0$ . Then

$$r' = |A \setminus A'| + |A \setminus B'| + r - \Delta. \quad (4.8)$$

Since  $|A'| + |B'| + r' = |A' + B'| = |2A| - \Delta$ , it follows from (4.4) and  $|B'| \leq |A'|$  that

$$r' \leq |B'| - 4 - \Delta \quad \text{and} \quad r' \leq |A'| - 4 - \Delta. \quad (4.9)$$

Averaging both bounds in (4.9) along with the bound (4.8), and recalling that  $|2A| = 2|A| + r$ , we obtain

$$r' \leq \frac{1}{3}|2A| - \frac{8}{3} - \Delta. \quad (4.10)$$

### Step A

$$|-A' + \overline{A' + A}| \leq |\overline{A' + A}| + 2|A'| - 4.$$

*Proof.* If Step A fails, then combining its failure with  $p - |2A| = |\overline{2A}| \leq |\overline{A' + A}|$  and Lemma 4.9 yields

$$p - |2A| + 2|A'| - 3 \leq |\overline{A' + A}| + 2|A'| - 3 \leq |-A' + \overline{A' + A}| \leq |\overline{A}| = p - |A|,$$

which implies that  $|A| + 2|A'| - 3 \leq |2A|$ . This together with (4.4) and  $|B'| \leq |A'| \leq |A|$  implies  $|A| + 2|A'| - 3 \leq |A'| + 2|B'| - 4 \leq |A| + 2|A'| - 4$ , which is not possible.  $\square$

### Step B

$$|-A' + \overline{A' + A}| \leq |A'| + 2|\overline{A' + A}| - 3.$$

*Proof.* If Step B fails, then combining its failure with  $2p - 4|A| - 2r = 2|\overline{2A}| \leq 2|\overline{A' + A}|$  and Lemma 4.9 yields

$$|A'| + 2p - 4|A| - 2r - 2 \leq |A'| + 2|\overline{A' + A}| - 2 \leq |-A' + \overline{A' + A}| \leq |\overline{A}| = p - |A|.$$

Collecting terms in the above inequality, multiplying by 2, and applying the estimates  $|B'| \leq |A'|$  and (4.10) yields

$$\begin{aligned} 2p &\leq 6|A| + 4r - 2|A'| + 4 \leq 3|2A| + r - |A'| - |B'| + 4 \\ &= 3|2A| - |A' + B'| + r + r' + 4 = 2|2A| + \Delta + r + r' + 4 \\ &\leq \frac{7}{3}|2A| + r + \frac{4}{3}. \end{aligned}$$

Hence  $|2A| \geq \frac{6}{7}p - \frac{3}{7}r - \frac{4}{7}$ . Combined with (4.2) and (4.3), we conclude that

$$\frac{6}{7}p - \frac{3}{7}\alpha\left(\frac{3p+12}{8}\right) + \frac{5}{7} < \frac{6}{7}p - \frac{3}{7}\beta|A| + \frac{5}{7} = \frac{6}{7}p - \frac{3}{7}r - \frac{4}{7} \leq |2A| \leq \varepsilon p \leq \frac{3}{4}p,$$

which yields the contradiction  $0 < (\frac{6}{7} - \frac{3}{4} - \frac{9}{56}\alpha)p < \frac{36}{56}\alpha - \frac{5}{7} < 0$  (in view of  $\alpha < \frac{1}{2}$ ), completing Step B.  $\square$

By our application of the  $3k-4$  Theorem (Theorem 4.8) to  $\psi(-a_0 + A') + \psi(-b_0 + B')$ , we know that  $A' + B'$  contains an arithmetic progression  $P_{A+B}$  with difference  $g$  and length  $|P_{A+B}| \geq |A'| + |B'| - 1$ , which implies

$$\ell_g(\overline{A' + B'}) \leq p - |A'| - |B'| + 1.$$

By (4.6) and (4.9), we obtain

$$\ell_g(-A') = \ell_g(A') \leq |A'| + r' + 1 \leq |A'| + |B'| - 3, \quad (4.11)$$

whence  $\ell_g(-A') + \ell_g(\overline{A' + B'}) \leq p - 2$ , ensuring  $-A' + \overline{A' + B'}$  rectifies via the difference  $g$ . Since  $\overline{A' + A} \subseteq \overline{A' + B'}$ , it follows that  $-A' + \overline{A' + A}$  also rectifies via the difference  $g$ .

By our application of the  $3k-4$  Theorem (Theorem 4.8) to  $\psi(-a_0 + A') + \psi(-b_0 + B')$ , we know  $\psi(-a_0 + A')$  is contained in the arithmetic progression  $\psi(-a_0 + P_A) = [0, m]$  with difference 1 and length  $|P_A| \leq |A'| + r' + 1$ , with the latter inequality by (4.6). Moreover,  $r' + 1 \leq |B'| - 3 \leq |A'| - 3$  (by (4.9)), so that  $|A'| > \lceil \frac{1}{2}|P_A| \rceil$ , meaning  $\psi(-a_0 + A')$  must contain at least 2 consecutive elements. Hence

$$\gcd^*(\psi(-a_0 + A')) = 1. \quad (4.12)$$

Since  $-A' + \overline{A' + A}$  rectifies via the difference  $g$ , it is then isomorphic to the integer sumset  $\psi(a_0 + mg - A') + \psi(x + \overline{A' + A})$  for an appropriate  $x \in \mathbb{Z}_p$ . Hence, in view of (4.12), Step A and Step B, we can apply the  $3k-4$  Theorem (Theorem 4.8) to the isomorphic sumset  $\psi(a_0 + mg - A') + \psi(x + \overline{A' + A})$  and thereby conclude that there is an arithmetic progression  $P \subseteq -A' + \overline{A' + A}$  with difference  $g$  and length  $|P| \geq |A'| + |\overline{A' + A}| - 1 \geq |A'| + |2\overline{A}| - 1 = p - |2A| + |A'| - 1$ . Consequently, since Lemma 4.9 ensures that  $P \subseteq -A' + \overline{A' + A} \subseteq \overline{A}$ , it follows that  $\ell_g(A) \leq |2A| - |A'| + 1$ . Combined with (4.11), we find that

$$\ell_g(A') + \ell_g(A) \leq |2A| + r' + 2. \quad (4.13)$$

If  $A' + A$  does not rectify, then (4.13) and (4.10) imply  $p \leq |2A| + r' \leq \frac{4}{3}|2A| - \frac{8}{3}$ , whence  $|2A| \geq \frac{3}{4}p + 2 > \varepsilon p$ , contrary to hypothesis. Therefore  $A' + A$  rectifies. This contradicts the maximality of  $|A'| + |B'|$  since by (4.7) we have  $|A| > |B'|$ , which completes Case 1.

**Case 2:** Every pair of subsets  $A' \subseteq A$  and  $B' \subseteq A$  with  $|B'| \leq |A'|$  whose sumset  $A' + B'$  rectifies has

$$|A'| + 2|B'| \leq |2A| + 3. \quad (4.14)$$

Let  $\ell := |2A| = 2|A| + r$ . For the rest of this proof, let us identify  $\mathbb{Z}_p$  with the set of integers  $[0, p-1]$  with addition mod  $p$ . Then, for every  $X \subseteq \mathbb{Z}_p$  and  $d \in \mathbb{Z}_p$ , we define the exponential sum  $S_X(d) = \sum_{x \in X} e^{\frac{2\pi i}{p} dx} \in \mathbb{C}$ .

The idea is to use Freiman's estimate [59, Theorem 1] for such sums to show that the assumption (4.14) implies

$$|S_A(d)| \leq \frac{1}{3}|A| + \frac{2}{3}r + 2 \quad \text{for all nonzero } d \in \mathbb{Z}_p. \quad (4.15)$$

For any  $u \in [0, 2\pi)$ , consider the open arc  $C_u = \{e^{ix} : x \in (u, u + \pi)\}$  of length  $\pi$  in the unit circle in  $\mathbb{C}$ . Let  $A' = \{x \in A : e^{\frac{2\pi i}{p} dx} \in C_u\}$ . Since the set of  $p$ -th roots of unity contained in  $C_u$  correspond to an arithmetic progression of difference 1 in  $\mathbb{Z}_p$ , it is clear that, for  $d^*$  the multiplicative inverse of  $d$  modulo  $p$ , we have  $\ell_{d^*}(A') \leq \frac{p+1}{2}$ . Hence the sumset  $A' + A'$  rectifies. Then the assumption (4.14) implies that  $3|A'| \leq |2A| + 3$ . This shows that every open half arc of the unit circle contains at most  $n = \frac{1}{3}|2A| + 1$  of the  $|A|$  terms involved in the sum  $S_A(d)$ . By [59, Theorem 1] applied with this  $n$ ,  $N = |A|$ , and  $\varphi = \pi$ , we obtain  $|S_A(d)| \leq 2n - N = \frac{2}{3}|2A| + 2 - |A|$ , and (4.15) follows.

To complete the proof, we now exploit (4.15) to obtain a contradiction, using in particular the following manipulations which are standard in the additive combinatorial use of Fourier analysis (e.g. [39, pp. 290–291])

By Fourier inversion and the fact that  $S_A(0) = |A|$  and  $S_{2A}(0) = \ell$ , we

have

$$\begin{aligned}
|A|^{2p} &= \sum_{x \in \mathbb{Z}_p} S_A(x) S_A(x) \overline{S_{2A}(x)} \\
&= S_A(0) S_A(0) \overline{S_{2A}(0)} + \sum_{x \in (\mathbb{Z}_p) \setminus \{0\}} S_A(x) S_A(x) \overline{S_{2A}(x)} \\
&= |A|^2 \ell + \sum_{x \in (\mathbb{Z}_p) \setminus \{0\}} S_A(x) S_A(x) \overline{S_{2A}(x)} \\
&\leq |A|^2 \ell + \sum_{x \in (\mathbb{Z}_p) \setminus \{0\}} |S_A(x)| |S_A(x)| |S_{2A}(x)| \\
&\leq |A|^2 \ell + \left(\frac{1}{3}|A| + \frac{2}{3}r + 2\right) \sum_{x \in (\mathbb{Z}_p) \setminus \{0\}} |S_A(x)| |S_{2A}(x)|.
\end{aligned}$$

This last sum is at most  $\left(\sum_{x \in (\mathbb{Z}_p) \setminus \{0\}} |S_A(x)|^2\right)^{1/2} \left(\sum_{x \in (\mathbb{Z}_p) \setminus \{0\}} |S_{2A}(x)|^2\right)^{1/2}$  by the Cauchy-Schwarz inequality. We thus conclude that

$$|A|^{2p} \leq |A|^2 \ell + \frac{|A| + 2r + 6}{3} (|A|p - |A|^2)^{1/2} (\ell p - \ell^2)^{1/2}.$$

Rearranging this inequality, we obtain

$$\frac{|A| + 2r + 6}{3|A|} \geq \frac{|A|(p - \ell)}{|A|^{1/2}(p - |A|)^{1/2} \ell^{1/2}(p - \ell)^{1/2}} = \left(\frac{\frac{p}{\ell} - 1}{\frac{p}{|A|} - 1}\right)^{1/2}. \quad (4.16)$$

By hypothesis  $r = \beta|A| - 3$ , and  $\ell = |2A| = (2 + \beta)|A| - 3$ , so  $|A| = \frac{\ell+3}{2+\beta} > \frac{\ell}{2+\beta}$ . Using these estimates in (4.16) yields

$$\begin{aligned}
\frac{1 + 2\beta}{3} &= \frac{|A| + 2(\beta|A| - 3) + 6}{3|A|} = \frac{|A| + 2r + 6}{3|A|} \\
&\geq \left(\frac{\frac{p}{\ell} - 1}{\frac{p}{|A|} - 1}\right)^{1/2} > \left(\frac{\frac{p}{\ell} - 1}{(2 + \beta)\frac{p}{\ell} - 1}\right)^{1/2}.
\end{aligned}$$

Rearranging the above inequality yields (in view of  $0 < \beta \leq \alpha < 1$ )

$$\varepsilon p \geq \ell > \frac{1 - \left(\frac{1+2\beta}{3}\right)^2 (2 + \beta)}{1 - \left(\frac{1+2\beta}{3}\right)^2} p. \quad (4.17)$$

Since  $\beta \leq \alpha < 1$ , rearranging the above inequality yields

$$4\beta^3 + (12 - 4\varepsilon)\beta^2 + (9 - 4\varepsilon)\beta + 8\varepsilon - 7 > 0. \quad (4.18)$$

Thus  $f(\beta) > 0$ , with  $f(x) = 4x^3 + (12 - 4\varepsilon)x^2 + (9 - 4\varepsilon)x + 8\varepsilon - 7$ . As noted at the start of the proof,  $f(x)$  is increasing for  $x \geq 0$  with a unique positive root  $\alpha$ . As a result, (4.18) ensures that  $\beta > \alpha$ , which is contrary to hypothesis, completing the proof.  $\square$

*Remark 4.10.* Our restriction  $|2A| \leq \frac{3}{4}p$  in Theorem 4.7 could be relaxed somewhat further, but at increasingly greater cost to the resulting constant  $\alpha$ . One simply needs to strengthen the hypothesis of (4.4) and appropriately adjust the Fourier analytic calculation in Case 2 in the above proof, using the correspondingly weakened inequality for (4.14).

*Proof of Theorem 4.3.* As mentioned earlier, Theorem 4.3 is just the special case of Theorem 4.7 with  $\varepsilon = \frac{3}{4}$ .  $\square$

We now proceed to prove the variant that we shall apply in the next section.

*Proof of Theorem 4.4.* The proof is very close to that of Theorem 4.7, with the most significant difference occurring in Case 2. We only highlight the few differences in the argument.

First observe that, if  $p = 2$ , then  $|2A| < p$  forces  $|A| = 1$ , in which case the theorem holds trivially. Therefore we can assume  $p \geq 3$ . Next observe (via Taylor series expansion) that  $p \sin(\pi/p)$  is an increasing function for  $p > 1$  with limit  $\pi$ . The function  $\eta / \sin(\pi\eta/3)$  is also an increasing function for  $\eta \in (0, 1)$ . Thus  $\alpha \leq -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\pi/\sin(\pi/3)} < 0.3$ . By hypothesis,  $|A| \leq \frac{p-r}{3} = \frac{1}{3}p - \frac{1}{3}\beta|A| + 1$ , implying

$$|A| \leq \frac{p+3}{\beta+3} < \frac{p+3}{3}, \quad (4.19)$$

which replaces (4.3) for the proof. Also,  $|2A| = 2|A| + r \leq 2(\frac{p-r}{3}) + r = \frac{2p+r}{3}$ .

At the end of Step B in Case 1, we instead obtain  $\frac{6}{7}p - \frac{3}{7}r - \frac{4}{7} \leq |2A| \leq \frac{2p+r}{3}$ , which implies

$$\frac{2}{3}p \geq \frac{6}{7}p - \frac{16}{21}r - \frac{4}{7} \geq \frac{6}{7}p - \frac{16}{21}\alpha|A| + \frac{16}{7} - \frac{4}{7} > \frac{6}{7}p - \frac{16}{21}\alpha\left(\frac{p+3}{3}\right) + \frac{16}{7} - \frac{4}{7},$$

with the final inequality above in view of (4.19). Thus  $0 < (\frac{6}{7} - \frac{2}{3} - \frac{16}{63}\alpha)p < \frac{16}{21}\alpha - \frac{12}{7} < 0$  (in view of  $0 < \alpha < 0.3$ ), which is the contradiction that instead completes Step B.

At the end of Case 1, we instead likewise obtain

$$\frac{3}{4}p + 2 \leq |2A| \leq \frac{2p+r}{3} \leq \frac{2}{3}p + \frac{1}{3}\alpha|A| - 1 < \frac{2}{3}p + \frac{1}{3}\alpha\left(\frac{p+3}{3}\right) - 1.$$

This yields the contradiction  $0 < (\frac{3}{4} - \frac{2}{3} - \frac{\alpha}{9})p < \frac{\alpha}{3} - 3 < 0$  (in view of  $0 < \alpha < 0.3$ ) in order to complete Case 1.

For Case 2, we begin by following the argument that proves (4.15), except that we use Lev's sharper estimate [59, Theorem 2] instead of [59, Theorem 1]. Thus, using that any two distinct terms in  $S_A$  have the shortest arc between them of length at least  $\delta = 2\pi/p$ , we obtain by [59, Theorem 2] applied with  $n = \frac{1}{3}|2A| + 1 \leq p/2$  (so  $\delta n \leq \pi$ ) that, for every such nonzero  $d$ , we have

$$|S_A(d)| \leq \frac{\sin\left(\left(\frac{1}{3}|2A| + 1 - \frac{1}{2}|A|\right)\frac{2\pi}{p}\right)}{\sin\left(\frac{\pi}{p}\right)} = \frac{\sin\left(\left(\frac{1}{3}|A| + \frac{2}{3}r + 2\right)\frac{\pi}{p}\right)}{\sin\left(\frac{\pi}{p}\right)}. \quad (4.20)$$

Let  $M = \frac{1}{3}|A| + \frac{2}{3}r + 2$ , and let  $y = M/p$ . Note  $M \leq (\frac{1}{3} + \frac{2}{3}\alpha)|A| < (\frac{1}{3} + \frac{2}{3}(0.3))\frac{p+3}{3} < \frac{p}{2}$  in view of  $r \leq \alpha|A| - 3$  and (4.19), ensuring  $y \in (\frac{\eta}{3}, \frac{1}{2})$ . Then the inequality in (4.20) becomes  $|S_A(d)| \leq \frac{\sin(y\pi)}{yp \sin(\frac{\pi}{p})} M$ . The function  $f(p, y) = \frac{\sin(y\pi)}{yp \sin(\frac{\pi}{p})}$  is decreasing in  $y \in (0, 1/2)$  for any fixed  $p \geq 3$ , as can be seen by considering the Taylor series expansion of its partial derivative. It is also decreasing in  $p$  for every fixed  $y \in (0, 1/2)$  by a similar analysis. Letting  $\gamma = f(p, \frac{\eta}{3}) > 0$ , we can therefore replace (4.15) by the bound

$$|S_A(d)| \leq \gamma\left(\frac{1}{3}|A| + \frac{2}{3}r + 2\right). \quad (4.21)$$

Since  $M\frac{\pi}{p} < \frac{\pi}{2}$ ,  $M > 1$  and  $p \geq 3$ , it follows that  $\sin(M\frac{\pi}{p}) - M \sin(\frac{\pi}{p}) \leq 0$  (as can be seen by considering derivatives with respect to  $M$  and using the Taylor series expansion of  $\tan(\frac{\pi}{p})$  to note  $\tan(\frac{\pi}{p}) > \frac{\pi}{p}$ ). Consequently, we see that the bound in (4.20) is at most  $M$ , ensuring  $\gamma \leq 1$ . We now obtain the following inequality instead of (4.16):

$$\gamma \frac{1+2\beta}{3} = \frac{\gamma\left(\frac{1}{3}|A| + \frac{2}{3}r + 2\right)}{|A|} \quad (4.22)$$

$$\geq \frac{|A|(p - \ell)}{|A|^{1/2}(p - |A|)^{1/2}\ell^{1/2}(p - \ell)^{1/2}} = \left(\frac{\frac{p}{\ell} - 1}{\frac{p}{|A|} - 1}\right)^{1/2}.$$

A similar rearrangement as the one that yielded (4.17) now leads to

$$\begin{aligned} \frac{2p + \frac{\beta}{3+\beta}(p+3) - 3}{3} &\geq \frac{2p + \beta|A| - 3}{3} = \frac{2p + r}{3} \\ &\geq |2A| > \frac{1 - \gamma^2\left(\frac{1+2\beta}{3}\right)^2(2+\beta)}{1 - \gamma^2\left(\frac{1+2\beta}{3}\right)^2}p, \end{aligned} \quad (4.23)$$

with the first inequality following from (4.19). Since  $0 \leq \beta < 1$  and  $0 < \gamma \leq 1$ , we have  $\frac{\beta}{3+\beta} < 1$  and also  $1 - \gamma^2\left(\frac{1+2\beta}{3}\right)^2 > 0$ , whence (4.23) implies

$$\left(\frac{\beta+2}{\beta+3}\right)\left(1 - \gamma^2\left(\frac{1+2\beta}{3}\right)^2\right) > 1 - \gamma^2\left(\frac{1+2\beta}{3}\right)^2(2+\beta).$$

Multiplying both sides by  $\beta+3 > 0$  and grouping on the left side the terms involving  $\gamma$ , we obtain  $(\beta+2)^2\gamma^2\left(\frac{1+2\beta}{3}\right)^2 > 1$ . Taking square roots and expanding, we deduce  $2\beta^2 + 5\beta + 2 - 3\gamma^{-1} > 0$ . The quadratic formula thus implies that either  $\beta < \frac{-5 - \sqrt{9+24\gamma^{-1}}}{4} < 0$  or  $\beta > \frac{-5 + \sqrt{9+24\gamma^{-1}}}{4} = \alpha$ . Since  $\beta > 0$ , this contradicts the hypothesis  $\beta \leq \alpha$ , completing the proof.  $\square$

### 4.3 Bounds for $m$ -sum-free sets in $\mathbb{Z}_p$

In this section, we give new bounds for the quantity

$$d_m(\mathbb{Z}_p) = \max \left\{ \frac{|A|}{p} : A \subseteq \mathbb{Z}_p \text{ is } m\text{-sum-free} \right\}.$$

In the first subsection below, we present some examples of large  $m$ -sum-free sets, and in Subsection 4.3.2, we apply Theorem 4.4 to give a new upper bound for  $d_m(\mathbb{Z}_p)$ .

#### 4.3.1 Lower bounds for $d_m(\mathbb{Z}_p)$

As mentioned in the introduction, a simple example of a large  $m$ -sum-free

set is the interval  $(\frac{2}{m^2-4}p, \frac{m}{m^2-4}p)$ , having asymptotic density  $\frac{1}{m+2}$  as  $p \rightarrow \infty$ . This gives the largest known example for  $m \leq 7$ , but not for greater values of  $m$ . Indeed, there is the following construction, due to Tomasz Schoen.

**Lemma 4.11** (T. Schoen). *For each integer  $m \geq 3$ , we have  $d_m(\mathbb{Z}_p) \geq \frac{\lfloor m/4 \rfloor}{m} \frac{p-1}{2p}$  for every prime  $p$  of the form  $p = 2mn + 1$ . In particular,*

$$\lim_{\substack{p \rightarrow \infty \\ p \text{ prime}}} d_m(\mathbb{Z}_p) \geq \frac{1}{2m} \lfloor \frac{m}{4} \rfloor.$$

*Proof.* We identify  $\mathbb{Z}_p$  with the interval of integers  $[0, p-1]$  with addition mod  $p$ . Let  $J$  be the interval  $[1, (p-1)/2] = [1, mn]$  in  $\mathbb{Z}_p$ . We construct an  $m$ -sum-free set  $A$  by picking appropriate elements from  $J$ . We need to ensure that  $2A \cap (m \cdot A) = \emptyset$ , and for this it suffices to have  $2A \cap (m \cdot J) = \emptyset$ .

Now  $m \cdot J$  is an arithmetic progression of difference  $m$ . Taking blocks of  $2n$  consecutive terms, we partition  $m \cdot J$  into progressions  $U_1, U_2, \dots, U_s$ ,  $s = \lfloor \frac{m}{2} \rfloor$ , together with a final remainder progression  $U_{s+1}$  of length 0 if  $m$  is even and length  $n$  if  $m$  is odd. More precisely, we have  $U_1 = \{m, 2m, \dots, 2mn\}$ , then  $U_2 = \{m-1, 2m-1, \dots, 2mn-1\}$ , and so on, up to  $U_s = \{m-(s-1), \dots, 2mn-(s-1)\}$ , with  $U_{s+1} = \emptyset$  or  $\{m-s, \dots, mn-s\}$ .

Looking at this modulo  $m$ , we see  $m \cdot J$  is confined to the congruence classes  $0, -1, \dots, -\lfloor \frac{m-1}{2} \rfloor \pmod{m}$ . Therefore, it suffices to ensure that  $2A$  occupies the other congruence classes mod  $m$ . For example, the following set in  $\mathbb{Z}_p$  is  $m$ -sum-free:

$$A = \{x \in J : x \in [1, \lfloor m/4 \rfloor] \pmod{m}\},$$

since  $2A \pmod{m}$  is included in  $[1, \lfloor \frac{m}{2} \rfloor]$  which is the complement of  $[\lceil \frac{m+1}{2} \rceil, m] \pmod{m}$  with  $m \cdot J \subseteq [\lceil \frac{m+1}{2} \rceil, m] \pmod{m}$ . We have  $|A| = n \lfloor m/4 \rfloor = \frac{\lfloor m/4 \rfloor}{m} \frac{p-1}{2}$ , and the result follows as there are an infinite number of primes of the form  $2mn + 1$  for fixed  $m$ .  $\square$

*Remark 4.12.* A noteworthy feature of the lower bound in Lemma 4.11 is that it stabilizes at a value separated from 0 as  $m$  increases (namely the value  $1/8$ ). It is also worth noting that this type of stabilization holds more generally for linear equations over  $\mathbb{Z}_p$ , and that this was already a consequence of previous work of Schoen. More precisely, given an equation  $a_1x_1 + \dots + a_kx_k = 0$  with integer coefficients  $a_i$  satisfying  $a_1 + \dots + a_k \neq 0$ , we may ask whether the maximal density of sets in  $\mathbb{Z}_p$  without solution

to this equation has a positive lower bound depending only on  $k$ . Letting  $d$  denote the maximal density in question, it follows from [82, Theorem 1] that  $d \geq 2^{-k \log(2k^2) - 5}$ , giving a lower bound on  $d$  depending only on  $k$  and not on the particular values of the coefficients  $a_i$ . The point of the lower bound in Lemma 4.11 is thus also the explicit value  $1/8$ , as a step towards determining the *best* bounds for  $d$  in the case of  $m$ -sum-free sets.

### 4.3.2 Upper bound for $d_m(\mathbb{Z}_p)$

In this final part of the chapter, we prove Theorem 4.5, which we restate here for convenience.

**Theorem 4.13.** *Let  $p \geq 5$  be a prime, let  $m$  be an integer in  $[2, p-2]$ , and let  $c = c(p)$  be the solution to the equation  $c = \frac{1+3/p}{3+\alpha(c,p)}$ , where  $\alpha = \alpha(c, p)$  is the parameter in Theorem 4.4 with  $\eta = c$ . Then  $d_m(\mathbb{Z}_p) < c$ . In particular,  $d_m \leq \frac{1}{3.1955}$ .*

The idea of the proof is roughly the following: either an  $m$ -sum-free set  $A$  has doubling constant at least  $2 + \alpha$ , in which case, since  $(m \cdot A) \cap 2A = \emptyset$ , we have  $(3 + \alpha)p = |(m \cdot A)| + |2A| \leq p$  and we are done, or we can apply Theorem 4.4, and thus, working with the two arithmetic progressions provided by the theorem, we reduce the problem essentially to bounding the size that two progressions  $I$  and  $J$  of equal difference can have if the dilate  $m \cdot J$  has small intersection with  $I$ . Let us begin by establishing this result about progressions.

**Lemma 4.14.** *Let  $p \geq 5$  be prime, let  $0 < \alpha \leq 1/5$ , and let  $d \in [2, p-2]$  and  $N$  be natural numbers with  $N \leq \frac{p+1}{3}$ . Let  $I$  and  $J$  be progressions in  $\mathbb{Z}_p$  having the same difference and satisfying  $|I| = 2N - 1$ ,  $|J| = \lfloor (1 + \alpha)N - 2 \rfloor$ , and  $|I \cap (d \cdot J)| \leq \alpha N - 2$ . Then  $N < \frac{p+3}{3+\alpha}$ .*

*Proof.* First note that, without loss of generality, we can assume  $d \leq \frac{p-1}{2}$ , since if the lemma is proved with this assumption, then, given  $d > \frac{p-1}{2}$ , we can multiply by  $-1$  and apply the lemma with the intervals  $-I$  and  $J$ . Let us proceed by contradiction supposing that there exists some  $N$  (along with  $p, d, \alpha, I$  and  $J$ ) such that the hypotheses of the lemma are satisfied but  $N \geq \frac{p+3}{3+\alpha}$ . Note that the supposed properties of  $I$  and  $J$  are conserved if we dilate by the inverse of their difference mod  $p$  and if we translate, replacing

$I$  by  $I + dz$  and  $J$  by  $J + z$ . It follows that, identifying  $\mathbb{Z}_p$  with the integers  $[0, p - 1]$  with addition mod  $p$ , we can assume that  $I = [p - |I|, p - 1]$  and  $J = x + [0, |J| - 1] \pmod p$  for some  $x \in [0, p - 1]$ .

If  $d \cdot x \in [d, p - |I| + d - 1] \pmod p$ , then  $d \cdot (x - 1) \notin I \pmod p$ , ensuring that the interval  $J' = (x - 1) + [0, |J| - 1]$  satisfies the hypotheses with  $|I \cap (d \cdot J')| \leq |I \cap (d \cdot J)|$ . On the other hand, if  $d \cdot x \in [p - |I|, p - 1]$ , then  $d \cdot x$  is an element from the intersection  $I \cap (d \cdot J)$  not contained in  $I \cap (d \cdot J')$ , where  $J' = (x + 1) + [0, |J| - 1]$ , whence the interval  $J' = (x + 1) + [0, |J| - 1]$  satisfies the hypotheses with  $|I \cap (d \cdot J')| \leq |I \cap (d \cdot J)|$ . In either case, by repeatedly shifting the interval  $J$ , we can w.l.o.g assume

$$d \cdot x \in [0, d - 1] \pmod p. \quad (4.24)$$

In view of (4.24), we may partition  $d \cdot J$  into successive progressions  $U_i$  (with difference  $d$ ) for  $i = 1, 2, \dots, s+1$  such that  $U_i = (\min U_i + d\mathbb{Z}) \cap [0, p - 1]$  with  $\min U_i \in [0, d - 1]$  for  $i \in [1, s]$ , and  $U_{s+1}$  is either empty or consists of an initial portion of  $(\min U_{s+1} + d\mathbb{Z}) \cap [0, p - 1]$  with  $\min U_{s+1} \in [0, d - 1]$ . Then

$$|U_i \cap I| \geq \left\lfloor \frac{|I|}{d} \right\rfloor \quad \text{for } i \in [1, s]. \quad (4.25)$$

In view of (4.25), we have

$$\alpha N - 2 \geq |(d \cdot J) \cap I| \geq s \left\lfloor \frac{|I|}{d} \right\rfloor. \quad (4.26)$$

Note first that, since the intersection of  $y + d\mathbb{Z}$  with an interval of length  $p$  has size at most  $\lceil p/d \rceil$ , we have

$$s \geq \left\lfloor \frac{|J|}{\lceil p/d \rceil} \right\rfloor \geq \left\lfloor \frac{|J|d}{p + d - 1} \right\rfloor \geq \frac{|J|d + 1}{p + d - 1} - 1 > \frac{((1 + \alpha)N - 3)d + 1}{p + d - 1} - 1. \quad (4.27)$$

We claim that  $s \geq 1$ . Indeed, otherwise  $|J| \leq |(d \cdot J) \cap I| + |(d \cdot J) \cap [0, p - |I| - 1]| \leq \alpha N - 2 + \lceil \frac{p - |I|}{d} \rceil$ . Using that  $|J| > (1 + \alpha)N - 3$ ,  $|I| = 2N - 1$ ,  $d \geq 2$  and  $p \geq 5$ , we conclude that  $N < \frac{p + 2d}{d + 2} \leq (p + 4)/4$ . Thus  $N \leq \frac{p + 3}{4}$ , which combined with our assumption  $N \geq (p + 3)/(3 + \alpha)$  yields  $(1 - \alpha)(p + 3) \leq 0$ , contradicting that  $\alpha < 1$ , which proves our claim.

Since  $s \geq 1$ , (4.26) yields

$$|(d \cdot J) \cap I| \geq \lfloor |I|/d \rfloor \geq \frac{2N}{d} - 1. \quad (4.28)$$

Using again the hypothesis  $|(d \cdot J) \cap I| \leq \alpha N - 2$ , it follows that  $(\alpha N - 1)d \geq 2N > 0$ . Hence  $\alpha N - 1 > 0$  and  $d \geq \frac{2N}{\alpha N - 1} > \frac{2}{\alpha}$ , whence  $d \geq 11$  follows in view of  $\alpha \leq \frac{1}{5}$ . Thus  $11 \leq d \leq \frac{p-1}{2}$ , implying  $p \geq 23$  and  $N \geq \frac{p+3}{3+\alpha} > 6$  (in view of  $\alpha \leq 1$ ).

Note that  $\lfloor |I|/d \rfloor \geq 1$ , for otherwise  $2N = |I| + 1 < d + 1 \leq \frac{p+1}{2}$ , contradicting our assumptions  $N \geq \frac{p+3}{3+\alpha}$  and  $\alpha \leq 1$ . Combining this with (4.26) and (4.27), we obtain  $\alpha N - 2 > \frac{((1+\alpha)N-3)d+1}{p+d-1} - 1$ , which means  $d \leq \left(\alpha - \frac{1-2\alpha}{N-2}\right)(p-1) < \alpha p$  (in view of  $\alpha \leq \frac{1}{2}$  and  $N \geq 3$ ).

So far we have that, if  $N \geq \frac{p+3}{3+\alpha}$  holds, then  $11 \leq d < \alpha p \leq p/5$ , and therefore

$$p > 55.$$

Also, we have  $\frac{2N}{d} - 1 > 0$ , for otherwise we obtain the contradiction  $\frac{p}{4} \leq \frac{p+3}{3+\alpha} \leq N \leq \frac{d}{2} < \frac{1}{2}\alpha p \leq \frac{p}{10}$ . The final part of the proof is a calculation involving (4.26) which will yield a contradiction. Combining (4.26) with (4.28) and (4.27), we obtain

$$\begin{aligned} \alpha N - 2 &> \left( \frac{((1+\alpha)N-3)d+1}{p+d-1} - 1 \right) \left( \frac{2N}{d} - 1 \right) \\ &= \frac{2d(1+\alpha)}{d(p+d-1)} N^2 - \left( \frac{(1+\alpha)d}{p+d-1} + \frac{6d-2}{d(p+d-1)} + \frac{2}{d} \right) N \\ &\quad + 1 + \frac{3d-1}{p+d-1}. \end{aligned}$$

We group all terms involving  $N$  on the right side, we note that the other terms grouped on the left side amount to a negative number, and we multiply through by  $\frac{p+d-1}{2(1+\alpha)N}$ , to deduce that

$$N < \frac{1}{2(1+\alpha)} \left( (1+2\alpha)d + \left(\frac{2}{d} + \alpha\right)p + 8 - \frac{4}{d} - \alpha \right). \quad (4.29)$$

Using that  $11 \leq d < p/5$  and the assumption  $N \geq \frac{p+3}{3+\alpha}$ , we see that (4.29) implies

$$\frac{p+3}{3+\alpha} < \frac{1}{2(1+\alpha)} \left( (1+2\alpha)\frac{p}{5} + \left(\frac{2}{11} + \alpha\right)p + 8 - \frac{4}{11} - \alpha \right).$$

Grouping terms involving  $p$  to the left side and multiplying through by  $110(1+\alpha)(3+\alpha)$  yields

$$p(47 - 142\alpha - 77\alpha^2) < 930 - 75\alpha - 55\alpha^2.$$

The polynomial in  $\alpha$  on the left side is positive for  $\alpha \in [0, 1/5]$ , whence

$$p \leq \frac{55\alpha^2 + 75\alpha - 930}{77\alpha^2 + 142\alpha - 47},$$

which is a bound increasing for  $\alpha \geq 0$ , thus maximized for  $\alpha = \frac{1}{5}$ , yielding  $p < 59$ . Since  $p$  is prime, this forces  $p \leq 53$ , contradicting that  $p > 55$ , which completes the proof.  $\square$

We can now prove the main result.

*Proof of Theorem 4.13.* Let  $A \subseteq \mathbb{Z}_p$  be an  $m$ -sum-free subset of maximum size, with  $|A| = \eta p$ , and let

$$\alpha = \alpha(\eta, p) = -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8\eta p \sin(\pi/p) / \sin(\pi\eta/3)}.$$

Assume by contradiction that  $\eta \geq c$ . Then, since  $x \mapsto \frac{1+3/p}{3+\alpha(x,p)}$  is decreasing in  $x \in (0, 1)$  and  $c = \frac{1+3/p}{3+\alpha(c,p)}$ , we deduce that  $\eta \geq c \geq \frac{1+3/p}{3+\alpha}$ , whence

$$|A| \geq \frac{p+3}{3+\alpha} > 1. \quad (4.30)$$

As noted at the start of the proof of Theorem 4.4,  $\alpha(\eta, p)$  is increasing for  $\eta \in (0, 1)$  with  $p \sin(\pi/p) \rightarrow \pi$  monotonically. Since  $2A$  and  $m \cdot A$  are disjoint, we have  $|2A| \leq p - |A|$ , while  $|2A| \geq 2|A| - 1$  by the Cauchy-Davenport Theorem. Thus  $2|A| - 1 \leq |2A| \leq p - |A|$ , implying  $|A| \leq \frac{p+1}{3}$  and  $\eta \leq \frac{p+1}{3p}$ . If  $p = 5$ , then  $1 < |A| \leq \frac{p+1}{3} = 2$  forces  $|A| = 2$  and  $\eta = \frac{2}{5}$ , whence  $\alpha < 0.167$ . If  $p = 7$ , then  $\eta \leq \frac{p+1}{3p} = \frac{8}{21}$  and  $\alpha \leq -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8(8/21)7 \sin(\pi/7) / \sin(\pi(8/21)/3)} < .183$ . For  $p \geq 11$ , we have  $\eta \leq \frac{p+1}{3p} \leq \frac{12}{33}$  and  $\alpha \leq -\frac{5}{4} + \frac{1}{4}\sqrt{9 + 8(12/33)\pi / \sin(\pi(12/33)/3)} < 0.199$ . Thus

$$\alpha < 0.2$$

in all cases.

Let  $|2A| = 2|A| + r$ . Since  $A$  is  $m$ -sum-free, the sets  $2A$  and  $m \cdot A$  are disjoint, which implies that  $|2A| < p$  (as  $A$  is nonempty) and that  $p \geq |2A| + |m \cdot A| = 3|A| + r$ . Thus

$$|A| \leq \frac{p-r}{3} \quad \text{and} \quad |2A| = 2|A| + r \leq \frac{2p+r}{3}.$$

Since  $|2A| < p$ , the Cauchy-Davenport Theorem implies  $r \geq -1$ .

If  $|2A| = 2|A| + r > (2 + \alpha)|A| - 3$ , then  $r > \alpha|A| - 3$ , in which case  $|A| \leq \frac{p-r}{3} < \frac{p-\alpha|A|+3}{3}$ , which contradicts (4.30). Therefore  $|2A| \leq (2 + \alpha)|A| - 3$  and  $r \leq \lfloor \alpha|A| - 3 \rfloor$ . We can now apply Theorem 4.4. As a result, there are arithmetic progressions  $P_A$  and  $P_{2A}$  with common difference  $g$  such that  $A \subseteq P_A$ ,  $P_{2A} \subseteq 2A$ ,

$$|P_A| = \lfloor (1 + \alpha)|A| - 2 \rfloor \leq p \quad \text{and} \quad |P_{2A}| = 2|A| - 1. \quad (4.31)$$

It follows that  $P := m \cdot P_A$  is an arithmetic progression with difference  $mg \neq \pm g$  such that

$$|P \cap P_{2A}| \leq |P \cap 2A| \leq |P_A \setminus A| \leq \alpha|A| - 2. \quad (4.32)$$

We can therefore apply Lemma 4.14 with  $N = |A|$  (as  $\alpha < 0.2$ ), deducing that  $|A| < \frac{p+3}{3+\alpha}$ , a contradiction. Therefore we must have  $\eta < c$ , so  $d_m(\mathbb{Z}_p) < c$ , which proves the first claim in the theorem. Taking the limit of  $c$  as  $p \rightarrow \infty$ , we deduce that  $d_m \leq t$  where  $t = \left(\frac{7}{4} + \frac{1}{4}\sqrt{9 + 8t\pi/\sin(\pi t/3)}\right)^{-1}$ , and the second claim in the theorem follows from solving for  $t$  numerically.  $\square$

## Acknowledgements

We are very grateful to Tomasz Schoen for providing the construction in Lemma 4.11 and for some useful remarks.

# Chapter 5

## Nilspaces and cubic couplings

This chapter summarizes the content of [9, 10, 17, 18], adding new proofs of known facts, and small results. The original parts are indicated at the beginning of each section in this chapter. It should be read in conjunction with Appendix A, where some longer proofs and auxiliary definitions have been placed.

### 5.1 Introduction

To study some problems in mathematics, it is often useful to define an object that encodes the relevant information about the problem and discards the rest. A good example of this is the concept of a group. In the 1830s, Évariste Galois proved that to study whether a polynomial equation has solutions using only radicals, it was convenient to study its (now-called) Galois group. He also introduced the name *group* to describe these objects that (roughly speaking) have one operation, the group law. We devote this chapter to a treatment of objects that encode much of the information needed in many problems in additive combinatorics and ergodic theory. These objects are called nilspaces.

The origins of these developments go back to 1936 in a paper of Erdős and Turán, [26]. In that work, they conjectured that any subset  $A \subset \mathbb{N}$  without non-trivial arithmetic progressions (we will omit the term *non-trivial* in the sequel) has size  $|A \cap [1, N]| = o(N)$ . In 1953, Roth proved (in [74]) the following result.

**Theorem 5.1** (Roth). *Let  $A \subset \mathbb{N}$  be a subset of the integers with no arithmetic progression of length three. Then*

$$|A \cap [1, N]| \ll \frac{N}{\log \log N}.$$

The equivalent question for progressions of arbitrary length remained open until the work of Szemerédi in 1975 [87]:

**Theorem 5.2** (Szemerédi). *Let  $k \geq 3$  be an integer. Then any  $A \subset \mathbb{N}$  with no  $k$  terms in arithmetic progression satisfies*

$$|A \cap [1, N]| = o_k(N).$$

Two years later, Furstenberg gave an ergodic-theoretic proof of Szemerédi's theorem, in [30]. Although the concept of a nilspace had not appeared yet, the aforementioned work showed that there was a relationship between ergodic theory and additive combinatorics.

The next main step was taken by Gowers in his breakthrough paper in 2001, [32]. Before explaining this result, let us mention one of the problems that motivated it. The proofs of Roth and Szemerédi were very different in nature. On the one hand, the proof of Roth seemed to work only for progressions of length three, used Fourier-analytic methods, and gave reasonably good bounds on  $|A \cap [1, N]|$ . On the other hand, the proof of Szemerédi used graph-theoretical methods, worked for progressions of any length, but the bounds on  $|A \cap [1, N]|$  were very poor. We did not write it explicitly in Theorem 5.2, but the bound was roughly  $N$  over a tower exponential depending on  $N$  and  $k$ . In [32], Gowers found the correct generalization of the arguments of Roth to the case of progressions on length four.

One of the key ideas was the introduction of the Gowers norms.

**Definition 5.3** (Gowers norms). Let  $k \geq 2$  be an integer, let  $G$  be a compact abelian group, and let  $f : G \rightarrow \mathbb{C}$  be any bounded Borel function. The Gowers  $U^k$  norm of  $f$ , denoted by  $\|f\|_{U^k}$ , is defined by

$$\|f\|_{U^k}^{2^k} := \mathbb{E}_{x \in G, \underline{h} \in G^k} \prod_{\underline{w} \in \llbracket k \rrbracket} \mathcal{C}^{|\underline{w}|} f(x + \underline{w} \cdot \underline{h}). \quad (5.1)$$

In [32], these norms are called uniformity norms, and are defined for  $G = \mathbb{Z}_p$ . It can be proved that for every  $k \geq 2$ , (5.1) gives a norm. Note that the

above definition for  $k = 0$  would give  $\mathbb{E}(f)$ , and for  $k = 1$ ,  $|\mathbb{E}(f)|$ . These are not norms, but it is useful to consider them sometimes.

Although it is not stated explicitly in the following form, Gowers proved that if a set  $A \subset \mathbb{Z}_p$  has no progression of length  $k + 1$ , then  $1_A - \mathbb{E}(1_A)$  has a large  $U^k$  norm. Using this fact (loosely speaking), Gowers adapted the *density increment* argument of Roth, and proved that if a set  $A \subset \mathbb{N}$  has no arithmetic progression of length  $k$ , then

$$|A \cap [1, N]| \ll \frac{N}{(\log \log N)^{c_k}}$$

for some explicit  $c_k > 0$ .

In 2005, Host and Kra published a paper that constitutes another milestone in these developments, [50]. In this work they proved that to study the convergence of some averages in some ergodic systems, it is enough to study the convergence on the corresponding characteristic factors. Most importantly, they showed that these factors are essentially (inverse limits of) nilmanifolds. Recall that nilmanifolds are examples of homogeneous spaces, and diffeomorphic to the quotient of a nilpotent Lie group by a discrete cocompact subgroup. The advantage of reducing to nilmanifolds is that in general, we know much better the behavior of nilmanifolds because of the rich structure they have. Host and Kra also defined a family of seminorms which, in the particular case where the probability space is  $\mathbb{Z}_p$ , are equal to the Gowers norms.

Also in 2005, Green and Tao were making significant progress in arithmetic combinatorics. In [36] (published on ArXiv in 2004) they had already used the Gowers norms to prove their celebrated result that the primes contain arbitrarily long arithmetic progressions. Motivated to a large extent by refining the analysis of progressions in primes, in their paper [37] (which was published in 2008, but was on ArXiv since 2005) they developed the concept of inverse theorems for the Gowers norms. These theorems say, roughly speaking, that if a bounded function  $f : G \rightarrow \mathbb{C}$  has a large Gowers  $U^k$  norm, then it has a large correlation with a nilsequence. For the precise definition of nilsequence, see [4, Definition 1.8].

The Gowers norms enable us to count not only the number of arithmetic progressions, but also more general types of linear configurations. In 2007, Gowers and Wolf published their work [34] in which they study which Gowers norm controls linear configurations of a given type.

Coming back to the roots of nilspaces, the first paper where we find a structure that later will be a special case of a nilspace is [49], due to Host and Kra. Here, they defined a general structure where a Gowers norm could be defined. They called these objects *parallelepiped structures*. This would correspond later to 2-step nilspaces. The authors also point out that a generalization of their arguments is possible. This generalization is what leads to the concept of a nilspace. In this paper, Host and Kra defined very important structures that we will discuss further below, like how to construct a nilspace from a nilpotent filtered group. They also proved that not every nilspace comes from such a group.

In 2010, Antolín Camarena and Szegedy published on ArXiv the preprint [1], introducing nilspaces. They defined these objects, they endowed them with a compact topology, and they proved important results like the inverse limit theorem for nilspaces and the structural description of toral nilspaces in terms of nilmanifolds. All these concepts will be explained in detail later. Indeed, this chapter is intended to exhibit the results of this paper among other things.

Following the influential paper mentioned in the previous paragraph, many authors started to work on nilspaces. Among such works we find those of Gutman, Manners, and Varjú; and Candela and Szegedy. The former ones developed the theory of nilspaces with the focus on studying dynamical systems, in the series of papers [40, 41, 42]. The latter ones explored further the connection between additive combinatorics and ergodic theory [17], and used it to prove a more general version of the inverse theorem [18].

One of the motivations of [17] was to find a generalization of the characteristic factors of Host and Kra in [50]. Indeed, Chapter 6 of this thesis concerns a result about nilspaces used to prove that generalization. The main idea introduced in the paper [17] is the concept of a *cubic coupling*. Roughly speaking, a cubic coupling is a family of measures such that we can define Gowers norms (or seminorms) on them. The main result of that paper shows that the characteristic factors of a cubic coupling are nilspaces.

The purpose of this chapter is to summarize the most important results of [1, 9, 10, 17]. As mentioned in the introduction, we will enrich the known theory of nilspaces with examples, different proofs of known results, and new small results that hopefully will be useful in the future.

Coming back to our opening mention of Galois theory, we would like to end this chapter pointing out that the similarities between nilspaces and

groups do not boil down only to their origins. Abelian groups will be a particular case of nilspaces, and many of the known results and concepts for groups will have an analog for nilspaces. Let us mention some of them:

Abelian groups	Nilspaces
<ul style="list-style-type: none"> <li>• Action by summing an element, <math>x \mapsto x + z</math>.</li> <li>• Surjective homomorphisms, <math>\varphi : Z \rightarrow Z'</math>.</li> <li>• Inverse Limit Theorem: Every compact abelian group <math>Z</math> can be expressed as <math>Z = \varprojlim Z_i</math> where <math>Z_i</math> are compact abelian Lie groups.</li> <li>• Automatic continuity ([56, Theorem 1]): A Borel measurable homomorphism is continuous.</li> </ul>	<ul style="list-style-type: none"> <li>• Action of the translation group in the nilspace <math>x \mapsto \alpha(x)</math>.</li> <li>• Fibrations, <math>\phi : X \rightarrow Y</math>.</li> <li>• Inverse Limit Theorem: Every compact nilspace <math>X</math> is an inverse limit <math>\varprojlim X_i</math> for some compact finite-rank nilspaces <math>X_i</math>.</li> <li>• Automatic continuity ([9, Theorem 2.4.6]): A Borel measurable morphism is continuous.</li> </ul>

This table is intended to serve as a reference throughout this chapter. We will carefully explain the concepts that appear on the right-hand side of the table in the sequel.

Just as groups can be thought of as purely algebraic objects, and then we can add a topology and call them topological groups, we can do the same with nilspaces. In Section 5.2, we define nilspaces as algebraic objects with three axioms, and we present their algebraic theory. In Section 5.3 we give nilspaces a compact topology, and we exhibit some of the most important results. Note that this is analogous to turning groups into *topological* groups. In Section 5.4, we define cubic couplings, and we sketch the proof of the regularity lemma using cubic couplings.

## 5.2 Algebraic theory of nilspaces

In this section, we present the algebraic definition and properties of nilspaces. The main inspiration here is the paper [9]. We will follow a similar structure as in the mentioned paper and we will constantly refer to it for references and further details. Every part of this section until we reach Subsection 5.2.5 *Construction of nilspaces, translation groups and non-coset nilspaces* will be a summary of [9]. This last subsection is an original one where we apply some of the results to produce some examples of nilspaces. For com-

pleteness, let us mention also that many results from [9] had been proved before in [1].

First of all, let us recall that  $\llbracket n \rrbracket$  is the set  $\{0, 1\}^n$  where  $n \geq 1$  and  $\llbracket 0 \rrbracket = \{0\}$ . Let us define:

**Definition 5.4** (Discrete-cube morphism). Let  $n, m \geq 0$ . A function  $\phi : \llbracket n \rrbracket \rightarrow \llbracket m \rrbracket$  is a discrete-cube morphism if it is the restriction of an affine homomorphism<sup>1</sup>  $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ .

It can be seen that a discrete-cube morphism  $\phi : \llbracket n \rrbracket \rightarrow \llbracket m \rrbracket$  must be of the following form (for a proof, see [9, Lemma 1.1.2]). For every  $i = 1, \dots, m$ , the  $i$ -th coordinate of  $\phi(\underline{v})$  must be either 0, 1,  $v(j_i)$  or  $1 - v(j_i)$  for some  $j_i \in \{1, \dots, n\}$ . As an example of this:  $\phi_1 : \llbracket 2 \rrbracket \rightarrow \llbracket 3 \rrbracket$  defined by  $(v(1), v(2)) \mapsto (0, v(2), 1 - v(1))$  is a discrete-cube morphism.

**Definition 5.5** (Faces and face maps). Let  $n \geq 0$ . A face  $F$  of dimension  $m \leq n$  is a subset of  $\llbracket n \rrbracket$  defined by fixing  $n - m$  coordinates. This is,  $F = \{\underline{v} \in \llbracket n \rrbracket : v(i) = t(i), i \in I\}$  for some  $I \subset \{1, \dots, n\}$  with  $|I| = n - m$  and  $t(i) \in \{0, 1\}$  for all  $i \in I$ . A face map  $\phi : \llbracket k \rrbracket \rightarrow \llbracket n \rrbracket$  is an injective discrete-cube morphism such that  $\phi(\llbracket k \rrbracket)$  is a face of dimension  $k$ .

The map  $\phi_1$  defined above is an example of a face map. Let us give another example of a discrete-cube morphism:  $\phi_2 : \llbracket 3 \rrbracket \rightarrow \llbracket 1 \rrbracket$  defined by  $(v(1), v(2), v(3)) \mapsto 1 - v(3)$ . This is clearly not a face map nor is it even injective.

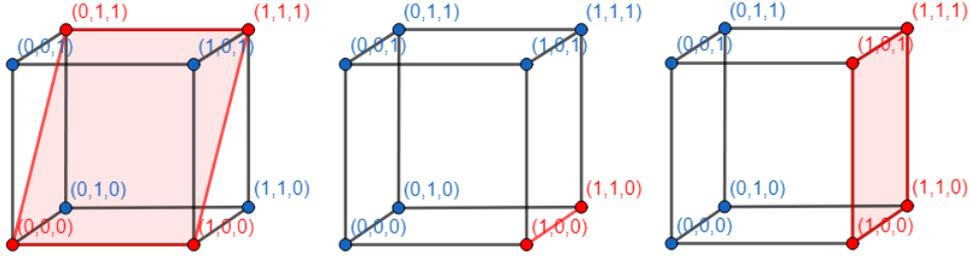
It is convenient to introduce a special type of faces, the so-called *upper and lower faces*.

**Definition 5.6** (Upper and lower faces). Let  $I \subset \{1, \dots, n\}$ . A face  $F = \{\underline{v} \in \llbracket n \rrbracket : v(i) = t(i), i \in I\}$  is an upper (resp. lower) face if  $t(i) = 1$  (resp.  $t(i) = 0$ ) for all  $i \in I$ . Equivalently, a face is an upper face if it contains  $1^n$ , and is a lower face if it contains  $0^n$ .

In the following picture we can see examples of the image of the discrete-cube morphism  $(v(1), v(2)) \mapsto (v(1), v(2), v(2))$ , a non-upper face of dimension 1, and an upper face of dimension 2 inside  $\llbracket 3 \rrbracket$ :

---

<sup>1</sup>An affine homomorphism  $f : Z_1 \rightarrow Z_2$  between abelian groups  $Z_1$  and  $Z_2$  is a function  $f(z) = g(z) + t$ , where  $g : Z_1 \rightarrow Z_2$  is a homomorphism and  $t \in Z_2$ .



Now we can state the main definition of this chapter:

**Definition 5.7** (Nilspace). A nilspace  $X$ , along with a collection of sets  $C^n(X) \subset X^{\llbracket n \rrbracket}$  for every  $n \geq 0$  satisfying:

1. Composition: For every discrete-cube morphism  $\phi : \llbracket m \rrbracket \rightarrow \llbracket n \rrbracket$  and every  $c \in C^n(X)$  we have that  $c \circ \phi \in C^m(X)$ .
2. Ergodicity:  $C^1(X) = X^{\llbracket 1 \rrbracket}$ .
3. Completion: Let  $c' : \llbracket n \rrbracket \setminus \{1^n\}$  be a function such that if  $\phi : \llbracket n-1 \rrbracket \rightarrow \llbracket n \rrbracket$  is a face map with  $\phi(\llbracket n-1 \rrbracket) \subset \llbracket n \rrbracket \setminus \{1^n\}$ , then  $c' \circ \phi \in C^{n-1}(X)$ . Then there exists  $c \in C^n(X)$  such that  $c = c'$  in  $\llbracket n \rrbracket \setminus \{1^n\}$ .

Note that this is only an algebraic definition. In the next section we will endow nilspaces with a topology. The elements of the sets  $C^n(X)$  are referred to as *cubes* or *n-cubes* if we want to stress the dimension  $n$ . Similarly, the functions  $c'$  from the Completion axiom are called *corners* or *n-corners*.

**Definition 5.8** (*k*-step nilspaces). We say that a nilspace  $X$  is *k*-step for some  $k \geq 0$  when  $(k + 1)$ -corners have a unique completion.

Some objects satisfy only some of the axioms by which we define nilspaces, but we will postpone the discussion about them to Appendix A, see Definition A.1 and Definition A.2.

A natural notion that arises in this context is the notion of morphisms between nilspaces.

**Definition 5.9** (Morphism and isomorphism). Let  $X$  and  $Y$  be nilspaces. A function  $\varphi : X \rightarrow Y$  is a morphism if for every cube  $c \in C^n(X)$ , we have that  $\varphi \circ c \in C^n(Y)$ . Moreover, if  $\varphi$  is invertible and the inverse is a morphism, we say that  $\varphi$  is an isomorphism.

Another important concept is the following:

**Definition 5.10** (*l-fold ergodic nilspace*). Let  $X$  be a nilspace and  $l \geq 0$  be an integer. We will say that  $X$  is *l-fold ergodic* if  $C^l(X) = X^{\llbracket l \rrbracket}$ .

By the composition axiom, it is easy to check that if a nilspace is *l-fold ergodic*, then it is also *j-fold ergodic* for all  $j \leq l$ .

### 5.2.1 Examples of nilspaces

Recall the definition of the commutator subgroups of a group. Given  $G$  a group and  $g, h \in G$ , we define the commutator of  $g$  and  $h$  as

$$[g, h] := g^{-1}h^{-1}gh.$$

For any two subgroups  $H, H' \leq G$ , the commutator of  $H$  and  $H'$  is defined by:

$$[H, H'] := \{h^{-1}h'^{-1}hh' : h \in H, h' \in H'\}.$$

**Definition 5.11** (*Filtration*). A filtration  $G_\bullet$  on a group  $G$  is a set of subgroups  $(G_i)_{i=0}^\infty$  such that

$$G = G_0 \geq G_1 \geq G_2 \geq \dots,$$

and  $[G_i, G_j] \subset G_{i+j}$  for all  $i, j \geq 0$ .

Typically, we will assume  $G_1 = G_0 = G$  unless otherwise stated. If our filtration does not satisfy that condition, we will say that it is a prefiltration. If for some  $k \geq 0$  we have that  $G_{k+1} = \{id\}$ , we will say that the filtration has degree  $k$ . A group  $G$  is a filtered group if there exists a filtration  $G_\bullet = (G_i)_{i=0}^\infty$  on  $G$ .

To define a nilspace from a filtered group, we need to define the following elements. Given  $g \in G$  and a face  $F \subset \llbracket n \rrbracket$ , we define  $g^F \in G^{\llbracket n \rrbracket}$  as the function

$$g^F(v) = \begin{cases} g & \text{if } v \in F \\ id & \text{otherwise.} \end{cases}$$

**Definition 5.12** (Group nilspaces). Given a filtered group  $G$  with filtration  $G_\bullet = (G_i)_{i=0}^\infty$ , we can define the nilspace  $X := G$  with the set of cubes

$$C^n(X) := \langle g^F : \text{for some } i \in \{0, \dots, n\} \text{ we have } g \in G_i \text{ and } \text{codim}(F) = i \rangle$$

for all  $n \geq 0$ . We will often write  $G$  as the nilspace and  $C^n(G)$  as its set of cubes when the filtration is clear, and  $C^n(G_\bullet)$  when we want to stress the filtration.

*Remark 5.13.* These cubes are also referred to as Host-Kra cubes.

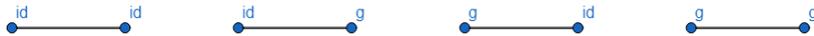
**Proposition 5.14.** *For every filtered group  $(G, G_\bullet)$ , the above construction gives us a nilspace  $X = G$ . Moreover, the nilspace will be  $k$ -step if and only if the degree of the filtration is at most  $k$ , and  $l$ -fold ergodic if and only if  $G_i = G$  for all  $i \in \{0, \dots, l\}$ .*

The proof of this proposition can be deduced from [9, Proposition 2.2.8 and Lemma 2.2.5].

Let us present some examples of group nilspaces. Take  $G = C_2 = \{id, g\}$  the cyclic group of two elements with filtration  $C_2 = C_2 \geq \{id\}$ , and consider the corresponding group nilspace  $X$ . This is, of course, the same as  $\mathbb{Z}_2$ , but just in this example we are going to use  $C_2$  to avoid the confusion between the elements of  $\llbracket n \rrbracket = \{0, 1\}^n$  and  $\mathbb{Z}_2 = \{0, 1\}$ . Let us familiarize with some examples of cubes for this nilspace. It is easy to check by hand that

$$C^0(X) = \{id, g\}.$$

To represent the elements of  $C^1(X)$ , we can write them as:



Each segment represents an element of  $C^1(X)$ , the value on the left is the value of the cube at 0, and the value on the right is the value at 1. It is easy to check that these are the four possibilities.

To compute the  $n$ -cubes for higher  $n$ 's, it is convenient first to introduce some characterization of the cubes. For any fixed  $n \geq 0$ , note that there are exactly  $2^n$  upper faces. Take any total order of these faces such that if  $F \subset F'$ , then  $F' \leq F$ . A possible ordering is the following: given  $\underline{v} \in \llbracket n \rrbracket$

we can define  $F_{\underline{v}} := \{\underline{w} \in \llbracket n \rrbracket : w(i) \geq v(i) \text{ for all } i = 1, \dots, n\}$ . These are all possible upper faces. We can order the elements  $\underline{v} \in \llbracket n \rrbracket$  using the lexicographic order and this gives a possible order for the upper faces. Recall that by definition  $\llbracket 0 \rrbracket = \{0\}$ . Another important concept is the alternating sum:

**Definition 5.15** (Alternating sum). Let  $G$  be any group. We define  $\sigma_0(f)$  for a function  $f_0 \in G^{\llbracket 0 \rrbracket}$  as  $\sigma_0(f_0) = f_0(0)$ . Then define recursively  $\sigma_n(f_n)$  for any  $f_n \in G^{\llbracket n \rrbracket}$  as

$$\sigma_n(f_n) := \sigma_{n-1}(f_n(\cdot, 1))^{-1} \sigma_{n-1}(f_n(\cdot, 0)),$$

where  $f_n(\cdot, i) \in G^{\llbracket n-1 \rrbracket}$  is the function that we obtain by fixing the last coordinate equal to  $i \in \{0, 1\}$ .

With this, we can give the following characterization of cubes:

**Proposition 5.16.** *Let  $X = G$  be the group nilspace coming from the filtered group  $(G, G_\bullet)$ . For any  $c \in G^{\llbracket n \rrbracket}$  the following are equivalent:*

1.  $c \in C^n(X)$ .
2. We can write  $c = g_0^{F_0} g_1^{F_1} \cdots g_{2^n-1}^{F_{2^n-1}}$  where  $F_i$  are the upper faces ordered as explained previously and  $g_i \in G_{\text{codim}(F_i)}$  for all  $i = 0, \dots, 2^n - 1$ .
3. For any face map  $\phi : \llbracket m \rrbracket \rightarrow \llbracket n \rrbracket$ , we have that  $\sigma_m(c \circ \phi) \in G_m$ .

A proof of this proposition can be found in [9, Proposition 2.2.28]. The second characterization gives us an easier way of finding all possible cubes for a given group nilspace. For instance, coming back to our example of  $X = G = C_2$  with filtration  $C_2 = C_2 \geq \{id\}$ , we know that there are exactly  $2^{n+1}$  elements in  $C^n(X)$ .

A further construction based on filtered groups is the following (for a proof, see [9, Proposition 2.3.1]):

**Definition 5.17** (Coset nilspaces). Let  $(G, G_\bullet)$  be a filtered group and let  $\Gamma$  be a subgroup of  $G$ . Let  $\pi : G \rightarrow G/\Gamma$  be the canonical projection for the equivalence relation defined on  $G$  by  $g \sim h \Leftrightarrow g^{-1}h \in \Gamma$ . Then we can define  $X = G/\Gamma$  as a nilspace with the set of cubes

$$C^n(X) := \{\pi \circ c : c \in C^n(G)\}.$$

Recall that  $C^n(G)$  are the set of cubes of the corresponding group nilspace. We will often write  $G/\Gamma$  for the nilspace and  $C^n(G/\Gamma)$  its set of cubes.

Important examples of nilspaces are those which are  $k$ -step and  $k$ -fold ergodic. It can be proved (see [9, Proposition 3.2.14]) that every such nilspace is a group nilspace. Furthermore, there exists an abelian group  $Z$  with filtration  $Z_\bullet = (Z_i)_{i=0}^\infty$  where  $Z_i = Z$  for  $i \leq k$  and  $Z_i = \{0\}$  for  $i > k$  such that  $X$  is isomorphic (see Definition 5.9) to the group nilspace  $(Z, Z_\bullet)$ . As we will use these special nilspaces in many occasions, it is convenient to give them a name:

**Definition 5.18.** Let  $k \geq 0$  be an integer. The nilspace  $\mathcal{D}_k(Z)$  is defined as the group nilspace coming from  $(Z, Z_\bullet)$ , where  $Z$  is an abelian group, and  $Z_\bullet = (Z_i)_{i=0}^\infty$  where  $Z_i = Z$  for  $i \leq k$  and  $Z_i = \{0\}$  for  $i > k$ .

Thus, the nilspace from the previous example was  $\mathcal{D}_1(C_2)$ . As all nilspaces are 1-fold ergodic, if they are also 1-step, then [9, Proposition 3.2.14] tells us the following:

**Corollary 5.19.** *Every 1-step nilspace is isomorphic to  $\mathcal{D}_1(Z)$  for some abelian group  $Z$ .*

There exist nilspaces that cannot be represented as coset nilspaces. We will prove this at the end of this section, giving explicit examples.

## 5.2.2 Characteristic factors and abelian bundles, morphisms and fibrations.

In the study of the structure of nilspaces, an important equivalence relation arises:

**Definition 5.20** (Characteristic factors). Let  $X$  be a nilspace and let  $k \geq 0$  be an integer. We define the following equivalence relation on  $X$ :

- We say  $x \sim_k y$  for  $x, y \in X$  if there exist cubes  $c_1, c_2 \in C^{k+1}(X)$  such that  $c_1(v) = c_2(v)$  for all  $v \neq 0^{k+1}$ ,  $c_1(0^{k+1}) = x$ , and  $c_2(0^{k+1}) = y$ .

We denote by  $X_k$  the set  $X / \sim_k$  and we call it the  $k$ -characteristic factor or  $k$ -factor for short.

To check that this is an equivalence relation, the transitivity property is the only non-trivial part; see Proposition A.23 for a proof.

*Remark 5.21.* There are cases where we need to work with different nilspaces  $X_1, X_2, \dots$ . In such cases, we will denote the characteristic factors of these nilspaces as  $\pi_j(X_i)$  for any  $i$  and  $j$  to avoid confusion.

The characteristic factors can be endowed with a nilspace structure as explained in the following lemma:

**Lemma 5.22.** *Let  $X$  be a nilspace and  $k \geq 0$  an integer. For all  $n \geq 0$  let us define*

$$C^n(X_k) := \{\pi_k \circ c : c \in C^n(X)\},$$

where  $\pi_k : X \rightarrow X_k$  is the canonical projection.

Then  $X_k$  with these cubes is a  $k$ -step nilspace.

For a proof of this lemma, see [9, Lemma 3.2.10].

In general, we will be interested in studying the structure of  $k$ -step nilspaces. This equivalence relation allows us to see  $k$ -step nilspaces as an iterated abelian bundle.

**Definition 5.23** (Abelian bundle). Let  $Z$  be an abelian group. We say that  $B$  is an abelian bundle over  $S$  with structure group  $Z$ , action  $\alpha : B \times Z \rightarrow B$ ,  $(b, z) \mapsto b + z$ , and projection  $\pi : B \rightarrow S$  when:

- The action  $\alpha$  is free, i.e.,  $\{z \in Z : b + z = b\} = \{0_Z\}$  for all  $b \in B$ .
- The action  $\alpha$  is transitive over the fibers of  $\pi$ . This means that for any  $b \in B$ ,  $\{b' \in B : \pi(b') = \pi(b)\} = \{b + z : z \in Z\}$ .

A set  $B$  is a  $k$ -fold abelian bundle with structure groups  $Z_1, \dots, Z_k$  if there is a sequence  $B_0, B_1, \dots, B_k$  such that  $B_0$  is a singleton,  $B_k = B$ , and  $B_j$  is an abelian bundle over  $B_{j-1}$  with structure group  $Z_j$  for all  $j = 1, \dots, k$ . We will denote by  $\pi_j : B \rightarrow B_j$  the iterated projection.

Recall from Definition A.2 the notion of a cubespace. We say that a set  $X$  together with a set of cubes  $C^n(X)$  for all  $n \geq 0$  is a cubespace when it satisfies the composition axiom of Definition 5.7 and  $C^0(X) = X$ .

**Definition 5.24** (Degree- $k$  bundle). A cubespace  $X$  is a degree- $k$  bundle if it is also a  $k$ -fold abelian bundle with factors  $B_0, B_1, \dots, B_k = X$  and structure groups  $Z_1, \dots, Z_k$  satisfying the following property. For every  $n \geq 0$  and every  $i = 0, \dots, k - 1$ ,  $C^n(B_i) = \{\pi_i \circ c : c \in C^n(X)\}$ , and for every  $c \in C^n(B_{i+1})$ ,

$$\{c' \in C^n(B_{i+1}) : \pi_i \circ c = \pi_i \circ c'\} = \{c + c^* : c^* \in C^n(\mathcal{D}_{i+1}(Z_{i+1}))\}.$$

The following result can be found in [9, Theorem 3.2.19]:

**Theorem 5.25.** *Let  $X$  be a cubespace. Then  $X$  is a  $k$ -step nilspace if and only if it is a degree- $k$  bundle. In addition,  $X_j = B_j$  for all  $j = 1, \dots, k$ .*

Graphically, the bundle structure of a  $k$ -step nilspace can be represented as:

$$\begin{array}{ccccccc} & \curvearrowright Z_k & & \curvearrowright Z_{k-1} & & & \\ X = X_k & \longrightarrow & X_{k-1} & \longrightarrow & \cdots & \longrightarrow & X_0 \end{array}$$

*Remark 5.26.* Not only nilspaces will be  $k$ -fold abelian bundles. For example, given a  $k$ -step nilspace  $X$ , for any fixed  $n \geq 0$ , the set  $C^n(X)$  is also a  $k$ -fold abelian bundle. The factors will be  $C^n(X_i)$  for  $i = 0, \dots, k$ . If  $\pi_{i,i+1} : X_{i+1} \rightarrow X_i$  for all  $i \geq 0$ , then the projections in  $C^n(X_{i+1})$  will be  $\pi_{i,i+1}^{[n]}$  and the structure groups will be  $C^n(\mathcal{D}_i(Z_i))$ . This fact, and a more general one, will be important when defining the Haar measure on cubes, but we postpone the discussion about them to Subsection A.1.3.

Now let us move our attention to morphisms between nilspaces.

**Definition 5.27** (Bundle morphism). Let  $B$  and  $B'$  be two  $k$ -fold abelian bundles (with factors  $B_i, B'_i$ , for  $i = 0, \dots, k$ , structure groups  $Z_i, Z'_i$  and projections  $\pi_i, \pi'_i$ , for  $i = 1, \dots, k$  respectively). A map  $\varphi : B \rightarrow B'$  is a bundle morphism if the following conditions hold:

- For every  $i = 0, \dots, k - 1$  and every  $x, y \in B$ , if  $\pi_i(x) = \pi_i(y)$ , then  $\pi'_i(\varphi(x)) = \pi'_i(\varphi(y))$ . This induces the maps  $\varphi_i : B_i \rightarrow B'_i$ .

- For every  $i = 0, \dots, k - 1$  there exists a map  $\alpha_i : Z_i \rightarrow Z'_i$  such that for all  $x \in B_i, z \in Z_i$  we have  $\varphi_i(x + a) = \varphi_i(x) + \alpha_i(z)$ . These maps will be called structure morphisms.

We say that  $\varphi$  is totally-surjective if all structure morphisms are surjective.

Note that this definition implies that the maps  $\alpha_i$  are homomorphisms. It can be proved that given a morphism  $\varphi : X \rightarrow Y$  between  $k$ -step nilspaces, then  $\varphi$  is a bundle morphism between the corresponding  $k$ -fold abelian bundles (see [9, Proposition 3.3.2]).

If we go back to the analogy between abelian groups and nilspaces made in the introduction of this chapter, we should see morphisms as the analogues of homomorphisms. Thus, we can ask ourselves what would be the analogues of surjective homomorphisms. The following definition was given in [40, Definition 7.1]:

**Definition 5.28** (Fibrations). Let  $X$  and  $Y$  be nilspaces. A morphism  $\phi : X \rightarrow Y$  is a fibration if the following holds. For every cube  $c \in C^n(Y)$  and every  $n$ -corner  $c' \in \text{Cor}^n(X)$  such that  $c(v) = \phi(c'(v))$  for all  $v \neq 1^n$ , there exists a completion  $\tilde{c}$  of  $c'$  such that  $\phi(\tilde{c}(1^n)) = c(1^n)$ .

The relationship between fibrations and surjective homomorphisms is given by the following lemma:

**Lemma 5.29.** *Let  $X$  and  $Y$  be  $k$ -step nilspaces, and let  $\phi : X \rightarrow Y$  be a morphism. Then  $\phi$  is a fibration if and only if it is a totally-surjective bundle morphism.*

*Proof.* See paragraph after [40, Remark 7.4]. □

*Remark 5.30.* In [40, Definition 7.1], the definition of fibration was introduced to use it with cubespaces that were not necessarily nilspaces. Similarly, the concept of totally-surjective bundle morphism was introduced in [1, Definition 2.9] because they needed to use it with  $k$ -fold abelian bundles. Those classes of objects are not included one inside the other, and depending on the context, it is preferable to use one or the other. Fortunately, both definitions are equivalent in the case of  $k$ -step nilspaces.

### 5.2.3 Group of translations

The previous results tell us that  $k$ -step nilspaces can be decomposed as abelian bundles with that extra condition on the cubes. However, in practice, it is much more useful to know that, for instance, a nilspace is a coset nilspace. To say whether or not a nilspace is a coset nilspace, we introduce the following concept. Given a function  $\alpha : X \rightarrow X$  and a face  $F \subset \llbracket n \rrbracket$  and a function  $g \in X^{\llbracket n \rrbracket}$ , we denote by  $\alpha^F(g) : X^{\llbracket n \rrbracket} \rightarrow X^{\llbracket n \rrbracket}$  the function such that

$$g \mapsto \begin{cases} \alpha(g(v)) & \text{if } v \in F \\ g(v) & \text{in any other case.} \end{cases}$$

**Definition 5.31** (Translations). Let  $X$  be a nilspace. For any  $i \geq 1$  we say that  $\alpha : X \rightarrow X$  is an  $i$ -translation if for every cube  $c \in C^n(X)$  and any face  $F \subset \llbracket n \rrbracket$  of codimension  $i$ , we have  $\alpha^F(c) \in C^n(X)$ . For every  $i \geq 1$  we denote this set of functions by  $\Theta_i(X)$ . By definition we take  $\Theta_0(X) := \Theta_1(X)$ .

**Lemma 5.32** (Translation group). *Let  $X$  be a nilspace. If  $\Theta(X) := \Theta_1(X)$ , then this is a filtered group with filtration  $\Theta(X)_\bullet := (\Theta_i(X))_{i \geq 0}$ . Moreover, if  $X$  is  $k$ -step, then so is  $(\Theta(X), \Theta(X)_\bullet)$ .*

*Proof.* See [9, Corollary 3.2.36]. □

### 5.2.4 Extensions and cocycles

In this section, we deal with the problem of constructing a new nilspace from a known one. For example, given a  $(k-1)$ -step nilspace  $X$ , the results here will allow us to describe all possible  $k$ -step nilspaces such that their  $(k-1)$ -factor is equal to  $X$ . The object that encodes all the information needed to extend a nilspace is the following:

**Definition 5.33** (Cocycle). Let  $X$  be a nilspace,  $Z$  an abelian group, and  $k \geq -1$  an integer. A cocycle of degree  $k$  is a function  $\rho : C^{k+1}(X) \rightarrow Z$  that satisfies the following conditions:

- If  $\theta : \llbracket k+1 \rrbracket \rightarrow \llbracket k+1 \rrbracket$  is an invertible discrete-cube morphism and  $c \in C^{k+1}(X)$ , then  $\rho(c \circ \theta) = (-1)^{|\theta(0^{k+1})|} \rho(c)$  where  $|\theta(0^{k+1})| := \sum_{i=1}^{k+1} \theta(0^{k+1})(i)$ .

- If  $c_1, c_2 \in C^{k+1}(X)$  are 1-adjacent<sup>2</sup>, then  $\rho(c_1 \prec_1 c_2) = \rho(c_1) + \rho(c_2)$ .

The precise way of constructing an extension is the following:

**Definition 5.34.** Let  $X$  be a  $(k-1)$ -step nilspace,  $Z$  an abelian group, and  $\rho : C^{k+1}(X) \rightarrow Z$  a degree  $k$  cocycle. Let us define  $M = M(\rho)$  as follows:

$$M := \bigsqcup_{x \in X} \{\rho_x + z : z \in Z\}$$

where  $\rho_x$  is the restriction of  $\rho$  to the set  $C_x^{k+1}(X) := \{c \in C^{k+1}(X) : c(0^{k+1}) = x\}$ . We also define the map  $\tilde{\pi} : M \rightarrow X$  by  $\rho_x + z \mapsto x$  and the action of  $Z$  over  $M$  as  $(\rho_x + z, z') \mapsto \rho_x + z + z'$ . The set of cubes  $C^n(M)$  is defined as follows.

- If  $n \leq k$  then a function  $c \in M^{\llbracket n \rrbracket}$  is in  $C^n(M)$  if and only if  $\tilde{\pi} \circ c \in C^n(X)$ .
- If  $n > k$  then a function  $c \in M^{\llbracket n \rrbracket}$  is in  $C^n(M)$  if and only if  $\tilde{\pi} \circ c \in C^n(X)$  and for every face map  $\phi : \llbracket k+1 \rrbracket \rightarrow \llbracket n \rrbracket$  we have that  $\rho(\tilde{\pi} \circ c \circ \phi) = \sigma_{k+1}(\rho_{\tilde{\pi} \circ c \circ \phi} - c \circ \phi)$ .

Then, by [9, Proposition 3.3.26], we have the following result:

**Proposition 5.35.** *With the same hypothesis as above, the set  $M$  with its set of cubes  $C^n(M)$  is a  $k$ -step nilspace. Moreover, the  $k$ -th structure group is  $Z$  and the  $(k-1)$ -factor is  $X$ .*

For a fixed  $(k-1)$ -step nilspace and abelian group  $Z$ , not all cocycles define a genuinely different nilspace (up to isomorphism). However, we can isolate such cocycles that produce the same nilspace.

**Definition 5.36** (Coboundary). Let  $X$  be a  $(k-1)$ -step nilspace and  $Z$  an abelian group. A degree  $k$  cocycle  $\rho : C^{k+1}(X) \rightarrow Z$  is a coboundary if there exists a function  $f : X \rightarrow Z$  such that  $\rho(c) = \sum_{v \in \llbracket k+1 \rrbracket} (-1)^{|v|} f(c(v))$ .

The proof of the following result can be found in [9, Corollary 3.3.29]:

---

<sup>2</sup>See Definition A.14 and Lemma A.15.

**Proposition 5.37.** *Let  $X$  be a  $(k-1)$ -step nilspace and  $Z$  an abelian group. Let also  $\rho_1, \rho_2 : C^{k+1}(X) \rightarrow Z$  be two cocycles. Then the extensions  $M(\rho_1)$  and  $M(\rho_2)$  are isomorphic if and only if  $\rho_1 - \rho_2$  is a coboundary.*

Any  $k$ -step nilspace can be regarded as an extension of its  $(k-1)$ -factor by some cocycle. That is, given a  $k$ -step nilspace  $X$ , there exists a cocycle  $\rho : C^{k+1}(X_{k-1}) \rightarrow Z_k$  such that the extension  $M(\rho)$  is isomorphic to  $X$ . To create this cocycle we need the following definition:

**Definition 5.38** (Cross-section). Let  $X$  be a  $k$ -step nilspace. A cross-section (depending on  $k$ ) is a function  $s : X_{k-1} \rightarrow X$  such that  $\pi_{k-1} \circ s = id$ .

*Remark 5.39.* Note that  $s$  need not be a morphism.

**Proposition 5.40.** *Let  $X$  be a  $k$ -step nilspace and  $s : X_{k-1} \rightarrow X$  a cross-section. Define  $f : X \rightarrow Z_k$  as  $y \mapsto (s \circ \pi_{k-1})(y) - y$  where  $Z_k$  is the  $k$ -th structure group of  $X$ . For any  $c \in C^{k+1}(X_{k-1})$  define  $\rho_s(c) := \sigma_{k+1}(f \circ c')$  where  $c' \in C^{k+1}(X)$  is any cube such that  $\pi_{k-1} \circ c' = c$ . Then  $\rho_s$  is a degree  $k$  cocycle and  $M(\rho_s)$  is isomorphic to  $X$ .*

*Proof.* See [9, Lemma 3.3.28]. □

### 5.2.5 Construction of nilspaces, translation groups and non-coset nilspaces

So far, we have presented the main ideas of [9] without giving any proof. Now with those tools, we are going to produce some explicit examples of many of the aforementioned concepts. First of all, we are going to present a small result that shows the importance of the translation group in deciding whether or not a nilspace is a coset nilspace.

**Definition 5.41** (Action of the translation group over  $C^n(X)$ ). Let  $X$  be a nilspace and  $n \geq 0$  an integer. We can define an action of the group  $C^n(\Theta(X))$  over the set  $C^n(X)$  as follows. Given an element  $\mathbf{d} = \mathbf{d}(v) \in C^n(\Theta(X))$  and  $c \in C^n(X)$ , we define the action  $\mathbf{d} \cdot c \in C^n(X)$  as  $(\mathbf{d} \cdot c)(v) := \mathbf{d}(v)(c(v))$  for  $v \in \llbracket n \rrbracket$ .

**Lemma 5.42.** *Let  $X$  be a nilspace. Then  $X$  is isomorphic to a coset nilspace  $G/\Gamma$  for some filtered group  $G$  and some subgroup  $\Gamma \leq G$  if and only if  $C^n(\Theta(X))$  acts transitively on  $C^n(X)$  for all  $n \geq 0$ .*

*Proof.* The *only if* direction is trivial. For the converse, fix an element  $e \in X$  and take

$$\Gamma := \{\alpha \in \Theta(X) : \alpha(e) = e\}$$

the stabilizer of  $e$ . Let  $\pi_\Gamma : \Theta(X) \rightarrow \Theta(X)/\Gamma$ ,  $\alpha \mapsto \alpha\Gamma$  be the canonical projection. Then we claim that the following is a nilspace isomorphism between  $X$  and  $\Theta(X)/\Gamma$ :

$$\begin{aligned} \varphi : \Theta(X)/\Gamma &\rightarrow X \\ \alpha\Gamma &\rightarrow \alpha(e). \end{aligned}$$

This is well-defined by the definition of  $\Gamma$ . The fact that it is bijective is easy to check: if  $\alpha(e) = \beta(e)$ , it is clear that  $\alpha\Gamma = \beta\Gamma$ ; and the transitivity of  $C^0(\Theta(X)) = \Theta(X)$  over  $C^0(X) = X$  ensures that  $\varphi$  is also surjective.

To check that  $\varphi$  is a morphism, recall by Definition 5.41 the action of  $C^n(\Theta(X))$  on  $C^n(X)$ . For any  $\mathbf{d} \in C^n(\Theta(X))$ ,  $\varphi \circ \pi_\Gamma \circ \mathbf{d} = \mathbf{d} \cdot e_n \in C^n(X)$  where  $e_n \in C^n(X)$  is the constant cube  $e_n(v) = e \in X$  for all  $v \in \llbracket n \rrbracket$ . To see that  $\varphi^{-1}$  is also a morphism, take a cube  $c \in C^n(X)$  which, by transitivity of  $C^n(\Theta(X))$  over  $C^n(X)$  can be expressed as  $c = \mathbf{d} \cdot e_n$  for some  $\mathbf{d} \in C^n(\Theta(X))$ . Thus  $\varphi^{-1} \circ c = \varphi^{-1} \circ (\mathbf{d} \cdot e_n) = \pi_\Gamma \circ \mathbf{d} \in C^n(\Theta(X)/\Gamma)$ .  $\square$

Now we are going to use all that we have seen so far to study all possible 2-step nilspaces that have  $\mathcal{D}_1(\mathbb{Z}_2)$  as their 1-factor. By our results with cocycles, it suffices to analyse what are the possible cocycles  $C^3(\mathcal{D}_1(\mathbb{Z}_2)) \rightarrow Z$  for  $Z$  any abelian group. The defining properties in Definition 5.33 force that  $\rho(c) = 0$  for almost every  $c \in C^3(\mathcal{D}_1(\mathbb{Z}_2))$ . The reason is that if  $c \in C^3(\mathcal{D}_1(\mathbb{Z}_2))$  is  $i$ -adjacent with itself for some  $i = 1, 2$ , or  $3$ , then by the second property of Definition 5.33 (together with an application of a discrete-cube isomorphism), we have  $\rho(c) = \rho(c \prec_1 c) = \rho(c) + \rho(c)$ . There are only two cubes that can have a non-trivial value. One of them is  $c^* \in C^3(\mathcal{D}_1(\mathbb{Z}_2))$  defined by  $c^*(v) := v(1) + v(2) + v(3)$  and the other is  $c^* + 1$ . As they are 1-adjacent, we know that  $\rho(c^*) + \rho(c^* + 1) = 0$  (because its concatenation is one of the cubes that are forced to have value 0 through  $\rho$ ).

Therefore, any cocycle in this case is defined by the value of (say)  $\rho(c^*) = z^* \in Z$ . We will denote this cocycle by  $\rho^{z^*}$ . This gives us all possible cocycles, but recall that by Proposition 5.37, not all of them give us different nilspaces. Any addition of a coboundary will result in the same nilspace. The possible coboundaries are very easy to compute, just take any  $f :$

$\mathbb{Z}_2 \rightarrow Z$  and define  $\rho^f(c) := \sum_{v \in \llbracket 3 \rrbracket} (-1)^{|v|} f(c(v))$ . Therefore, all extensions arising for the cocycle  $\rho^{z^*}$  are isomorphic to the extensions arising from  $\rho^{z^*} + \rho^f$  for any  $f$ . As the value of  $\rho^{z^*}$  is determined by the value at  $c^*$ , and  $\rho^f(c^*) = 4(f(0) - f(1))$ , we have the following result:

**Proposition 5.43.** *Fix an abelian group  $Z$  and define  $g : Z \rightarrow Z$  by  $z \mapsto 4z$ . Then, all possible 2-step nilspaces with structure groups  $Z_1 = \mathbb{Z}_2$  and  $Z_2 = Z$  are in bijection with the set  $Z/\text{Im}(g)$ .*

A consequence of this result is for example that there exists only one 2-step nilspace with structure groups  $\mathbb{Z}_2$  and  $\mathbb{R}$ , namely  $\mathcal{D}_1(\mathbb{Z}_2) \times \mathcal{D}_2(\mathbb{R})$ .

Now we are going to compute explicitly the translation group of all these nilspaces, and we will give a criterion to decide when the nilspace is indeed a coset nilspace. Let us call  $X$  the nilspace generated by the cocycle  $\rho^{z^*}$ . First of all, by [9, Lemma 3.2.37], we know that  $\Theta_2(X) = Z$ , i.e., any  $\tau \in \Theta_2(X)$  corresponds to an element  $a \in Z$  (so  $\tau = \tau_a$ ) and the action of this element is  $\rho_x^{z^*} + z \mapsto \rho_x^{z^*} + z + a$  for all  $x \in \mathbb{Z}_2$  and  $z \in Z$ .

To compute  $\Theta_1(X)$  we will rely on some auxiliary results. The first one is [9, Lemma 3.2.13]. In our case, this lemma implies that given a translation  $\alpha \in \Theta_1(X)$ , we just have to check that for any  $c \in C^3(X)$  and any face  $F$  of codimension 1 we have  $\alpha^F(c) \in C^3(X)$ . The other result needed is [9, Lemma 3.2.24]. In our case, it implies that translations are equivariant, i.e., that for any  $\alpha \in \Theta(X)$ ,  $z \in Z$ , and any  $m \in X$ , we have that  $\alpha(m + z) = \alpha(m) + z$ . Thus, it is enough to determine the value of  $\alpha(\rho_x^{z^*})$  for  $x = 0, 1$ .

As translations are fibrations (this can be easily seen using the mentioned results), we know that there will be (at most) two types of elements in  $\Theta_1(X)$ . Let us denote by  $\alpha_{a,b}$  the element of  $\Theta_1(X)$  such that

$$\alpha_{a,b}(\rho_x^{z^*}) = \begin{cases} \rho_1^{z^*} + a & \text{if } x = 0 \\ \rho_0^{z^*} + b & \text{if } x = 1 \end{cases}$$

(if it exists), and by  $\beta_{c,d}$  the element of  $\Theta_1(X)$  such that

$$\beta_{c,d}(\rho_x^{z^*}) = \begin{cases} \rho_0^{z^*} + c & \text{if } x = 0 \\ \rho_1^{z^*} + d & \text{if } x = 1 \end{cases}$$

(if it exists). A priori, we do not know if all these elements are translations, we have to check that acting on faces of codimension 1 of 3-cubes results in cubes as well.

One can check that the elements  $\alpha_{a,b}$  are in  $\Theta_1(X)$  if and only if  $2a - 2b = z^*$ , and that  $\beta_{c,d} \in \Theta_1(X)$  if and only if  $2c - 2d = 0$ . The proof involves checking what happens if we apply these functions to all possible cubes that lie above all elements in  $C^3(\mathcal{D}_1(\mathbb{Z}_2))$ . As the latter is finite, this can be easily done. Therefore, the group  $\Theta(X)$  can be described as

$$\Theta_1(X) = \langle \alpha_{a,b}, \beta_{c,d} : a, b, c, d \in Z, 2a - 2b = z^* \text{ and } 2c - 2d = 0 \rangle,$$

$$\Theta_2(X) = \langle \beta_{c,c} : c \in Z \rangle,$$

and

$$\Theta_3(X) = \{\beta_{0,0} = id\}.$$

The relations of this group are:

$$\begin{aligned} \beta_{c,d} \circ \beta_{c',d'} &= \beta_{c+c',d+d'}, & \alpha_{a,b} \circ \alpha_{a',b'} &= \beta_{b+a',a+b'}, \\ \text{and } \beta_{c,d} \circ \alpha_{a,b} \circ \beta_{c',d'} &= \alpha_{c'+a+d,d'+b+c}. \end{aligned}$$

Let us highlight that if there is no element  $t \in Z$  such that  $2t = z^*$ , then none of the functions  $\alpha_{a,b}$  appear, and the group just consists of the  $\beta_{c,d}$  elements. Indeed, this observation is the key to prove the following result:

**Lemma 5.44.** *Let  $X, Z, z^*$ , and  $\rho^{z^*}$  be as above. Then the nilspace  $X$  is a coset nilspace if and only if there exists  $t \in Z$  such that  $2t = z^*$ .*

*Proof.* By Lemma 5.42, suppose that the action of  $C^n(\Theta(X))$  on  $C^n(X)$  is transitive. Then, starting with the constant cube equal to  $\rho_0^{z^*}$  we could reach any other cube, for example a cube  $c \in C^3(X)$  such that  $\tilde{\pi} \circ c = c^*$  (recall that this is the cube in  $C^3(\mathcal{D}_1(\mathbb{Z}_2))$  such that  $c^*(v) = v_1 + v_2 + v_3$ ). But to produce this cube starting from the constant  $\rho_0^{z^*}$  we must have used at least one of the functions  $\alpha_{a,b}$  because otherwise it is impossible to create something such that its image through  $\tilde{\pi}$  is different from 0. So this means that  $2a - 2b = 2(a - b) = z^*$  for that pair  $a, b \in Z$ .

Now, to prove the converse, by [9, Lemma 3.2.13] it is enough to check that we can create all possible elements of  $C^3(X)$ . As there exists a translation  $\alpha_{a,b}$  for some pair  $a, b \in Z$ , it is easy to check that starting with the constant cube equal to  $\rho_0^{z^*}$ , using only translations applied to faces of codimension 1, given any  $c \in C^3(\mathcal{D}_1(\mathbb{Z}_2))$  we can create a cube  $c' \in C^3(X)$  such that  $\tilde{\pi} \circ c' = c$ . Then, using Theorem 5.25 we can *correct* the last structure group using elements of  $\Theta_2(X)$ .  $\square$

**Corollary 5.45.** *The nilspace with the smallest step and number of elements which is not a coset nilspace is the extension of  $\mathcal{D}_1(\mathbb{Z}_2)$  by the group  $Z = \mathbb{Z}_2$  via the cocycle  $\rho^1$ .*

*Proof.* First of all, if we want to look for nilspaces that are not coset nilspaces, by Corollary 5.19 the step of the nilspace must be at least 2. Then, we have to discard the nilspaces that have 1,2 or 3 elements and any other nilspace with 4 elements. The nilspace with 1 element is a coset nilspace trivially. As 2-step nilspaces are degree-2 bundles, by Definition 5.24, if the nilspace has 2 (resp. 3) elements, then either  $Z_1$  or  $Z_2$  has 2 (resp. 3) elements. Therefore, the other structure group must be trivial and the nilspace will be  $\mathcal{D}_i(\mathbb{Z}_2)$  (resp.  $\mathcal{D}_i(\mathbb{Z}_3)$ ) for  $i = 1$  or  $2$ . If the nilspace has 4 elements, a similar argument as before shows that the only possible non-coset nilspace will come from a degree-2 bundle with structure groups  $\mathbb{Z}_2$  and  $\mathbb{Z}_2$ . We have computed all possibilities, and only one of them is not a coset nilspace.  $\square$

### 5.3 Topological and measure-theoretic aspects of nilspaces

In this section, we are going to equip nilspaces with a compact topology and a Haar measure. All the results here are not original, with the exception of Definition 5.70 and Theorem 5.71. The proof of the latter theorem uses results from Chapter 6, which chronologically was written before this chapter, but we have included it here because it is an extension of the inverse limit theorem.

**Definition 5.46** (Compact space). By a compact space we shall mean a compact, Hausdorff, second-countable topological space.

*Remark 5.47.* Compact spaces are metrizable, see [10, Remark 2.1.3].

**Definition 5.48.** A nilspace  $X$  is a compact nilspace if  $X$  is a compact space and  $C^n(X)$  is a closed subset of  $X^{[n]}$  with the product topology for all  $n \geq 0$ .

This may be compared with the concept of group and topological group. What we did in the previous section was to define nilspaces algebraically.

Here, we are going to give nilspaces a topology compatible with the structure of nilspace. The property of  $C^n(X)$  being closed is analogous to addition being continuous in topological groups.

Recall from Definition 5.23 and Definition 5.24 the definitions of abelian bundle,  $k$ -fold abelian bundle and degree- $k$  bundle.

**Definition 5.49** (Continuous abelian bundle). Let  $B$  be an abelian bundle over  $S$  with structure group  $Z$ . Let  $\pi : B \rightarrow S$  be its projection. We say that the bundle  $B$  is continuous if the following conditions hold:

- $B$  and  $S$  are topological spaces, and  $Z$  is an abelian topological group.
- The action  $\alpha : B \times Z \rightarrow B$  is continuous.
- $\pi$  is a continuous open map.

If  $B, S$ , and  $Z$  are compact spaces we call  $B$  a compact abelian bundle. A  $k$ -fold abelian bundle  $B_0, B_1, \dots, B_k$  is a compact  $k$ -fold abelian bundle if  $B_i$  is a compact abelian bundle over  $B_{i-1}$  for all  $i = 1, \dots, k$ .

**Definition 5.50** (Compact degree- $k$  bundle). A degree- $k$  bundle is a compact degree- $k$  bundle if it is also a compact  $k$ -fold abelian bundle.

### 5.3.1 Haar measure on compact abelian bundles

Nilspaces can be endowed with a probability measure that respects the operation of addition when we see the nilspace as an abelian bundle. This may be seen as the analogue for nilspaces of the Haar measure for groups (and indeed, it will be constructed using this Haar measure). We need the following definition:

**Definition 5.51** (Continuous system of measures). Let  $X$  and  $Y$  be compact spaces and  $\pi : X \rightarrow Y$  a continuous function. A continuous system of measures (CSM) on  $\pi$  is a set of Borel measures  $\{\mu_y : y \in Y\}$  on  $X$  such that:

- For every  $y \in Y$ ,  $\mu_y(\pi^{-1}(y)) = 1$ .
- For every continuous function  $f : X \rightarrow \mathbb{C}$ , the function  $Y \rightarrow \mathbb{C}$ ,  $y \mapsto \int_{\pi^{-1}(y)} f d\mu_y$  is continuous.

The idea is that if we are given also a measure in  $Y$ , we can construct a measure on  $X$ . The precise statement is:

**Lemma 5.52.** *Let  $X$  and  $Y$  be compact spaces and  $\{\mu_y : y \in Y\}$  a CSM of probability measures on the projection  $\pi : X \rightarrow Y$ . Let also  $\nu$  be a Borel probability measure on  $Y$ . Then we can define a measure  $\mu$  on  $X$  by the following formula, for every Borel set  $E \subset X$ :*

$$\mu(E) := \int_Y \mu_y(E) d\nu(y) = \int_Y \mu_y(E \cap \pi^{-1}(y)) d\nu(y).$$

*Remark 5.53.* The last equality emphasizes the fact that  $\mu_y$  is supported on  $\pi^{-1}(y)$  for any  $y \in Y$ .

*Proof.* See [10, Definition 2.2.9]. □

A 1-step nilspace  $X$  is essentially an abelian group. Thus, the usual Haar measure on  $X$  seen as a homogeneous space over an abelian group is the only measure that is invariant under addition. For a higher step, by induction, we are going to construct a Haar measure on the nilspace. Moreover, we will be able to construct a Haar measure on every compact abelian bundle.

**Lemma 5.54.** *Let  $B$  be a compact abelian bundle over  $S$  with structure group  $Z$ . Suppose that  $\mu_S$  is a regular Borel probability measure on  $S$ . Then there is a unique Borel probability measure  $\mu$  on  $B$  invariant under the action of  $Z$  and such that  $\mu_S = \mu \circ \pi^{-1}$ .*

*Proof.* See [10, Lemma 2.2.4]. □

Using this result, it is easy to prove the following (see [10, Proposition 2.2.5]):

**Proposition 5.55.** *Let  $B$  be a compact  $k$ -fold abelian bundle, with factors  $B_i$  for  $i = 0, \dots, k$  and structure groups  $Z_i$  for  $i = 1, \dots, k$ . Then there exists a unique regular Borel probability measure  $\mu$  on  $B$  such that if  $\pi_i : B \rightarrow B_i$  is the projection on the  $i$ -th factor, then  $\mu \circ \pi_i^{-1}$  is invariant under the action of  $Z_i$ .*

*Remark 5.56.* Recall that by Remark 5.26, we can also define a Haar measure on the set of cubes  $C^n(X)$  for every  $n \geq 0$ . This construction will be crucial for the theory of cubic couplings.

The Haar measure on compact abelian groups has other interesting properties. One of those is that it is preserved through continuous surjective homomorphisms. Recall from Definition 5.28 the concept of fibration. In the introduction, we mentioned that it was the analogue for nilspaces of surjective homomorphisms for groups. This analogy holds also in the case of preserving Haar measures. More generally, it holds for totally-surjective bundle morphisms between  $k$ -fold abelian bundles.

**Proposition 5.57.** *Let  $B$  and  $B'$  be compact  $k$ -fold abelian bundles and  $\phi : B \rightarrow B'$  be a continuous totally-surjective bundle morphism. Then  $\phi$  preserves the Haar measure, i.e.,  $\mu_{B'} = \mu_B \circ \phi^{-1}$ .*

*Proof.* See [10, Lemma 2.2.6]. □

*Remark 5.58.* In particular, fibrations preserve the Haar measure of nilspaces.

*Remark 5.59.* Using Proposition 5.57, it is easy to check that if  $\phi : B \rightarrow B'$  is a continuous totally-surjective bundle morphism between compact  $k$ -fold abelian bundles  $B$  and  $B'$ , and  $g \in L^1(B')$ , then  $\int_{B'} g d\mu_{B'} = \int_B g \circ \phi d\mu_B$ .

With the same hypothesis as above, given any  $t \in B'$  we have that  $\phi^{-1}(t)$  is a compact  $k$ -fold abelian bundle (see [9, Lemma 3.3.6]). Thus we can define a Haar measure on it for every  $t \in B'$ . We then have the quotient integral formula for abelian bundles:

**Proposition 5.60** (Quotient integral formula). *Let  $B$  and  $B'$  be compact  $k$ -fold abelian bundles. Let  $\phi : B \rightarrow B'$  be a continuous totally-surjective bundle morphism, and for every  $t \in B'$ , denote by  $\mu_t$  the Haar measure on  $\phi^{-1}(t)$ . Then for every function  $f \in L^1(B)$  we have*

$$\int_B f d\mu = \int_{B'} \int_{\phi^{-1}(t)} f d\mu_t d\mu_{B'}.$$

*Proof.* See [10, Lemma 2.2.10] and combine it with the regular approximation of  $L^1$  functions by characteristic functions, then simple functions, etcetera. □

### 5.3.2 Topology of abelian bundles associated with a continuous system of measures

Recall that by Proposition 5.35, given a  $(k-1)$ -step nilspace  $X$  and a cocycle  $\rho : C^{k+1}(X) \rightarrow Z$ , we were able to define a nilspace  $M(\rho)$  such that its  $(k-1)$ -factor is  $X$  and its  $k$ -th structure group is  $Z$ . Now we would like to equip  $M(\rho)$  with a topology that makes it a compact nilspace. Moreover, by Proposition 5.40, given a  $k$ -step nilspace  $Y$ , we were able to express it as the extension of  $Y_{k-1}$  by some cocycle  $\rho'_s : C^{k+1}(Y_{k-1}) \rightarrow Z_k(Y)$  where  $s : Y_{k-1} \rightarrow Z_k(Y)$  was a cross-section. This was a purely algebraic construction, and now we would like the isomorphism between  $Y$  and  $M(\rho')$  to be also a homeomorphism.

The way we constructed  $\rho'_s$  give us a clue on how regular can we expect a cocycle to be. Recall that  $s : Y_{k-1} \rightarrow Z_k(Y)$  was any function such that  $\pi_{k-1} \circ s = id$ . If we consider now  $Y$  to be a compact nilspace, we know that  $\pi_{k-1}$  is continuous and by [10, Lemma 2.4.5], we know that then there always exists a Borel cross-section  $s$ , and the corresponding cocycle  $\rho'_s$  is also Borel measurable.

Therefore, the ingredients we are given are a  $(k-1)$ -step nilspace  $X$ , a compact abelian group  $Z$ , and a Borel measurable cocycle  $\rho : C^{k+1}(X) \rightarrow Z$ . The process of giving a topology to  $M(\rho) = \bigsqcup_{x \in X} \{\rho_x + z : z \in Z\}$  consists roughly in creating a larger space  $\mathcal{L}(C^{k+1}(X), Z)$ , and giving  $M(\rho) \subset \mathcal{L}(C^{k+1}(X), Z)$  the subspace topology (see [10, Proposition 2.4.2]). The details can be found in [10, pp. 20 - 33]. We define the spaces  $\mathcal{L}(V, Z)$  and their topology as follows.

**Definition 5.61.** Let  $X, Y$  be compact spaces and  $\mu$  be a Borel measure on  $X$ . We denote by  $L(X, Y)$  the set of Borel functions  $f : X \rightarrow Y$  modulo the equivalence relation  $f \sim g$  if and only if  $\mu(\{f(x) \neq g(x) : x \in X\}) = 0$ .

**Definition 5.62.** Let  $V, W$  and  $Z$  be compact spaces, and let  $\pi : V \rightarrow W$  be a continuous map. Let  $\{\mu_w : w \in W\}$  be a family of strictly positive probability measures forming a CSM on  $\pi$ . Let us define

$$\mathcal{L}(V, Z) := \bigsqcup_{w \in W} L(\pi^{-1}(w), Z).$$

For any  $f \in \mathcal{L}(V, Z)$ , we define  $\tilde{\pi} : \mathcal{L}(V, Z) \rightarrow W$  as  $\tilde{\pi}(f) \mapsto w$  where  $w \in W$  is the unique element such that  $f \in L(\pi^{-1}(w), Z)$ . The topology

we give to  $\mathcal{L}(V, Z)$  is the coarsest such that all the following functionals are continuous:

$$\varphi_{F_1, F_2} : f \mapsto \int_{\pi^{-1}(\tilde{\pi}(f))} F_1(f(v))F_2(v)d\mu_{\tilde{\pi}(f)}(v)$$

where  $F_1 : Z \rightarrow \mathbb{C}$  and  $F_2 : V \rightarrow \mathbb{C}$  are continuous functions.

**Proposition 5.63.** *The topological space  $\mathcal{L}(V, Z)$  is regular, Hausdorff, and second-countable. The map  $\tilde{\pi}$  is continuous.*

*Proof.* See [10, Proposition 2.3.3]. □

Let us close this subsection by stating the result of automatic continuity:

**Theorem 5.64.** *Let  $X, Y$  be compact nilspaces of finite step. Let also  $\phi : X \rightarrow Y$  be a Borel measurable morphism between them. Then  $\phi$  is continuous.*

*Proof.* See [10, Theorem 2.4.6]. □

This result is the analogue for nilspaces of [56, Theorem 1], which says that any Borel measurable homomorphism between compact groups is continuous.

### 5.3.3 Finite-rank nilspaces, inverse limit representation and rigidity of morphisms

Continuing our comparison of compact groups and compact nilspaces, let us recall the following classical theorem (see [44, Corollary 2.43]):

**Theorem 5.65.** *Any compact abelian group is the inverse limit of compact abelian Lie groups.*

Note that by [80, Theorem 5.2], any compact abelian Lie group is isomorphic to  $\mathbb{T}^l \times Z$  where  $l \geq 0$  is an integer and  $Z$  is a finite abelian group. The equivalent notion for nilspaces (and more generally, for abelian bundles) of a Lie group is the following:

**Definition 5.66** (Finite rank). Let  $B$  be a  $k$ -fold compact abelian bundle. We say that it is of finite rank if all its structure groups are abelian Lie groups.

The notion of an inverse system for nilspaces is the following:

**Definition 5.67** (Inverse system). Let  $X_i$  be a family of compact nilspaces for  $i \in \mathbb{N}$ , and let  $\phi_{i,j} : X_j \rightarrow X_i$  be morphisms for  $i, j \in \mathbb{N}$ ,  $i \leq j$ . We say that they form an inverse system if  $\phi_{i,i}$  is the identity map for all  $i \in \mathbb{N}$ , and for all positive integers  $i \leq j \leq l$ ,  $\phi_{i,l} = \phi_{i,j} \circ \phi_{j,l}$ . Furthermore, if all  $\phi_{i,j}$  are fibrations, then we will call the system strict.

**Lemma 5.68** (Inverse limit). Let  $X_i$  and  $\phi_{i,j} : X_i \rightarrow X_j$ , for  $i, j \in \mathbb{N}$   $i \leq j$ , be a strict inverse system. Define

$$X := \{(x_i)_{i \in \mathbb{N}} \in \prod_{i \in \mathbb{N}} X_i : \phi_{i,j}(x_j) = x_i, \text{ for all } i \leq j\},$$

and for every  $n \geq 0$ ,

$$C^n(X) := \{(c_i)_{i \in \mathbb{N}} \in \prod_{i \in \mathbb{N}} C^n(X_i) : \phi_{i,j} \circ c_j = c_i, \text{ for all } i \leq j\}.$$

Then  $X$ , with the set of cubes  $C^n(X)$ , is a compact nilspace, and it will be denoted by  $\varprojlim_i X_i$ . Furthermore,  $X$  is  $k$ -step if and only if  $X_i$  is  $k$ -step for all  $i \in \mathbb{N}$ .

*Proof.* See [10, Lemma 2.7.2]. □

In particular, any inverse limit of finite-rank nilspaces is a compact nilspace. Moreover, any compact nilspace can be expressed as such a limit.

**Theorem 5.69** (Inverse limit theorem). Let  $X$  be a  $k$ -step compact nilspace. Then  $X$  is the inverse limit of finite-rank compact nilspaces.

*Proof.* See [10, Theorem 2.7.3]. □

To conclude this subsection, we are going to prove a version of this theorem for a particular class of nilspaces.

**Definition 5.70** (Inverse factor nilspaces). Let  $X$  be a compact nilspace. We say that it is an inverse factor nilspace if  $X = \varprojlim_i X_i$ , where  $X_i$  are the characteristic factors of  $X$ , and  $\phi_{i,j} = \pi_{i,j}$  are the projections to the characteristic factors.

This class of nilspaces will be very useful later for the structural description of cubic couplings. We have the following result:

**Theorem 5.71.** *Let  $X$  be an inverse factor compact nilspace. Then  $X = \varprojlim_i Y_i$  where  $Y_j$  are  $j$ -step finite-rank compact nilspaces for all  $j \geq 1$ .*

*Remark 5.72.* Note that the result does not follow from the inverse limit theorem. If we apply it, we would have that  $X = \varprojlim_i \varprojlim_j X_{i,j}$  where  $X_{i,j}$  are finite-rank  $i$ -step nilspaces. We claim that we can *glue* those factors together in a single inverse limit.

*Proof.* We will use a small result that follows from some results of Chapter 6:

**Claim:** Let  $Q, N$  be  $k$ -step compact nilspaces with  $N$  of finite rank, and let  $\varphi : Q \rightarrow N$  be a fibration. Let also  $(Q_i)_{i \geq 1}$  be a strict inverse system such that  $Q = \varprojlim_i Q_i$  with projections  $\phi_j : Q \rightarrow Q_j$ . Then, there exists a constant  $M = M((Q_i)_{i \geq 1}, N, \varphi) > 0$  such that, for any  $j \geq M$ , there exists a fibration  $\lambda_j : Q_j \rightarrow N$  with  $\varphi = \lambda_j \circ \phi_j$ .

*Proof of the Claim.* It follows from the proof of Theorem 6.7 that for some  $M \geq 1$ , there exists a morphism  $\lambda_M : Q_M \rightarrow N$  such that  $\varphi = \lambda_M \circ \phi_M$ . Arguing as in the proof of Lemma 6.15, we can conclude that  $\lambda_M$  is also a fibration. To prove that this is valid for any  $j \geq M$ , just take  $\lambda_j := \lambda_M \circ \phi_{M,j}$  where  $\phi_{M,j} : Q_j \rightarrow Q_M$  are the fibrations of the strict inverse system.  $\square$

For any  $k$ -step nilspace  $Q_k$  and any  $j \in \{0, \dots, k\}$ , let us denote by  $\pi_{j,k} : Q_k \rightarrow Q_j$  the projection to the  $j$ -factor. By definition of  $X$ , we have that  $X = \varprojlim_i X_i$ , where  $X_i$  is the  $i$ -factor of  $X$ , and  $\pi_{i,j} : X_j \rightarrow X_i$  are the fibrations of the strict inverse system (for  $j \geq i$ ). By the inverse limit theorem, each  $X_i$  can be expressed as the strict inverse limit of finite-rank  $i$ -step compact nilspaces,  $X_i = \varprojlim_j X_{i,j}$ . Let us denote by  $\phi_j^{(i)} : X_i \rightarrow X_{i,j}$  the projections to the factors given by the inverse limit. Similarly, let  $\phi_{j,l}^{(i)} : X_{i,l} \rightarrow X_{i,j}$ , for  $i \in \mathbb{N}$  and  $j \leq l$ , be the fibrations of the inverse system.

Imagine that we know that there exists fibrations  $\varphi_{i,j} : X_{i+1,j} \rightarrow X_{i,j}$  for all  $i, j \in \mathbb{N}$  such that the following diagram commutes:

$$\begin{array}{ccc}
 X_{i+1,j} & \xleftarrow{\phi_{j,j+1}^{(i+1)}} & X_{i+1,j+1} \\
 \varphi_{i,j} \downarrow & & \searrow \varphi_{i,j+1} \\
 X_{i,j} & \xleftarrow{\phi_{j,j+1}^{(i)}} & X_{i,j+1} .
 \end{array}$$

Then, it is clear that we could take the diagonal  $X_{i,i}$ , and  $\phi_{i,i+1}^{(i)} \circ \varphi_{i,i+1} : X_{i+1,i+1} \rightarrow X_{i,i}$  for  $i \in \mathbb{N}$  as our strict inverse system and the result would be proved.

We are going to prove that we can represent  $X_i$  as the inverse limit of some factors  $Y_{i,j}$  for all  $i, j \in \mathbb{N}$  such that the previous fibrations  $\varphi$  exist. First, take  $Y_{1,j} = X_{1,j}$  for all  $j \in \mathbb{N}$  (so  $X_1$  will be represented as the same inverse limit given by the inverse limit theorem). Now, to create  $Y_{2,1}$  we do the following. Consider the fibration  $\phi_1^{(1)} \circ \pi_{2,1} : X_2 \rightarrow X_{1,1}$ . By our **Claim**, we know that there exists a fibration  $\varphi_{1,1} : X_{2,j_1} \rightarrow X_{1,1}$ , for some  $j_1 \geq 1$ , such that  $\phi_1^{(1)} \circ \pi_{2,1} = \varphi_{1,1} \circ \phi_{j_1}^{(2)}$ . Thus, we define  $Y_{2,1} := X_{2,j_1}$ .

Let us now show how we can create the factor  $Y_{2,2}$ . Consider the map  $\phi_{j_1+1}^{(2)} : X_2 \rightarrow X_{2,j_1+1}$ . We have the following diagram

$$\begin{array}{ccc}
 X_2 & \xrightarrow{\phi_{j_1+1}^{(2)}} & X_{2,j_1+1} \\
 \pi_{1,2} \downarrow & & \searrow \pi_{1,2} \\
 X_1 & \xrightarrow{(\phi_{j_1+1}^{(2)})_1} & \pi_1(X_{2,j_1+1}) \\
 \phi_{l_2}^{(1)} \downarrow & & \nearrow \lambda \\
 X_{1,l_2} & & 
 \end{array}$$

Recall that  $(\phi_{j_1+1}^{(2)})_1$  is the induced morphism between the 1-factors of  $X_2$  and  $X_{2,j_1+1}$ . This map is equal to  $\lambda \circ \phi_{l_2}^{(1)}$  for some  $l_2 \geq 2$  and some fibration  $\lambda$  (by our **Claim**). Now we can apply Lemma 6.17 with the values

$$\begin{aligned}
 X &= X_2, & Y &= X_{2,j_1+1}, & W &= X_{1,l_2}, & \psi_1 &= \phi_{j_1+1}^{(2)}, \\
 \psi_2 &= \phi_{l_2}^{(1)} \circ \pi_{1,2}, & \text{and} & & \psi_3 &= \lambda.
 \end{aligned}$$

Let us denote the resulting fiber product of  $X_{2,j_1+1}$  with  $X_{1,l_2}$  by

$$X_{2,j_1+1} \times_{\pi_1(X_{2,j_1+1})} X_{1,l_2}.$$

It is then easy to see by our **Claim** that we can factorize this by an element of the inverse limit of  $\varprojlim_j X_{2,j}$ . This is, for some  $j_2 \geq j_1 + 1$ , there exists a fibration  $\gamma : X_{2,j_2} \rightarrow X_{2,j_1+1} \times_{\pi_1(X_{2,j_1+1})} X_{1,l_2}$  such that  $\Delta(\phi_{j_1}^{(2)}, \phi_{l_2}^{(1)} \circ \pi_{1,2}) = \gamma \circ \phi_{j_2}^{(2)}$  (for the notation  $\Delta(\cdot, \cdot)$  see Definition 6.14). To conclude, define  $Y_{2,2} := X_{2,j_2}$  and  $\varphi_{2,2} : Y_{2,2} \rightarrow Y_{1,2}$ ,  $\varphi_{2,2} := \phi_{2,l_2}^{(1)} \circ p_2 \circ \gamma$ , where  $p_2 : X_{2,j_1+1} \times_{\pi_1(X_{2,j_1+1})} X_{1,l_2} \rightarrow X_{1,l_2}$  is the projection to the second coordinate. It is then straightforward to check that this construction works.

Repeating this argument is easy to see that we can create a whole family of factors  $Y_{i,j}$  with the desired properties.  $\square$

Let us now close this subsection with another result. This one will be used in the proof of the inverse theorem and the regularity lemma.

**Definition 5.73** ( $\varepsilon$ -modification). Let  $X$  be a set,  $(Y, d)$  a metric space, and  $\varepsilon > 0$  a constant. If we have two maps  $\psi, \psi' : X \rightarrow Y$ , we say that  $\psi'$  is an  $\varepsilon$ -modification of  $\psi$  if  $d(\psi(x), \psi'(x)) \leq \varepsilon$  for all  $x \in X$ .

**Definition 5.74** ( $\delta$ -quasimorphism). Let  $X$  be a compact nilspace,  $Y$  a compact  $k$ -step nilspace with some metric  $d$  generating its topology, and  $\delta > 0$ . We say that  $\phi : X \rightarrow Y$  is a  $\delta$ -quasimorphism if for every cube  $c \in \mathcal{C}^{k+1}(X)$ , there exists  $c' \in \mathcal{C}^{k+1}(Y)$  such that  $d((\phi \circ c)(v), c'(v)) \leq \delta$  for all  $v \in \llbracket k+1 \rrbracket$ .

**Lemma 5.75** (Rigidity of morphisms). *Let  $X$  be a  $k$ -step compact nilspace with a fixed metric  $d$ . For every  $\varepsilon > 0$  there exists  $\delta = \delta(\varepsilon, X) > 0$  such that for every  $\delta$ -quasimorphism there exists an  $\varepsilon$ -modification which is a continuous morphism.*

*Proof.* See [10, Theorem 2.8.2].  $\square$

### 5.3.4 Toral nilspaces

Recall that in the previous section, we were interested in deciding whether a nilspace was a coset nilspace and that the group of translations played an important role in that task. Now, we are going to study what happens if we

have additional topological information about the nilspace. Toral nilspaces would be a subclass of nilspaces which are always coset nilspaces. For the rest of the section, we are going to abbreviate “compact and finite-rank” by CFR.

Let us start by defining a topology for the group of translations.

**Definition 5.76.** Let  $X$  be a CFR  $k$ -step nilspace and  $d$  a metric that generates its topology. For every  $i = 1, \dots, k$ , the group  $\Theta_i(X)$  will be equipped with the restriction of the uniform metric on  $C(X, X)$  ( $d_\infty(f, g) = \sup_{x \in X}(f(x), g(x))$  for all  $f, g \in C(X, X)$ ).

*Remark 5.77.* By [10, Lemma 2.9.2], this definition makes  $\Theta_i(X)$  a Polish group.

Moreover, we can prove the following about the translation groups:

**Lemma 5.78.** *Let  $X$  be a CFR  $k$ -step nilspace. For any  $i = 1, \dots, k$  the group  $\Theta_i(X)$  is a Lie group.*

*Proof.* See [10, Theorem 2.9.10]. □

The following definition is the main one in this subsection:

**Definition 5.79** (Toral nilspaces). Let  $X$  be a CFR  $k$ -step nilspace. We say that it is a toral nilspace if all its structure groups are connected.

*Remark 5.80.* This was proved to be equivalent to the fact that all cube sets  $C^n(X)$  are connected for all  $n \geq 0$  in [42, Theorem 1.22], where they call this class of nilspaces *strongly connected*. Furthermore, it was proved in [18, Theorem 1.9] that it is equivalent to the set  $C^k(X)$  being connected.

For any topological group  $G$ , let us define  $G^0$  as the connected component that contains the identity element. Then the main result of this subsection is the following:

**Theorem 5.81.** *Let  $X$  be CFR  $k$ -step toral nilspace. Then  $X$  is the coset nilspace  $G^0/\Gamma$ , where  $G = \Theta(X)$ ,  $G_\bullet = (\Theta_i(X)^0)_{i=0}^\infty$ , and  $\Gamma = \text{Stab}_G(x)$  for any fixed  $x \in X$ .*

*Proof.* See [10, Theorem 2.9.17]. □

## 5.4 Cubic couplings

In this section, almost all results and definitions appeared originally in [17, 18]. The only original part (and the only result with an actual proof) is Lemma 5.108.

### 5.4.1 Results in measure theory

First, let us recall some notions in measure theory that will be used throughout the rest of the section.

**Definition 5.82** (Conditional expectation). Let  $(\Omega, \mathcal{A}, \mu)$  be a probability space, and let  $\mathcal{B} \subset \mathcal{A}$  be a sub- $\sigma$ -algebra. Given a function  $f \in L^1(\mathcal{A})$ , we define the conditional expectation  $\mathbb{E}(f|\mathcal{B})$  as the unique  $\mathcal{B}$ -measurable function (a.s.) such that

$$\int_A f d\mu = \int_A \mathbb{E}(f|\mathcal{B}) d\mu$$

for all  $A \in \mathcal{B}$ .

The following are well known facts about the conditional expectation:

**Proposition 5.83.** *Let  $(\Omega, \mathcal{A}, \mu)$  be a probability space, and let  $\mathcal{B} \subset \mathcal{A}$  be a sub- $\sigma$ -algebra. Then the following holds:*

- For any  $f \in L^1(\mathcal{A})$ , the conditional expectation  $\mathbb{E}(f|\mathcal{B})$  exists, is unique<sup>3</sup>, and is in  $L^1(\mathcal{B})$  (This can be seen using the Radon-Nikodym derivative).
- For any  $1 \leq p \leq \infty$ , if  $f \in L^p(\mathcal{A})$ , then  $\mathbb{E}(f|\mathcal{B}) \in L^p(\mathcal{B})$ .
- For any  $1 \leq p \leq \infty$ , the operator  $\mathbb{E}(\cdot|\mathcal{B}) : L^p(\mathcal{A}) \rightarrow L^p(\mathcal{B})$  is a bounded linear operator of norm 1.
- Let  $1 \leq p \leq \infty$  and  $\frac{1}{p} + \frac{1}{q} = 1$ . If  $f \in L^p(\mathcal{A})$ , then for any  $g \in L^q(\mathcal{B})$ ,

$$\int gf d\mu = \int g \mathbb{E}(f|\mathcal{B}) d\mu.$$

---

<sup>3</sup>As usual, up to null sets.

There exist two main operations with  $\sigma$ -algebras that we will need.

**Definition 5.84** (Join of  $\sigma$ -algebras). Let  $\mathcal{A}, \mathcal{B}$  be two  $\sigma$ -algebras on a set  $\Omega$ . The join  $\sigma$ -algebra, denoted by  $\mathcal{A} \vee \mathcal{B}$ , is defined as the smallest  $\sigma$ -algebra that includes  $\mathcal{A}$  and  $\mathcal{B}$ , namely  $\sigma(\mathcal{A} \cup \mathcal{B})$ .

**Definition 5.85** (Meet of  $\sigma$ -algebras). Let  $(\Omega, \mathcal{A}, \mu)$  be a probability space. Let  $\mathcal{B}_0, \mathcal{B}_1$  be two sub- $\sigma$ -algebras of  $\mathcal{A}$ . The meet of  $\mathcal{B}_0$  with  $\mathcal{B}_1$ , denoted by  $\mathcal{B}_0 \wedge_\mu \mathcal{B}_1$ , is the sub- $\sigma$ -algebra of elements  $A \in \mathcal{A}$  such that there exists  $B_0 \in \mathcal{B}_0$  and  $B_1 \in \mathcal{B}_1$  with  $\mu(B_0 \Delta A) = 0$  and  $\mu(B_1 \Delta A) = 0$ <sup>4</sup>.

When the measure  $\mu$  is clear from the context, we will just write  $\mathcal{B}_0 \wedge \mathcal{B}_1$ . It may be false that  $\mathcal{B}_0 \wedge \mathcal{B}_1 \subset \mathcal{B}_0$ , but the inclusion holds *up to null sets*. Given two  $\sigma$ -algebras  $\mathcal{B}, \mathcal{B}' \subset \mathcal{A}$  where  $(\Omega, \mathcal{A}, \mu)$  is a probability space, we say that  $\mathcal{B} \subset_\mu \mathcal{B}'$  if for every  $A \in \mathcal{B}$ , there exists  $A' \in \mathcal{B}'$  such that  $\mu(A \Delta A') = 0$ . We will say that  $\mathcal{B} =_\mu \mathcal{B}'$  if both  $\mathcal{B} \subset_\mu \mathcal{B}'$  and  $\mathcal{B}' \subset_\mu \mathcal{B}$  hold. Using this relation, it is true that  $\mathcal{B}_0 \wedge_\mu \mathcal{B}_1 \subset_\mu \mathcal{B}_0$ .

The concept of conditional independence will be very important in the sequel:

**Definition 5.86** (Conditional independence of two  $\sigma$ -algebras with respect to a third one). Let  $(\Omega, \mathcal{A}, \mu)$  be a probability space, and let  $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B} \subset \mathcal{A}$  be sub- $\sigma$ -algebras. We say that  $\mathcal{B}_0, \mathcal{B}_1$  are conditionally independent with respect to  $\mathcal{B}$  if one of the following equivalent statements holds:

- For any  $f_0 \in L^\infty(\mathcal{B}_0)$  and  $f_1 \in L^\infty(\mathcal{B}_1)$  we have

$$\mathbb{E}(f_0 f_1 | \mathcal{B}) = \mathbb{E}(f_0 | \mathcal{B}) \mathbb{E}(f_1 | \mathcal{B}).$$

- Let  $1 \leq p \leq \infty$ . For any  $f \in L^p(\mathcal{B}_1)$  we have

$$\mathbb{E}(f | \mathcal{B}_0 \vee \mathcal{B}) = \mathbb{E}(f | \mathcal{B}).$$

For a proof of the equivalence, see [17, Theorem 2.4]. As a special case of this definition, we define the following:

**Definition 5.87** (Conditional independence of two sub- $\sigma$ -algebras). Let  $(\Omega, \mathcal{A}, \mu)$  be a probability space, and let  $\mathcal{B}_0, \mathcal{B}_1 \subset \mathcal{A}$  be sub- $\sigma$ -algebras. We say that  $\mathcal{B}_0$  and  $\mathcal{B}_1$  are conditionally independent, and we will denote it by  $\mathcal{B}_0 \perp\!\!\!\perp_\mu \mathcal{B}_1$ , if  $\mathcal{B}_0$  and  $\mathcal{B}_1$  are conditionally independent with respect to  $\mathcal{B}_0 \wedge_\mu \mathcal{B}_1$ .

---

<sup>4</sup>Here  $\Delta$  stands for the symmetric difference,  $A \Delta B = (A \setminus B) \cup (B \setminus A)$ .

If the measure  $\mu$  is clear from the context, we will just write  $\mathcal{B}_0 \perp\!\!\!\perp \mathcal{B}_1$ .

A useful criterion to decide whether two  $\sigma$ -algebras are conditionally independent is the following:

**Proposition 5.88.** *Let  $(\Omega, \mathcal{A}, \mu)$  be a probability space, and let  $\mathcal{B}_0, \mathcal{B}_1 \subset \mathcal{A}$  be sub- $\sigma$ -algebras. Then the following are equivalent*

- $\mathcal{B}_0 \perp\!\!\!\perp_{\mu} \mathcal{B}_1$ .
- Let  $1 \leq p \leq \infty$  and  $i \in \{0, 1\}$ . For any  $f \in L^p(\mathcal{A})$  we have that

$$\mathbb{E}(\mathbb{E}(f|\mathcal{B}_i)|\mathcal{B}_{1-i}) = \mathbb{E}(f|\mathcal{B}_0 \wedge \mathcal{B}_1).$$

*Proof.* See [17, Proposition 2.10], and combine it with Proposition 5.83 and density arguments of  $L^\infty(\mathcal{A})$  inside  $L^p(\mathcal{A})$ .  $\square$

For the rest of the section, we will be interested in working with Borel probability spaces.

**Definition 5.89** (Borel probability spaces). Let  $(\Omega, \mathcal{A}, \mu)$  be a probability space. We will say it is a Borel probability space if there exists a Polish topology  $\tau$  on  $\Omega$  such that  $\mathcal{A}$  is the Borel  $\sigma$ -algebra generated by  $\tau$ ,  $\mathcal{A} = \sigma(\tau)$ .

*Remark 5.90.* The measure  $\mu$  of a Borel probability space is automatically regular [24, Proposition 8.1.12].

In order to define the cubes of the characteristic factors of a cubic coupling we will need the following definition:

**Definition 5.91** (Support of a Borel measure). Let  $(\Omega, \mathcal{A}, \mu)$  be a Borel probability space. The support of  $\mu$  is defined as the closed set  $\text{Supp}(\mu) := \{x \in \Omega : \text{for any neighborhood } U \text{ of } x, \mu(U) > 0\}$ .

Let us close this subsection stating a very useful fact:

**Proposition 5.92.** *Let  $(\Omega, \mathcal{A}, \mu)$  and  $(\Omega', \mathcal{A}', \mu')$  be probability spaces. Let also  $\phi : \Omega \rightarrow \Omega'$  be a measure-preserving surjective map and  $\mathcal{B} \subset \mathcal{A}'$  be a sub- $\sigma$ -algebra. Then for any  $f \in L^1(\mathcal{A}')$  we have that*

$$\mathbb{E}_{\mu'}(f|\mathcal{B}) \circ \phi = \mathbb{E}_{\mu}(f \circ \phi|\phi^{-1}\mathcal{B}).$$

*Proof.* It follows easily from the definition of conditional expectation. See also [17, Lemma 2.17].  $\square$

### 5.4.2 Couplings

Let us introduce an important definition (for a slightly more general one, see [17, Definition 2.18]):

**Definition 5.93** (Coupling). Let  $S$  be a finite set and  $(\Omega, \mathcal{A}, \lambda)$  be a probability space. A coupling (more precisely, a self-coupling of  $\lambda$  with index set  $S$ ) is a measure  $\mu$  on  $(\prod_{s \in S} \Omega, \bigvee_{s \in S} \mathcal{A}) = (\Omega^S, \mathcal{A}^S)$  such that if  $p_s : \Omega^S \rightarrow \Omega$  is the projection to the  $s$ -th coordinate, then  $\lambda = \mu \circ p_s^{-1}$  for all  $s \in S$ .

Note that if  $(\Omega, \mathcal{A}, \lambda)$  is a Borel probability space, then so is  $(\Omega^S, \mathcal{A}^S, \mu)$ . For the rest of the section,  $S$  will always stand for a finite set.

We are interested in defining a topology on the space of couplings. To do so, we need the following definition:

**Definition 5.94.** Let  $\mu$  be a coupling of  $\Omega^S$ . For any system of bounded measurable functions  $F = (f_s)_{s \in S}$ ,  $f_s : \Omega \rightarrow \mathbb{C}$ , we define the functionals  $\xi(\mu, F)$  as

$$\xi(\mu, F) := \int_{\Omega^S} \prod_{s \in S} f_s \circ p_s d\mu.$$

The following definition is a particular version of [17, Definition 2.20]:

**Definition 5.95** (Coupling space). Let  $(\Omega, \mathcal{A}, \lambda)$  be a probability space and  $S$  a finite set. Let us denote by  $\mathbf{Cg}(\Omega, S)$  the set of couplings of  $\Omega$  over  $S$  with the coarsest topology making the functionals  $\xi(\cdot, F)$  continuous for all systems of bounded measurable functions  $F = (f_s : \Omega \rightarrow \mathbb{C})_{s \in S}$ .

**Proposition 5.96.** *Let  $S$  be a finite set and  $(\Omega, \mathcal{A}, \lambda)$  be a Borel probability space. Then  $\mathbf{Cg}(\Omega, S)$  is a non-empty convex<sup>5</sup> compact Polish space.*

*Proof.* See [17, Proposition 2.21]. □

The next definition is [17, Definition 2.23]:

---

<sup>5</sup>This means that for every borel probability measure  $\nu$  on  $\mathbf{Cg}(\Omega, S)$ ,  $\int_{\mathbf{Cg}(\Omega, S)} \mu d\nu(\mu) \in \mathbf{Cg}(\Omega, S)$ .

**Definition 5.97** (Relative independence over a factor). Let  $(\Omega, \mathcal{A}, \lambda)$  be a probability space,  $S$  a finite set, and  $\mathcal{B} \subset \mathcal{A}$  a sub- $\sigma$ -algebra. Then we say that  $\mu$  is relatively independent over  $\mathcal{B}^S$  if for all systems of bounded measurable functions  $F = (f_s : \Omega \rightarrow \mathbb{C})_{s \in S}$ , we have that  $\xi(\mu, F) = \xi(\mu, G)$  where  $G = (\mathbb{E}(f_s | \mathcal{B}) : \Omega \rightarrow \mathbb{C})_{s \in S}$ .

Given a coupling  $\mu \in \mathbf{Cg}(\Omega, S)$ , sometimes it will be useful to restrict this measure to some  $T \subset S$ . This is the motivation for the following definition:

**Definition 5.98** (Subcoupling along sets). Let  $\mu \in \mathbf{Cg}(\Omega, S)$  and  $T \subset S$  be finite sets. The coupling  $\mu_T \in \mathbf{Cg}(\Omega, T)$  is defined as  $\mu \circ p_T^{-1}$  where  $p_T : \Omega^S \rightarrow \Omega^T$  is the projection to the  $T$ -th coordinates.

Let us also define now the sub- $\sigma$ -algebras  $\mathcal{A}_T^S := p_T^{-1}(\mathcal{A}^T)$  for any  $T \subset S$ . If  $T = \{t\}$  is a singleton, we will write  $\mathcal{A}_t^S$  instead of  $\mathcal{A}_{\{t\}}^S$ . With this, we can now state one of the most important definitions in [17], see [17, Definition 2.29].

**Definition 5.99** (Conditionally independent system of sets). Let  $\mu \in \mathbf{Cg}(\Omega, S)$  and  $T_1, T_2 \subset S$ . We will say that  $T_1, T_2$  are conditionally independent in  $\mu$  if  $\mathcal{A}_{T_1}^S \perp\!\!\!\perp_{\mu} \mathcal{A}_{T_2}^S$  and

$$\mathcal{A}_{T_1}^S \wedge_{\mu} \mathcal{A}_{T_2}^S =_{\mu} \mathcal{A}_{T_1 \cap T_2}^S.$$

In this case, we will write  $T_1 \perp_{\mu} T_2$ .

The next proposition is a useful criterion to determine when a pair of subsets is conditionally independent in a coupling.

**Proposition 5.100.** *Let  $\mu \in \mathbf{Cg}(\Omega, S)$  and  $T_1, T_2 \subset S$ . The following are equivalent:*

- $T_1 \perp_{\mu} T_2$ .
- Let  $1 \leq p \leq \infty$ . For any  $f \in L^p(\Omega^S)$  we have that

$$\mathbb{E}(\mathbb{E}(f | \mathcal{A}_{T_1}^S) | \mathcal{A}_{T_2}^S) = \mathbb{E}(f | \mathcal{A}_{T_1 \cap T_2}^S).$$

*Proof.* This follows from the proof of [17, Lemma 2.30]. □

One of the important consequences of Definition 5.99 is the following result.

**Definition 5.101** (Orthogonal coupling). Let  $S, S'$  be two sets, and  $\mu \in \mathbf{Cg}(\Omega, S)$  and  $\mu' \in \mathbf{Cg}(\Omega, S')$  be couplings such that  $\mu_{S \cap S'} = \mu'_{S \cap S'}$ . Then, there exists a unique coupling  $\nu \in \mathbf{Cg}(\Omega, S \cup S')$  such that  $\nu_S = \mu$ ,  $\nu_{S'} = \mu'$ , and  $S \perp_\nu S'$ . We will call  $\nu$  the orthogonal coupling of  $\mu$  and  $\mu'$ .

*Proof.* See [17, Definition 2.34 and Lemma 2.35]. □

The original result is a little stronger, but for this exposition, this is enough.

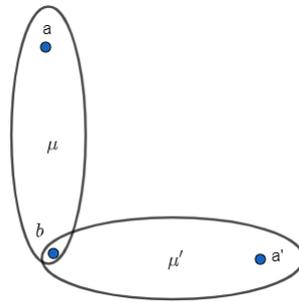
### 5.4.3 Idempotent couplings

The following definition is also one of the most important ones in [17], see [17, Definition 2.57].

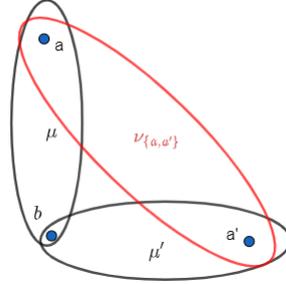
**Definition 5.102** (Idempotent coupling). Let  $\mu \in \mathbf{Cg}(\Omega, \{a, b\})$  be a coupling. Consider the coupling  $\mu' \in \mathbf{Cg}(\Omega, \{a', b\})$  defined by  $\mu' := \mu \circ T^{-1}$  where  $T : \Omega^{\{a, b\}} \rightarrow \Omega^{\{a', b\}}$ ,  $T(x(a), x(b))(a') = x(a)$ ,  $T(x(a), x(b))(b) = x(b)$ . Let  $\nu \in \mathbf{Cg}(\Omega, \{a, a', b\})$  be the orthogonal coupling of  $\mu$  and  $\mu'$ . Define now the map  $T^* : \Omega^{\{a, a'\}} \rightarrow \Omega^{\{a, b\}}$ ,  $T^*(x(a), x(a'))(a) = x(a)$ ,  $T^*(x(a), x(a'))(b) = x(a')$ . We will say that  $\mu$  is idempotent if

$$\nu_{\{a, a'\}} \circ (T^*)^{-1} = \mu.$$

Let us examine further this definition. The coupling  $\mu'$  is essentially  $\mu$ , we have just relabeled the first coordinate with another name to compute the orthogonal coupling. Thus, we have the following diagram



We know that under these conditions, there is always a unique orthogonal coupling  $\nu$  by Definition 5.101. The condition of being idempotent says that the diagonal coupling,  $\nu_{\{a,a'\}}$  is isomorphic to  $\mu$  (via a relabeling of the variables).



This should be compared with the discussion after Remark A.16, where we see how concatenations were another way of *taking diagonals*. Thus, the counterparts of concatenations for couplings are idempotent couplings. There is one significant difference between concatenations and idempotent couplings. The former is a consequence of the Composition and Completion axioms, whereas the latter is given as a definition. The main objective of [17] is to show that (in the sense of the characteristic factors), we can recover the Completion axiom from the idempotent condition. To make this possible we need the full definition of cubic coupling, see Definition 5.104 and Definition 5.105.

We have a nice characterization of idempotent couplings:

**Proposition 5.103.** *Let  $(\Omega, \mathcal{A}, \lambda)$  be a probability space, and let  $\mu$  be a coupling in  $\mathbf{Cg}(\Omega, \{a, b\})$ . Then the following are equivalent:*

- *The coupling  $\mu$  is idempotent.*
- *There exists a sub- $\sigma$ -algebra  $\mathcal{B} \subset \mathcal{A}$  such that*

$$\mu(A \times B) = \int_{\Omega} \mathbb{E}(1_A | \mathcal{B}) \mathbb{E}(1_B | \mathcal{B}) d\lambda$$

*for all  $A, B \in \mathcal{A}$ .*

*Proof.* See [17, Proposition 2.66]. □

### 5.4.4 Cubic couplings

Before stating the definition of cubic coupling, we need some technical notation. Let  $\phi : \llbracket m \rrbracket \rightarrow \llbracket n \rrbracket$  be an injective discrete-cube morphism. Given a coupling  $\mu \in \mathbf{Cg}(\Omega, \llbracket n \rrbracket)$ , where  $(\Omega, \mathcal{A}, \lambda)$  is a probability space, the morphism  $\phi$  induces a coupling  $\mu_\phi \in \mathbf{Cg}(\Omega, \llbracket m \rrbracket)$  as follows. Consider the projection  $p_\phi : \Omega^{\llbracket n \rrbracket} \rightarrow \Omega^{\llbracket m \rrbracket}$  where  $(p_\phi(\underline{x}))(i) = x(\phi(i))$ . We then define  $\mu_\phi := \mu \circ p_\phi^{-1}$ .

There are two equivalent definitions for cubic couplings ([17, Definition 3.1 and Definition 3.3]):

**Definition 5.104** (Cubic coupling). Let  $(\Omega, \mathcal{A}, \lambda)$  be a probability space and let  $(\mu^{\llbracket n \rrbracket} \in \mathbf{Cg}(\Omega, \llbracket n \rrbracket))_{n \geq 0}$  be a family of couplings. We say that it is a cubic coupling if the following conditions are satisfied:

1. Consistency: For any injective discrete-cube morphism  $\phi : \llbracket m \rrbracket \rightarrow \llbracket n \rrbracket$  we have  $\mu_\phi^{\llbracket n \rrbracket} = \mu^{\llbracket m \rrbracket}$ .
2. Ergodicity: The measure  $\mu^{\llbracket 1 \rrbracket}$  is  $\lambda \times \lambda$ .
3. Conditional independence:  $(\{0\} \times \llbracket n-1 \rrbracket) \perp_{\mu^{\llbracket n \rrbracket}} (\llbracket n-1 \rrbracket \times \{0\})$  for all  $n \geq 1$ .

**Definition 5.105** (Cubic coupling). Let  $(\Omega, \mathcal{A}, \lambda)$  be a probability space and let  $(\mu^{\llbracket n \rrbracket} \in \mathbf{Cg}(\Omega, \llbracket n \rrbracket))_{n \geq 0}$  be a family of couplings. We say that it is a cubic coupling if the following conditions are satisfied:

1. Face consistency: For any face map  $\phi : \llbracket m \rrbracket \rightarrow \llbracket n \rrbracket$  we have  $\mu_\phi^{\llbracket n \rrbracket} = \mu^{\llbracket m \rrbracket}$ .
2. Ergodicity: The measure  $\mu^{\llbracket 1 \rrbracket}$  is  $\lambda \times \lambda$ .
3. Idempotence: For any pair of opposite faces  $F_0, F_1 \subset \llbracket n \rrbracket$ , the coupling  $\mu^{\llbracket n \rrbracket}$  seen as an element of  $\mathbf{Cg}(\Omega^{\llbracket n-1 \rrbracket}, \{F_0, F_1\})$  is idempotent.

*Remark 5.106.* If  $((\Omega, \mathcal{A}, \lambda), (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  is a cubic coupling and  $(\Omega, \mathcal{A}, \lambda)$  is a Borel probability space, we say that  $((\Omega, \mathcal{A}, \lambda), (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  is a Borel cubic coupling.

For a proof of the equivalence, see [17, Lemma 3.4 and Lemma 3.5]. As an idea on how to prove that the second definition implies the first one (this

is the difficult implication), recall that the Idempotence axiom allows us to *take diagonals*. Thus, if we are given an injective discrete-cube morphism  $\phi : \llbracket n-1 \rrbracket \rightarrow \llbracket n \rrbracket$ , it is either a face map or it is the diagonal of two face maps. Using that idea, we can prove the Consistency axiom of the first definition using the Idempotence and Face consistency axioms (iterating that idea we can deal with general injective discrete-cube morphisms  $\phi : \llbracket m \rrbracket \rightarrow \llbracket n \rrbracket$ ).

For any  $k$ -step compact nilspace  $X$ , the family of Haar measures on  $C^n(X)$  define a cubic coupling. Recall that as  $C^n(X)$  is a  $k$ -fold abelian bundle, we can define a Haar measure  $\mu_{C^n(X)}$  for any  $n \geq 0$ , see Remark 5.56. The way of constructing a measure in  $X^{\llbracket n \rrbracket}$  is simple, take the inclusion  $i_n : C^n(X) \rightarrow X^{\llbracket n \rrbracket}$  and define  $\mu^{\llbracket n \rrbracket} := \mu_{C^n(X)} \circ i_n^{-1}$  for all  $n \geq 0$ . By abusing the notation, we will say that the Haar measure of  $X$  forms a self-coupling with index set  $\llbracket n \rrbracket$ , and we will denote it by  $\mu_{C^n(X)}$ .

**Proposition 5.107.** *Let  $X$  be a  $k$ -step compact nilspace. Then its Haar measures form a Borel cubic coupling.*

*Proof.* See [17, Proposition 3.6]. □

We can establish further relationships and analogies between the concepts of nilspaces and concepts of couplings. Recall the definition of *good pair* from Definition A.27.

**Lemma 5.108.** *Let  $P_0, P_1 \subset \llbracket n \rrbracket$  be a good pair. Then for any  $k$ -step compact nilspace  $X$ , the sets  $P_0, P_1$  are conditionally independent with respect to  $\mu_{C^n(X)}$ .*

*Proof.* Consider the map<sup>6</sup>

$$\begin{array}{ccc} \pi_{P_1} : \text{hom}(\llbracket n \rrbracket, X) & \rightarrow & \text{hom}(P_1, X) \\ \text{c} & \rightarrow & \text{c}|_{P_1}. \end{array}$$

which is measure preserving by Lemma A.28 and Proposition 5.57. Let  $\mathcal{A}$  be the  $\sigma$ -algebra generated by the topology of  $X$ . Given any  $f \in L^\infty(\mathcal{A}_{P_0}^{\llbracket n \rrbracket})$ , by Proposition 5.100, we have to check that  $\mathbb{E}(f|\mathcal{A}_{P_1}^{\llbracket n \rrbracket}) = \mathbb{E}(f|\mathcal{A}_{P_0 \cap P_1}^{\llbracket n \rrbracket})$ . Abusing the notation a little, we can assume that  $f$  is a function defined only in

---

<sup>6</sup>For the definitions of  $\text{hom}(P, X)$  and  $\text{hom}_f(P, X)$ , see Definition A.3 and Definition A.24 respectively.

$C^n(X) = \text{hom}(\llbracket n \rrbracket, X)$  (as the measure is supported in  $C^n(X)$ ). By Proposition 5.60, the disintegration of a measure is essentially the same as the conditional expectation. Thus

$$\mathbb{E}(f|\mathcal{A}_{P_1}^{\llbracket n \rrbracket})(c) = \int_{\text{hom}_{c|_{P_1}}(\llbracket n \rrbracket, X)} f(\tilde{c}) d\mu_{c|_{P_1}}(\tilde{c}),$$

where  $\mu_{c|_{P_1}}$  is the Haar measure of the  $k$ -fold abelian bundle  $\text{hom}_{c|_{P_1}}(\llbracket n \rrbracket, X)$ .

Now let us consider for every  $c \in C^n(X)$  the map

$$\begin{aligned} \phi_c : \text{hom}_{c|_{P_1}}(\llbracket n \rrbracket, X) &\rightarrow \text{hom}_{c|_{P_0 \cap P_1}}(P_0, X) \\ \tilde{c} &\rightarrow \tilde{c}|_{P_0}. \end{aligned}$$

This is a totally-surjective continuous bundle morphism by Lemma A.28. Thus, by Proposition 5.60 we can disintegrate  $\mathbb{E}(f|\mathcal{A}_{P_1}^{\llbracket n \rrbracket})(c)$ :

$$\int_{\text{hom}_{c|_{P_1}}(\llbracket n \rrbracket, X)} f(\tilde{c}) d\mu_{c|_{P_1}}(\tilde{c}) = \int_{\text{hom}_{c|_{P_0 \cap P_1}}(P_0, X)} \int_{\phi_c^{-1}(t)} f(\tilde{c}) d\mu_t(\tilde{c}) d\mu'(t),$$

where  $\mu_t$  is the Haar measure on the  $k$ -fold abelian bundle  $\phi_c^{-1}(t)$  and  $\mu'$  the Haar measure on  $\text{hom}_{c|_{P_0 \cap P_1}}(P_0, X)$ .

As  $f$  is a function that only depends on the coordinates indexed by  $P_0$ , we know that  $f = g \circ \pi_{P_0}$  for some  $g \in L^\infty(\text{hom}(P_0, X))$ . In the right hand side of the previous integral, if  $\tilde{c} \in \phi_c^{-1}(t)$  then  $t = \phi_c(\tilde{c}) = \tilde{c}|_{P_0}$ . Hence, the inner integral of the right hand side is just  $g(t)$ . Thus

$$\mathbb{E}(f|\mathcal{A}_{P_1}^{\llbracket n \rrbracket})(c) = \int_{\text{hom}_{c|_{P_0 \cap P_1}}(P_0, X)} g(t) d\mu'(t).$$

And to conclude, note that the restriction map

$$\begin{aligned} \psi_c : \text{hom}_{c|_{P_0 \cap P_1}}(\llbracket n \rrbracket, X) &\rightarrow \text{hom}_{c|_{P_0 \cap P_1}}(P_0, X) \\ \tilde{c} &\rightarrow \tilde{c}|_{P_0}, \end{aligned}$$

is also measure preserving (using the same argument as above). Therefore

$$\mathbb{E}(f|\mathcal{A}_{P_1}^{\llbracket n \rrbracket})(c) = \int_{\text{hom}_{c|_{P_0 \cap P_1}}(\llbracket n \rrbracket, X)} f(\tilde{c}) d\mu''(\tilde{c}),$$

where  $\mu''$  is the Haar measure on  $\text{hom}_{\mathbb{C}}|_{P_0 \cap P_1}(\llbracket n \rrbracket, X)$ . And this is equal to  $\mathbb{E}(f | \mathcal{A}_{P_0 \cap P_1}^{\llbracket n \rrbracket})(c)$ .  $\square$

This result can be used to easily prove that the couplings of a nilspace satisfy the Conditional independence axiom.

Now let us mention (very briefly) some of the concepts that play an important role in the proof of the main result, Theorem 5.116. Let us denote by  $K_d$  the set  $\llbracket d \rrbracket \setminus \{0^d\}$  for any  $d \geq 1$ .

**Definition 5.109** ( $U^d$ -convolution). Let  $(\Omega, (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  be a cubic coupling over a probability space  $(\Omega, \mathcal{A}, \lambda)$ , and let  $d \geq 0$  be an integer. Let  $F = (f_v : \Omega \rightarrow \mathbb{C})_{v \in K_d}$  be a system of bounded measurable functions. The  $U^d$ -convolution of  $F$  is the unique function  $[F]_{U^d}$  (up to  $\lambda$ -null sets) such that

$$\mathbb{E} \left( \prod_{v \in K_d} c^{|\underline{v}|+1} f_v \circ p_v | \mathcal{A}_{0^d}^{\llbracket d \rrbracket} \right) = [F]_{U^d} \circ p_{0^d}.$$

Similarly, we have the  $U^d$ -product:

**Definition 5.110** ( $U^d$ -product). Let  $(\Omega, (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  be a cubic coupling over a probability space  $(\Omega, \mathcal{A}, \lambda)$ , and let  $d \geq 1$  be an integer. Let  $F = (f_v : \Omega \rightarrow \mathbb{C})_{v \in \llbracket d \rrbracket}$  be a system of bounded measurable functions. The  $U^d$ -product of  $F$  is equal to

$$\langle F \rangle_{U^d} := \int_{\Omega^{\llbracket d \rrbracket}} \prod_{v \in \llbracket d \rrbracket} c^{|\underline{v}|} f_v \circ p_v d\mu^{\llbracket d \rrbracket}.$$

The latter definition is the generalization of the Gowers norms in this setting:

**Definition 5.111** ( $U^d$ -uniformity seminorm). Let  $(\Omega, (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  be a cubic coupling over a probability space  $(\Omega, \mathcal{A}, \lambda)$ , and let  $d \geq 1$  be an integer. Let  $f \in L^\infty(\Omega)$  and consider the system  $F = (f_v)_{v \in \llbracket d \rrbracket}$  where  $f_v = f$  for all  $v \in \llbracket d \rrbracket$ . Then the  $d$ -th uniformity seminorm is defined by the formula:

$$\|f\|_{U^d} := (\langle F \rangle_{U^d})^{1/2^d}.$$

We can for example prove a Gowers-Cauchy-Schwarz estimate (for a proof, see [17, Lemma 3.16]):

**Proposition 5.112.** *Let  $(\Omega, (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  be a cubic coupling and  $d \geq 1$  an integer. For every system  $F = (f_{\underline{v}})_{\underline{v} \in \llbracket d \rrbracket}$  of bounded measurable functions we have*

$$|\langle F \rangle_{U^d}| \leq \prod_{\underline{v} \in \llbracket d \rrbracket} \|f_{\underline{v}}\|_{U^d}.$$

The importance of the  $U^d$ -convolutions relies on the  $\sigma$ -algebra that they generate:

**Definition 5.113** (Fourier  $\sigma$ -algebra). Let  $(\Omega, (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  be a cubic coupling over a probability space  $(\Omega, \mathcal{A}, \lambda)$  and  $d \geq 0$  an integer. We define the  $d$ -th Fourier  $\sigma$ -algebra on  $\Omega$ , denoted by  $\mathcal{F}_d$  as the sub- $\sigma$ -algebra of  $\mathcal{A}$  generated by all possible  $U^{d+1}$ -convolutions of bounded  $\mathcal{A}$ -measurable functions.

Note that  $\mathcal{F}_0$  is the trivial  $\sigma$ -algebra, and by the Consistency axiom,  $\mathcal{F}_{d-1} \subset \mathcal{F}_d$  for all  $d \geq 1$ .

The next definition is important, as it is the explicit construction of the characteristic factors of a Borel cubic coupling (see [17, Definition 3.31]).

**Definition 5.114** (Topological factors of a Borel cubic coupling). Let  $(\Omega, (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  be a cubic coupling over a Borel probability space  $(\Omega, \mathcal{A}, \lambda)$ . For each  $k \geq 0$ , let  $\gamma_k : \Omega \rightarrow \mathbf{Cg}(\Omega, K_{k+1})$  be (up to null sets) a disintegration of the measure  $\mu^{\llbracket k+1 \rrbracket}$  in  $0^{k+1}$ . We define  $X_k := \text{Supp}(\lambda \circ \gamma_k^{-1}) \subset \mathbf{Cg}(\Omega, K_{k+1})$ . For each  $n \geq 0$ , the set of  $n$ -cubes of  $X_k$  will be defined as  $C^n(X_k) := \text{Supp}(\mu^{\llbracket n \rrbracket} \circ (\gamma_k^{\llbracket n \rrbracket})^{-1})$ .

See [17, 3.6 Topologization of cubic couplings] for more details of this construction. In particular, the relation with the Fourier  $\sigma$ -algebras is given by [17, Lemma 3.41]:

**Lemma 5.115.** *Let  $k \geq 0$  be an integer and let  $\mathcal{B}_k$  be the Borel  $\sigma$ -algebra on  $X_k$ . Then  $\gamma_k^{-1}(\mathcal{B}_k) =_{\lambda} \mathcal{F}_k$ .*

Now we can state the main result of [17], namely [17, Theorem 4.2]:

**Theorem 5.116** (Candela and Szegedy). *Let  $(\Omega, (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  be a cubic coupling over a Borel probability space  $(\Omega, \mathcal{A}, \lambda)$  and let  $X_k, C^n(X_k)$ , and  $\gamma_k$  be as in Definition 5.114. Then  $X_k$  is a  $k$ -step compact nilspace for every*

$k \geq 0$ , and for each  $n \geq 0$ , the image of  $\mu^{\llbracket n \rrbracket}$  through  $\gamma_k^{\llbracket n \rrbracket}$  is the Haar measure on  $C^n(X_k)$ . Furthermore,  $\mu^{\llbracket k+1 \rrbracket}$  is relatively independent over  $(\gamma_k^{\llbracket k+1 \rrbracket})^{-1}(\mathcal{B}_k^{\llbracket k+1 \rrbracket})$  as in Definition 5.97.

Informally, this says that if we are working on a problem that involves (say)  $U^d$  convolutions in a general Borel probability space, we can move our problem to a nilspace, and use all the rigid structure that these spaces have. We can rephrase it using inverse factor nilspaces (see Definition 5.70):

**Theorem 5.117** (Candela and Szegedy). *Let  $(\Omega, (\mu^{\llbracket n \rrbracket})_{n \geq 0})$  be a cubic coupling over a Borel probability space  $(\Omega, \mathcal{A}, \lambda)$ . Then there exists an inverse factor compact nilspace  $X$  and a measure-preserving map  $\gamma : \Omega \rightarrow X$  such that for every  $n \geq 0$ , the map  $\gamma^{\llbracket n \rrbracket} : (\Omega^{\llbracket n \rrbracket}, \mu^{\llbracket n \rrbracket}) \rightarrow (X^{\llbracket n \rrbracket}, \mu_{C^n(X)})$  is measure preserving. Furthermore,  $\mu^{\llbracket n \rrbracket}$  is relatively independent over  $(\gamma^{\llbracket n \rrbracket})^{-1}(\mathcal{B}^{\llbracket n \rrbracket})$  as in Definition 5.97.*

Here, the nilspace  $X$  will be defined as the inverse limit of the nilspaces  $X_k$  obtained in Theorem 5.116.

### 5.4.5 Applications of the cubic coupling theory

Apart from the extension of the Host and Kra result on characteristic factors (which will be discussed in Chapter 6), the other famous results that can be deduced are the inverse theorem and the regularity lemma. In [18], the authors show how to prove these results using the theory of cubic couplings and nilspaces. Let us state the regularity lemma [18, Theorem 1.5], and give an idea of the proof (for the complete proof, see [18]):

**Theorem 5.118** (Candela and Szegedy). *Let  $k \geq 0$  and  $\mathcal{D} : \mathbb{R}_{>0} \times \mathbb{N} \rightarrow \mathbb{R}_{>0}$  be an arbitrary function. For every  $\varepsilon > 0$ , there exists  $N = N(\varepsilon, \mathcal{D}) > 0$  such that the following holds. For every compact nilspace  $X$  that is the inverse limit of compact finite-rank coset nilspaces and every measurable function  $f : X \rightarrow \mathbb{C}$  with  $|f| \leq 1$ , we can find a decomposition  $f = f_s + f_e + f_r$  and a number  $m \leq N$  such that:*

1.  $f_s$  is a  $\mathcal{D}(\varepsilon, m)$ -balanced nilspace polynomial of degree  $k$  with  $|f_s| \leq 1$  and complexity at most  $m$ .
2.  $\|f_e\|_{L^1} \leq \varepsilon$ .

3.  $\|f_r\|_{U^{k+1}} \leq \mathcal{D}(\varepsilon, m)$ ,  $|f_r| \leq 1$  and  $\max(|\langle f_r, f_s \rangle|, |\langle f_r, f_e \rangle|) \leq \mathcal{D}(\varepsilon, m)$ .

Let us give an idea of the concepts present in this theorem. A nilspace polynomial is a composition  $F \circ \varphi$  where  $\varphi : X \rightarrow Y$  is a morphism between nilspaces, with  $Y$  being of finite rank, and  $F : Y \rightarrow \mathbb{C}$  is a continuous function<sup>7</sup>. If it is of degree  $k$ , it means that  $Y$  is  $k$ -step. The complexity of this polynomial refers to both that the Lipschitz constant of  $F$  (using a fixed metric that we can fix on every  $k$ -step, compact, and finite-rank nilspace) is bounded by  $m$ ; and that the nilspace  $Y$  belongs to a finite subset (of size at most  $m$ ) of all compact,  $k$ -step, and finite-rank nilspaces. Finally, the concept of being balanced informally says that the Haar measure on  $C^n(Y)$  is very well approximated (up to a certain  $n$ ) by the Haar measure on  $C^n(X)$  (via  $(\varphi^{\llbracket n \rrbracket})^{-1}$ ). The operator  $\langle \cdot, \cdot \rangle$  represents, as usual, the scalar product (equivalently, the  $U^1$ -convolution).

The idea of the proof is the following. In [18], the authors argue by contradiction, assuming the result is false for a sequence of functions, nilspaces, etc. Then, they construct the ultraproduct of them. This ultraproduct with the Loeb measure is *almost* a cubic coupling (an important part of the proof consists in overcoming this difficulty). Once this is done, using Theorem 5.116, they move the problem to a compact nilspace. Using Theorem 5.69, they arrive to a compact and finite-rank nilspace. The structured part will *essentially* be (recall that we are working in an ultraproduct, the objects are ultralimits of functions) the conditional expectation with respect to the  $k$ -th Fourier  $\sigma$ -algebra. Finally, once we have done this decomposition, we have to untangle all the results with ultraproducts and inverse limits to get functions in the original spaces.

---

<sup>7</sup>This concept generalizes that of nilsequences, see [4, Definition 1.8].

# Chapter 6

## On nilspace systems and their morphisms

First published in Ergodic Theory and Dynamical Systems in 2019, published by the Cambridge University Press. This work was made in collaboration with Pablo Candela and Balázs Szegedy. For the original publication see [13].

### 6.1 Introduction

Nilsystems are important examples of measure-preserving systems and their study has a long history in ergodic theory, beginning with works including [2, 29, 62, 66]. This study gained strong motivation especially through the essential role of nilsystems in the structural theory of measure-preserving systems and the analysis of multiple ergodic averages, topics that have kept growing with vibrant progress to the present day. We refer to the book [48] for a thorough treatment of these rich topics and for a broad bibliography.

In recent works stemming from the connections between ergodic theory and arithmetic combinatorics, objects known as *compact nilspaces* are found to be useful generalizations of nilmanifolds. Similarly to how nilsystems are constructed using nilmanifolds, one can define generalizations of nilsystems using compact nilspaces, thus obtaining measure-preserving systems that we call *nilspace systems*. These systems emerge as natural objects to consider when trying to extend the structural theory of measure-preserving systems,

or that of topological dynamical systems, beyond works such as that of Host and Kra [50], Ziegler [90], or Host Kra and Maass [51], and especially when seeking extensions valid for nilpotent group actions; see [17, 31].

The theory of nilspaces is growing into a subject of intrinsic interest. In addition to the original preprint [1], there are now several references that detail the basics of this theory; see [9, 10, 40, 41]. To state the definition of a nilspace system below, we use the notions of a compact nilspace  $X$  and of the translation group  $\Theta(X)$ , which can be recalled from [10, Definition 1.0.2] and [9, Definition 3.2.27] respectively. Recall also that, on a *compact* nilspace, translations are supposed to be homeomorphisms; see [10, §2.9].

**Definition 6.1.** A *nilspace system* is a triple  $(X, H, \phi)$  where  $X$  is a compact nilspace,  $H$  is a topological group, and  $\phi : H \rightarrow \Theta(X)$  is a continuous group homomorphism. We say that  $(X, H, \phi)$  is a *k-step nilspace system* if  $X$  is a *k-step nilspace*.

Nilspace systems are indeed generalizations of nilsystems: given a nilmanifold  $G/\Gamma$  and a map  $T : G/\Gamma \rightarrow G/\Gamma$ ,  $x\Gamma \mapsto hx\Gamma$  for some  $h \in G$ , it is seen from the definitions that  $T$  is a translation on  $X$ , where  $X$  is the nilspace obtained by endowing  $G/\Gamma$  with the cube structure induced by the Host-Kra cubes  $C^n(G_\bullet)$  relative to any given filtration  $G_\bullet$  on  $G$  (see [9, Definition 2.2.3 and Proposition 2.3.1]). A nilspace system can be viewed as a measure-preserving system, by equipping the compact nilspace with its Haar probability measure, which is invariant under any translation; see [1] and [10, Proposition 2.2.5 and Corollary 2.2.7]. The term *nilsystem* can also be used more generally, when instead of a single map  $T$  we have an action of a group  $H$  (usually supposed to be countable and discrete) on  $G/\Gamma$  via a homomorphism  $\varphi : H \rightarrow G$ , action defined by  $(h, x\Gamma) \mapsto \varphi(h)x\Gamma$ .

It is natural to seek expressions for nilspace systems in terms of nilsystems, so as to reduce questions involving the former systems to questions involving the better-known latter systems. One of the central results in nilspace theory is the inverse limit theorem [1, Theorem 4]; in particular this result characterizes a general class of compact nilspaces (those with connected structure groups) as inverse limits of nilmanifolds. This motivates the problem of expressing nilspace systems as inverse limits of nilsystems. Similar problems are treated by Gutman, Manners and Varjú in [42] from the different viewpoint of applications in topological dynamics, concerning the *regionally proximal relations*. Further motivation comes from the use of nilspace systems in [17] to extend the structure theorem of Host and Kra

[50, Theorem 10.1] to nilpotent group actions.

To obtain such expressions of nilspace systems in terms of nilsystems, it is suitable first to focus on certain more fundamental questions concerning nilspace systems in themselves, and especially on how translations on a compact nilspace  $X$  can interact with continuous<sup>1</sup> morphisms from  $X$  to another compact nilspace. As we show in this chapter, once these questions are solved, the sought expressions for nilspace systems can be obtained swiftly.

One fundamental question of the above kind asks whether a given nilspace morphism satisfies the following property relative to a given translation.

**Definition 6.2.** Let  $X, Y$  be nilspaces, let  $\psi : X \rightarrow Y$  be a morphism, and let  $\alpha$  be a translation in  $\Theta(X)$ . We say that  $\psi$  is  $\alpha$ -consistent if for every  $x, y \in X$  we have  $(\psi(x) = \psi(y)) \Rightarrow (\psi \circ \alpha(x) = \psi \circ \alpha(y))$ . Given a set of translations  $H \subset \Theta(X)$ , we say that  $\psi$  is  $H$ -consistent if  $\psi$  is  $\alpha$ -consistent for each  $\alpha \in H$ .

The question of whether a morphism is  $\alpha$ -consistent is particularly relevant for the special class of morphisms termed *fiber-surjective morphisms*. Introduced in [1] (see also [10, Definition 3.3.7]), these morphisms play an important role in nilspace theory. The term *fibration* was introduced in [40, Definition 7.1] for a notion which is equivalent to that of a fiber-surjective morphism as far as nilspaces are concerned, and which gives a useful alternative definition; we shall use the two terms interchangeably. We recall these notions in Definition 6.3 below. This definition uses the characteristic factors  $X_n = \mathcal{F}_n(X)$  of a nilspace  $X$ , and the associated canonical projections  $\pi_n : X \rightarrow X_n$  (see [9, Definition 3.2.3]). When we need to emphasize on which nilspace  $X$  the map  $\pi_n$  is being considered, we denote this map by  $\pi_{n,X}$ . We also use the notation  $\llbracket n \rrbracket$  for the discrete  $n$ -cube  $\{0, 1\}^n$ , and  $C^n(X)$  for the set of  $n$ -cubes on  $X$ . Finally, let us recall the notion of an  $n$ -corner on  $X$ , that is, a map  $c' : \llbracket n \rrbracket \setminus \{1^n\} \rightarrow X$  (where  $1^n = (1, \dots, 1)$ ) such that the restriction of  $c'$  to any  $(n - 1)$ -face of  $\llbracket n \rrbracket$  not containing  $1^n$  is an  $(n - 1)$ -cube (see [9, Definition 1.2.1]). We denote the set of  $n$ -corners on  $X$  by  $\text{Cor}^n(X)$ .

---

<sup>1</sup>In this chapter every morphism between compact nilspaces is automatically supposed to be a continuous map, and from now on we usually do not specify this continuity explicitly.

**Definition 6.3.** Let  $X, Y$  be nilspaces. A morphism  $\psi : X \rightarrow Y$  is said to be *fiber-surjective*, or a *fibration*, if for every  $n \geq 0$  it maps  $\pi_n$ -fibers to  $\pi_n$ -fibers, that is, for every fiber  $\pi_{n,X}^{-1}(x)$ ,  $x \in X_n$ , we have  $\psi(\pi_{n,X}^{-1}(x)) = \pi_{n,Y}^{-1}(y)$  for some  $y \in Y_n$ . Equivalently  $\psi$  is a fibration if for every  $n$ -corner  $c'$  on  $X$ , and every completion  $c'' \in C^n(Y)$  of the  $n$ -corner  $\psi \circ c'$ , there is  $c \in C^n(X)$  completing  $c'$  such that  $\psi \circ c = c''$ .

*Remark 6.4.* Note that a fibration is always a surjective map, since for every  $k$ -step nilspace  $Y$  the fiber of  $\pi_0$  is the whole of  $Y$  (note that  $Y_0$  is a singleton).

The equivalence stated in Definition 6.3 follows from the properties of the equivalence relations  $\sim_n$  associated with the quotient maps  $\pi_n$  (see [9, Definition 3.2.3]).

The following simple result illustrates the relevance of  $\alpha$ -consistency for fibrations.

**Lemma 6.5.** *Let  $X, Y$  be compact nilspaces, let  $\psi : X \rightarrow Y$  be a fibration, and let  $\alpha \in \Theta(X)$ . If  $\psi$  is  $\alpha$ -consistent then we can define  $\beta \in \Theta(Y)$  by setting  $\beta(y) = \psi(\alpha(x))$  for any  $x \in \psi^{-1}(y)$ . Moreover, if for every translation  $\alpha \in \Theta(X)$  such that  $\psi$  is  $\alpha$ -consistent, we denote by  $\widehat{\psi}(\alpha)$  the corresponding translation  $\beta \in \Theta(Y)$  thus defined, then, whenever  $\psi$  is  $\{\alpha_1, \alpha_2\}$ -consistent, we have that  $\psi$  is  $\alpha_1\alpha_2$ -consistent and  $\widehat{\psi}(\alpha_1\alpha_2) = \widehat{\psi}(\alpha_1)\widehat{\psi}(\alpha_2)$ .*

In particular, if  $S$  is a subset of  $\Theta(X)$  such that  $\psi$  is  $S$ -consistent, and  $H = \langle S \rangle$  is the subgroup of  $\Theta(X)$  generated by  $S$ , then  $\psi$  is also  $H$ -consistent, the map  $\widehat{\psi}$  is a homomorphism  $H \rightarrow \Theta(Y)$ , and  $\widehat{\psi}$  is an  $(H, \widehat{\psi}(H))$ -equivariant map, i.e., for all  $\alpha \in H$ ,  $x \in X$  we have  $\psi(\alpha(x)) = \widehat{\psi}(\alpha)(\psi(x))$ . We leave the proof of Lemma 6.5 to Section 6.4.

To what extent can  $\alpha$ -consistency be guaranteed for a given fibration and a given translation  $\alpha$ ? If  $Z, Z'$  are compact abelian groups equipped with their standard nilspace structure (see [9, Section 2.1]), and  $\psi : Z \rightarrow Z'$  is a fibration between these nilspaces, then  $\psi$  is a surjective affine homomorphism (by [9, Lemma 3.3.8] say), and must then clearly be  $\alpha$ -consistent for every  $\alpha \in \Theta(Z)$  (since  $\alpha$  must be of the form  $\alpha(z) = z + t$  for some fixed  $t \in Z$ ). However, this automatic translation-consistency does not hold for fibrations between more general nilspaces; we illustrate this with Example 6.2 in the next section.

While translation consistency can fail, we prove a result that can be viewed as the next best thing, namely Theorem 6.6 below. Indeed, this result

tells us that by performing a relatively simple refinement of the fibration's target nilspace, one can always obtain a factorization of the fibration in which the first applied map has the desired consistency. The simplicity of the refinement consists in that, if the original target nilspace is of finite rank, then the new refined nilspace is also of finite rank. Recall that a compact nilspace has finite rank if each of its structure groups is a Lie group (see [10, Definition 2.5.1]). These nilspaces form a more manageable class among general compact nilspaces, playing a role in the theory similar to the role of compact abelian Lie groups in relation to general compact abelian groups (see for instance the inverse limit theorem [10, Theorem 2.7.3]).

**Theorem 6.6.** *Let  $X, Y'$  be compact  $k$ -step nilspaces, with  $Y'$  of finite rank, let  $\psi' : X \rightarrow Y'$  be a fibration, and let  $H \subset \Theta(X)$  be finite. Then there is a compact finite-rank nilspace  $Y$ , an  $H$ -consistent fibration  $\psi : X \rightarrow Y$ , and a fibration  $p : Y \rightarrow Y'$  such that  $\psi' = p \circ \psi$ .*

This theorem is our main result in Section 6.4. It relies on the following more fundamental result concerning morphisms between compact nilspaces, proved in Section 6.3.

**Theorem 6.7.** *Let  $X, Y$  be compact nilspaces, with  $Y$  of finite rank, and let  $m : X \rightarrow Y$  be a morphism. Then there exist a compact finite-rank nilspace  $Q$ , a fibration  $\psi : X \rightarrow Q$ , and a morphism  $\psi' : Q \rightarrow Y$ , such that  $m = \psi' \circ \psi$ .*

Recall that a strict inverse system of compact nilspaces  $X_i$ ,  $i \in \mathbb{N}$ , is a system of fibrations  $(\psi_{i,j} : X_j \rightarrow X_i)_{i,j \in \mathbb{N}, i \leq j}$  such that  $\psi_{i,i} = \text{id}$  for all  $i \in \mathbb{N}$  and  $\psi_{i,j} \circ \psi_{j,k} = \psi_{i,k}$  for all  $i \leq j \leq k$  (see [10, Definition 2.7.1]).

In Section 6.5, we apply our results to give a swift proof of the following stronger version of the inverse limit theorem for compact nilspaces.

**Theorem 6.8.** *Let  $X$  be a compact nilspace and let  $H$  be a finite subset of  $\Theta(X)$ . Then there is a strict inverse system  $(\psi_{i,j} : X_j \rightarrow X_i)_{i,j \in \mathbb{N}, i \leq j}$  of compact finite-rank nilspaces  $X_i$  such that  $X = \varprojlim X_i$  and such that the limit maps  $\psi_i : X \rightarrow X_i$  are all  $\langle H \rangle$ -consistent.*

As a special case we obtain that for every *ergodic* nilspace system, if its corresponding group  $H$  is a *finitely-generated* subgroup of  $\Theta(X)$ , then the nilspace system is an inverse limit of nilsystems; see Theorem 6.19. Thus we also provide a different proof of a result from [42]; see Remark 6.22. Theorem 6.19 is used in [17] to extend the structure theorem of Host and Kra to finitely generated nilpotent group actions; see [17, Theorem 5.12].

## 6.2 Some motivating examples

We begin with a simple example showing that a fibration on a compact nilspace  $X$  need not be  $\alpha$ -consistent for every  $\alpha \in \Theta(X)$ .

*Example:* Recall the definition of the degree- $k$  nilspace structure  $\mathcal{D}_k(\mathbb{Z})$  on an abelian group  $\mathbb{Z}$ , in terms of the Gray-code alternating sum  $\sigma_k$ ; see [9, Definition 2.2.30]. Let  $X$  be the product nilspace  $\mathcal{D}_1(\mathbb{Z}_2) \times \mathcal{D}_2(\mathbb{Z}_2)$  (where by  $\mathbb{Z}_2$  we denote the 2-element group  $\mathbb{Z}/2\mathbb{Z}$ ), and let  $Y$  be the nilspace  $\mathcal{D}_2(\mathbb{Z}_2)$ . Thus  $X, Y$  are 2-step compact finite-rank nilspaces (actually finite and with the discrete topology). Let  $\psi$  denote the 2-nd coordinate projection  $X \rightarrow Y$ ,  $(a, b) \mapsto b$ . Using the third sentence in Definition 6.3, it is easily checked that  $\psi$  is a fibration.

Let  $\alpha : X \rightarrow X$  be the map  $(a, b) \mapsto (a + 1, b + a)$ . We claim that  $\alpha \in \Theta(X)$ . To see this, by [9, Definition 3.2.27 and Lemma 3.2.13] it suffices to check that for every 3-cube  $c \in C^3(X)$ , and any 2-face  $F \subset \llbracket 3 \rrbracket$ , defining  $\alpha^F(c) : \llbracket 3 \rrbracket \rightarrow X$  by  $\alpha^F(c)(v) = \alpha(c(v))$  for  $v \in F$  and  $c(v)$  otherwise, we have  $\alpha^F(c) \in C^3(X)$ . Let  $c' := \alpha^F(c)$ . By definition of the product nilspace structure, we have  $c' \in C^3(X)$  if and only if the coordinate projections  $p_1 : X \rightarrow \mathcal{D}_1(\mathbb{Z}_2)$  and  $p_2 : X \rightarrow \mathcal{D}_2(\mathbb{Z}_2)$  satisfy  $p_i \circ c' \in C^3(\mathcal{D}_i(\mathbb{Z}_2))$  for  $i = 1, 2$ . By definition of  $\mathcal{D}_1(\mathbb{Z}_2)$  and  $\mathcal{D}_2(\mathbb{Z}_2)$ , we therefore have  $c' \in C^3(X)$  if and only if the Gray-code alternating sum  $\sigma_3(p_2 \circ c')$  is 0 and for every 2-face map  $\phi : \llbracket 2 \rrbracket \rightarrow \llbracket 3 \rrbracket$  we have  $\sigma_2(p_1 \circ c' \circ \phi) = 0$ . Now from the definition of  $\alpha$ , we deduce that  $c' = c + c''$  where  $c''(v) = (1, p_1 \circ c(v))$  if  $v \in F$  and  $c''(v) = (0, 0)$  otherwise. We then have  $\sigma_3(p_2 \circ c') = \sigma_3(p_2 \circ c) + \sigma_3(p_2 \circ c'') = 0$ , and also  $\sigma_2(p_1 \circ c' \circ \phi) = \sigma_2(p_1 \circ c \circ \phi) + \sigma_2(p_1 \circ c'' \circ \phi) = 0$ . This proves our claim. Note also that  $\alpha$  is a minimal map.

Now observe that  $\psi$  is not  $\alpha$ -consistent. Indeed, for example  $(1, 0), (0, 0) \in X$  satisfy  $\psi(1, 0) = \psi(0, 0) = 0$ , but  $\psi \circ \alpha(1, 0) = 1 \neq 0 = \psi \circ \alpha(0, 0)$ .

One may try to avoid such examples by assuming that the fibration  $\psi$  has additional properties. For instance, noting that if  $\psi$  is injective then trivially it is  $\alpha$ -consistent, one may hope that if  $\psi$  is “sufficiently close” to being injective then it should also be  $\alpha$ -consistent. A way to capture closeness to injectivity could be to assume that every preimage  $\psi^{-1}(y)$ ,  $y \in Y$  is a set of diameter<sup>2</sup> at most some small fixed  $\delta > 0$ , for some fixed metric on  $X$ .

<sup>2</sup>For a metric space  $(X, d)$  and  $B \subset X$ , we define the *diameter* of  $B$  by  $\text{diam}(B) := \sup_{x, y \in B} d(x, y)$ .

However, one can elaborate on Example 6.2 to produce translations  $\alpha$  such that even morphisms arbitrarily close to being injective in this sense can fail to be  $\alpha$ -consistent. Let us outline such a construction.

*Example:* Let  $X_0$  be the nilspace  $\mathcal{D}_1(\mathbb{Z}_2) \times \mathcal{D}_2(\mathbb{Z}_2)$  from Example 6.2. Let  $X$  be the compact nilspace consisting of the power  $X_0^{\mathbb{N}}$  with the product compact-nilspace structure. Let  $\alpha_0 \in \Theta(X_0)$  be the translation  $(a, b) \mapsto (a+1, b+a)$  from Example 6.2. Let  $\alpha$  denote the translation on  $X$  defined by applying  $\alpha_0$  to each coordinate of  $x = (x_i)_{i \in \mathbb{N}} \in X$ , i.e.  $\alpha(x) = (\alpha_0(x_i))_{i \in \mathbb{N}}$ . We can metrize  $X$  with  $d(x, y) = \sum_{i \in \mathbb{N}} 2^{-i} d_0(x_i, y_i)$  for  $d_0$  the discrete metric on  $X_0$ . Consider now the following sequence of fibrations: for each  $i \in \mathbb{N}$  let  $Y_i$  denote the product nilspace  $X_0^i \times \mathcal{D}_2(\mathbb{Z}_2)$ , and let  $\psi_i : X \rightarrow Y_i$ ,  $x \mapsto (x_1, \dots, x_i, \psi(x_{i+1}))$ , where  $\psi$  is the projection to the second coordinate on  $X_0$  as in Example 6.2. We then have the following facts (we leave the proofs to the reader):

1. For every  $i \in \mathbb{N}$  the map  $\psi_i$  is a (continuous) fibration.
2. We have  $\sup_{y \in Y_i} \text{diam}(\psi_i^{-1}(y)) = 2^{-i} \rightarrow 0$  as  $i \rightarrow \infty$ . And yet,
3. For every  $i$ , letting  $\mathbf{0}$  be the element of  $X$  with all components equal to  $(0, 0)$ , and  $x$  the element with  $x_j = (0, 0)$  for  $j \neq i+1$  and  $x_{i+1} = (1, 0)$ , we have  $\psi_i(x) = \psi_i(\mathbf{0})$  and  $\psi_i \circ \alpha(x) \neq \psi_i \circ \alpha(\mathbf{0})$ , so  $\psi_i$  is not  $\alpha$ -consistent.

Thus, Example 6.2 shows that for  $k > 1$  there can be a translation on a  $k$ -step nilspace  $X$  and fibrations  $\psi : X \rightarrow Y$  that are arbitrarily close to being injective and yet still fail to be  $\alpha$ -consistent. As we explain in the sequel, if we are willing to *refine* a fibration  $\psi : X \rightarrow Y$  by considering how  $\psi$  factors through nilspaces finer than  $Y$ , then the  $\alpha$ -consistency can be ensured for some such factor.

### 6.3 Finite-rank valued morphisms factor through fibrations

In this section we prove Theorem 6.7, which we recall here for convenience. This is used in Section 6.4 to show that a fibration into a finite-rank nilspace

always factors through some fibration consistent with a prescribed translation (Theorem 6.6).

**Theorem 6.7.** *Let  $X, Y$  be compact nilspaces, with  $Y$  of finite rank, and let  $m : X \rightarrow Y$  be a morphism. Then there exist a compact finite-rank nilspace  $Q$ , a fibration  $\psi : X \rightarrow Q$ , and a morphism  $\psi' : Q \rightarrow Y$ , such that  $m = \psi' \circ \psi$ .*

Our proof of this theorem can be summarized simply as follows: we take the inverse limit expression  $X = \varprojlim X_i$  given by [1, Theorem 4] (see also [10, Theorem 2.7.3]) and we show that, for some  $i$  sufficiently large, the map  $m$  factors through the limit map  $\psi_i : X \rightarrow X_i$ , so that we can set  $\psi = \psi_i$ . The proof uses some lemmas which we detail as follows.

Firstly, we have the following topological lemma.

**Lemma 6.9.** *Let  $T, T_1, T_2, \dots$  be compact metric spaces, and let  $(\psi_i : T \rightarrow T_i)_{i \in \mathbb{N}}$  be a sequence of surjective continuous maps with the following properties:*

1. *For all  $i \leq j$  and  $x, y \in T$  with  $\psi_j(x) = \psi_j(y)$ , we have  $\psi_i(x) = \psi_i(y)$ .*
2. *For every  $x \neq y$  there exists  $i$  such that  $\psi_i(x) \neq \psi_i(y)$ .*

*Let  $(M, d)$  be a metric space and let  $f : T \rightarrow M$  be continuous. Then for every  $\varepsilon > 0$  there exists  $i$  such that for every  $x \in T_i$  we have  $\text{diam}(f(\psi_i^{-1}(x))) \leq \varepsilon$ .*

The assumptions (i), (ii) in this lemma are satisfied in particular when  $T$  is the topological inverse limit of the spaces  $T_i$ .

*Proof.* Suppose for a contradiction that for some  $\varepsilon > 0$ , for all  $i \in \mathbb{N}$  there exist  $x_i, y_i \in T$  such that  $\psi_i(x_i) = \psi_i(y_i)$  and  $d(f(x_i), f(y_i)) \geq \varepsilon$ . Since  $T$  is compact, we can assume (passing to subsequences if necessary) that there exist  $x, y \in T$  with  $x_i \rightarrow x$  and  $y_i \rightarrow y$  as  $i \rightarrow \infty$ . By continuity of  $f$  and  $d$  we have  $d(f(x), f(y)) \geq \varepsilon$ , so in particular  $x \neq y$ . By (ii), this implies that  $\psi_k(x) \neq \psi_k(y)$  for some  $k$ . However, by assumption  $\psi_j(x_j) = \psi_j(y_j)$  for every  $j$ , and if  $j > k$  then by (i) we therefore have  $\psi_k(x_j) = \psi_k(y_j)$ . Letting  $j \rightarrow \infty$ , by continuity of  $\psi_k$  we deduce that  $\psi_k(x) = \psi_k(y)$ , a contradiction.  $\square$

Secondly, we have the following algebraic result, which is a basic fact about nilspaces.

**Lemma 6.10.** *Let  $X, Y$  be  $k$ -step nilspaces, and let  $\psi : X \rightarrow Y$  be a fibration. Then for every  $y \in Y$  the preimage  $\psi^{-1}(y)$  is a sub-nilspace of  $X$ .*

*Proof.* Of the three nilspace axioms (see [9, Definition 1.2.1]), the composition and ergodicity axioms are clearly satisfied. The corner-completion axiom follows readily from the third sentence in Definition 6.3 (using that for all  $n$  the constant map  $[[n]] \rightarrow \{y\}$  is a cube).  $\square$

We now move on to the main element in the proof of Theorem 6.7, which is a lemma that extends the following result from [1] (see also [10, Corollary 2.9.8]).

**Lemma 6.11** ([1, Corollary 3.2]). *For every compact finite-rank abelian group  $Z'$  and  $j \in \mathbb{N}$ , there exists  $\varepsilon > 0$  such that the following holds. For every compact  $k$ -step nilspace  $X$  and continuous morphism  $m : X \rightarrow \mathcal{D}_j(Z')$ , if  $\text{diam}(m(X)) \leq \varepsilon$  then  $m$  is constant.*

The extension in question is the following.

**Lemma 6.12.** *For every compact finite-rank  $k$ -step nilspace  $Y$ , there exists  $\delta > 0$  such that the following holds. For every compact  $k$ -step nilspace  $X$  and continuous morphism  $m : X \rightarrow Y$ , if  $\text{diam}(m(X)) \leq \delta$  then  $m$  is constant.*

For  $i \leq j$ , we denote by  $\pi_{i,j} : Y_j \rightarrow Y_i$  the projection between the two factors of  $Y$  (thus  $\pi_i = \pi_{i,k}$  if  $Y$  is  $k$ -step). Our proof of Lemma 6.12 uses the following result.

**Proposition 6.13.** *Let  $Y$  be a compact finite-rank  $k$ -step nilspace, with a fixed metric  $d_Y$ , and for each  $i \in [k]$  let  $Z_i$  be the  $i$ -th structure group of  $Y$ , with a fixed metric  $d_{Z_i}$ . Then there is a collection of compact nilspace isomorphisms  $\psi_{i,y} : \pi_{i-1,i}^{-1}(y) \rightarrow \mathcal{D}_i(Z_i)$  for  $i \in [k]$ ,  $y \in Y_{i-1}$ , such that the following holds: for every  $\varepsilon > 0$  there exists  $\delta > 0$  such that for all  $a, b \in Y$  with  $\pi_{i-1}(a) = \pi_{i-1}(b) = y$ , if  $d_Y(a, b) < \delta$  then  $d_{Z_i}(\psi_{i,y} \circ \pi_i(a), \psi_{i,y} \circ \pi_i(b)) < \varepsilon$ .*

*Proof of Lemma 6.12 assuming Proposition 6.13.* For each  $i \in [k]$  let  $\varepsilon_i$  be the number  $\varepsilon(Z_i, i) > 0$  given by Lemma 6.11. Let  $0 < \varepsilon < \min_{i \in [k]} \varepsilon_i$ , and apply Proposition 6.13 to obtain the corresponding  $\delta > 0$  and functions  $\psi_{i,y}$ . We prove by induction on  $i \in [0, k]$  that  $\pi_i \circ m$  is constant.

The case  $i = 0$  is trivial since  $Y_0$  is the one-point space. We assume that  $\pi_{i-1} \circ m$  is constant, thus  $\pi_{i-1} \circ m(X) = y \in Y_{i-1}$ . By Proposition 6.13 we have  $\text{diam}(\psi_{i,y} \circ \pi_i \circ m(X)) < \varepsilon < \varepsilon(Z_i, i)$ . This together with the fact that  $\psi_{i,y} \circ \pi_i \circ m$  is a morphism  $X \rightarrow \mathcal{D}_i(Z_i)$  implies, by Lemma 6.11, that this map is constant. Hence  $\pi_i \circ m$  is constant, since  $\psi_{i,y}$  is injective.  $\square$

*Proof of Proposition 6.13.* We first prove the case  $i = k$ . By [41, Proposition A.1] there exists  $\delta_k > 0$  such that if  $x \in Y$  and  $z \in Z_k$  satisfy  $d_Y(x, x+z) < \delta_k$  then  $d_{Z_k}(0, z) < \varepsilon$ . Now for each fiber  $\pi_{k-1}^{-1}(y)$ ,  $y \in Y_{k-1}$ , fix any point  $y'$  in this fiber and define  $\psi_{k,y} : \pi_{k-1}^{-1}(y) \rightarrow Z_k$  by  $\psi_{k,y}(y' + z) := z$  (recalling from [9, Theorem 3.2.19] that each point in this fiber is of the form  $y' + z$  for a unique  $z \in Z_k$ ). Note that, since  $d_{Z_k}$  is translation-invariant, if  $a, b$  are points in such a fiber  $\pi_{k-1}^{-1}(y)$  with  $d_Y(a, b) < \delta_k$  and  $a = y' + z_1$ ,  $b = y' + z_2$ , then  $d_{Z_k}(\psi_{k,y}(a), \psi_{k,y}(b)) = d_{Z_k}(z_1, z_2) = d_{Z_k}(0, z_2 - z_1) \leq \varepsilon$ .

For  $i \leq k - 1$  we argue similarly with  $Y_i$  instead of  $Y$ , and with the same fixed  $\varepsilon > 0$ . Thus we obtain a function  $\psi_{i,y}$  for each  $y \in Y_{i-1}$ , and some  $\delta'_i > 0$  given by applying [41, Proposition A.1], with the property that for every  $a, b \in Y_i$  in the same fiber of  $\pi_{i-1,i}$ , if  $d_{Y_i}(a, b) \leq \delta'_i$  then  $d_{Z_i}(\psi_{i,y}(a), \psi_{i,y}(b)) \leq \varepsilon$ . Moreover, since  $\pi_i : Y \rightarrow Y_i$  is a continuous function between compact metric spaces, it is uniformly continuous, so there exists  $\delta_i > 0$  such that if  $d_Y(a, b) < \delta_i$  then  $d_{Y_i}(\pi_i(a), \pi_i(b)) < \delta'_i$ .

Finally, we let  $\delta = \min_{1 \leq i \leq k} \delta_i$ , and the result follows.  $\square$

We can now prove the main result of this section.

*Proof of Theorem 6.7.* Let  $\varepsilon$  be the number  $\delta$  given by Lemma 6.12 applied to  $Y$ . Let  $X = \varprojlim X_i$  be an inverse limit decomposition given by [1, Theorem 4] (see also [10, Theorem 2.7.3]); thus  $X_i$  is a compact finite-rank nilspace and  $\psi_i : X \rightarrow X_i$  is a fibration for each  $i$ . Applying Lemma 6.9 with  $T = X$ ,  $T_i = X_i$  and  $\varepsilon$ , we obtain  $i_0$  such that  $\text{diam}(m(\psi_{i_0}^{-1}(x))) < \varepsilon$  for all  $x \in X_{i_0}$ . We claim that we can set  $Q := X_{i_0}$  and  $\psi := \psi_{i_0}$ . To prove this we show that there exists a morphism  $\psi' : Q \rightarrow Y$  such that  $m = \psi' \circ \psi$ . First note that setting  $\psi'(x) := m(\psi^{-1}(x))$  gives a well-defined map  $\psi' : Q \rightarrow Y$ , because  $m(\psi^{-1}(x))$  is a singleton for every  $x \in Q$ . Indeed  $\psi^{-1}(x)$  is a sub-nilspace of  $X$ , by Lemma 6.10, and  $m$  restricted to this fiber is a morphism with image of diameter less than  $\varepsilon$ , so by Lemma 6.12 this morphism is constant, so  $\psi'$  is indeed well-defined. Moreover  $\psi'$  is a morphism, since, by [9, Lemma 3.3.9], for every  $c \in C^n(Q)$  there exists  $c' \in C^n(X)$  such that  $c = \psi \circ c'$ , so

$\psi' \circ c = m \circ c' \in C^n(Y)$ . Finally  $\psi'$  is continuous, for if  $U$  is a closed subset of  $Y$  then, since  $m^{-1}(U) = \psi^{-1}(\psi'^{-1}(U))$ , and  $\psi$  is surjective (see Remark 6.4) and is closed [65, p. 171, No. 6], we have  $\psi'^{-1}(U) = \psi(m^{-1}(U))$ , a closed subset of  $Q$ .  $\square$

## 6.4 Finite-rank-valued fibrations factor through translation-consistent fibrations

In this section our main goal is to prove Theorem 6.6, which we recall here.

**Theorem 6.6.** *Let  $X, Y'$  be compact  $k$ -step nilspaces, with  $Y'$  of finite rank, let  $\psi' : X \rightarrow Y'$  be a fibration, and let  $H \subset \Theta(X)$  be finite. Then there is a compact finite-rank nilspace  $Y$ , an  $H$ -consistent fibration  $\psi : X \rightarrow Y$ , and a fibration  $p : Y \rightarrow Y'$  such that  $\psi' = p \circ \psi$ .*

Let us begin by proving Lemma 6.5 from the introduction, which we recall here as well.

**Lemma 6.5.** *Let  $X, Y$  be compact nilspaces, let  $\psi : X \rightarrow Y$  be a fibration, and let  $\alpha \in \Theta(X)$ . If  $\psi$  is  $\alpha$ -consistent then we can define  $\beta \in \Theta(Y)$  by setting  $\beta(y) = \psi(\alpha(x))$  for any  $x \in \psi^{-1}(y)$ . Moreover, if for every translation  $\alpha \in \Theta(X)$  such that  $\psi$  is  $\alpha$ -consistent, we denote by  $\widehat{\psi}(\alpha)$  the corresponding translation  $\beta \in \Theta(Y)$  thus defined, then, whenever  $\psi$  is  $\{\alpha_1, \alpha_2\}$ -consistent, we have that  $\psi$  is  $\alpha_1\alpha_2$ -consistent and  $\widehat{\psi}(\alpha_1\alpha_2) = \widehat{\psi}(\alpha_1)\widehat{\psi}(\alpha_2)$ .*

Given a map  $g : X \rightarrow X$ , a map  $c : \llbracket n \rrbracket \rightarrow X$ , and a set  $F \subset \llbracket n \rrbracket$ , we denote by  $g^F(c)$  the map  $\llbracket n \rrbracket \rightarrow X$  defined by  $g^F(c)(v) = g(c(v))$  if  $v \in F$  and  $g^F(c)(v) = c(v)$  otherwise.

*Proof.* The  $\alpha$ -consistency implies clearly that  $\beta$  is a well-defined map.

To see that  $\beta$  is a translation, we check that [9, Definition 3.2.27] holds: let  $c \in C^n(Y)$  and  $F$  be any face of codimension 1 in the cube  $\llbracket n \rrbracket$ , and note that by fiber-surjectivity (see [9, Lemma 3.3.9]) there is  $c' \in C^n(X)$  such that  $\psi \circ c' = c$ . Hence  $\beta^F(c) = \psi \circ (\alpha^F(c'))$ . This equality implies that  $\beta^F(c) \in C^n(Y)$ , since  $\psi$  is a morphism and  $\alpha^F(c') \in C^n(X)$ .

Moreover, the translation  $\beta$  is *continuous*, for if  $C \subset Y$  is closed then  $\beta^{-1}(C) = \psi((\psi \circ \alpha)^{-1}(C))$  is closed, since  $\psi \circ \alpha$  is continuous and  $\psi$  is a closed surjective map by [65, p. 171] and Remark 6.4.

The last sentence of the lemma is straightforward to check. □

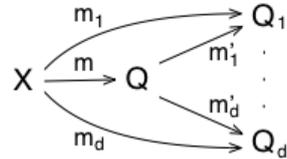
We now turn to the proof of Theorem 6.6. Our strategy is to obtain this as a consequence of Theorem 6.7. We use the following notation.

**Definition 6.14** (Diagonal products). Given maps  $\psi_i : X \rightarrow Y_i, i \in [n]$ , we denote by  $\Delta(\psi_1, \dots, \psi_n)$  their *diagonal product*  $X \rightarrow Y_1 \times \dots \times Y_n$ , defined by  $\Delta(\psi_1, \dots, \psi_n)(x) = (\psi_1(x), \dots, \psi_n(x))$ , and we denote by  $\psi_1 \times \dots \times \psi_n$  their *product*  $X^n \rightarrow Y_1 \times \dots \times Y_n, (x_1, \dots, x_n) \mapsto (\psi_1(x_1), \dots, \psi_n(x_n))$ .

A first fact that follows from Theorem 6.7, and which we use for further results in this section, is the following “common-refinement” lemma.

**Lemma 6.15.** *Let  $X, Q_1, Q_2, \dots, Q_d$  be compact nilspaces, with  $Q_i$  of finite rank for each  $i \in [d]$ , and let  $m_i : X \rightarrow Q_i$  be a fibration for each  $i$ . Then there is a compact finite-rank nilspace  $Q$  and fibrations  $m : X \rightarrow Q, m'_i : Q \rightarrow Q_i$  such that  $m_i = m'_i \circ m$  for each  $i \in [d]$ .*

The lemma yields the following commutative diagram:



*Proof.* Let  $m' = \Delta(m_1, \dots, m_d)$ , and note that this map is a continuous morphism from  $X$  to the product nilspace  $Q_1 \times \dots \times Q_d$ . Applying Theorem 6.7 to  $m'$ , we obtain a compact finite-rank nilspace  $Q$ , a fibration  $m : X \rightarrow Q$ , and a morphism  $\phi : Q \rightarrow Q_1 \times \dots \times Q_d$ , such that  $m' = \phi \circ m$ . We then set  $m'_i = p_i \circ \phi$  for  $i \in [d]$ , where  $p_i : Q_1 \times \dots \times Q_d \rightarrow Q_i$  are the coordinate projections, which are fibrations. We claim that, since  $m_i = m'_i \circ m$  and both  $m_i$  and  $m$  are fiber-surjective, each  $m'_i$  is also fiber-surjective. To see this, fix any fiber  $F' = \pi_{n,Q}^{-1}(x')$ , and note that since  $m$  is fiber-surjective there exists a fiber  $F = \pi_{n,X}^{-1}(x)$  such that  $m(F) = F'$ . Thus  $m'_i(F') = m_i(F)$ , and since  $m_i$  is fiber-surjective, we have that  $m'_i(F')$  is a  $\pi_{n,Q_i}$ -fiber, as claimed. □

For two maps  $\psi_i : X \rightarrow Y_i$ ,  $i = 1, 2$  defined on all of  $X$  (but with  $Y_1, Y_2$  possibly different spaces), we write  $\psi_1 \lesssim \psi_2$  if the partition generated by the latter map refines the partition generated by the former, i.e. if the partitions  $\mathcal{P}_i := \{\psi_i^{-1}(y) : y \in \psi_i(X)\}$ ,  $i = 1, 2$  satisfy that every set in  $\mathcal{P}_1$  is a union of some sets in  $\mathcal{P}_2$ . We write  $\psi_1 \approx \psi_2$  to mean that  $\psi_1 \lesssim \psi_2$  and  $\psi_2 \lesssim \psi_1$  both hold. If  $X, Y$  are  $k$ -step nilspaces and  $\psi : X \rightarrow Y$  is a morphism, then for each  $i \in [k]$  there is a morphism  $\pi_i(X) \rightarrow \pi_i(Y)$ , which we denote by  $(\psi)_{(i)}$ , such that  $(\psi)_{(i)} \circ \pi_{iX} = \pi_{iY} \circ \psi$ ; see [9, Definition 3.3.1 and Proposition 3.3.2]. It is seen straight from the definitions that if  $\psi$  is a fibration then so is  $(\psi)_{(i)}$  for each  $i$ .

Our proof of Theorem 6.6 works by induction on the step  $k$ . A key ingredient in the induction is Lemma 6.17 below. That lemma in turn relies on the fiber-product construction in the category of compact nilspaces, which we detail as follows.

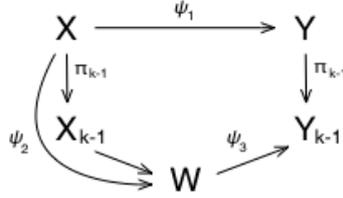
**Lemma 6.16.** *Let  $X^{(1)}, X^{(2)}, X^{(3)}$  be compact nilspaces and let  $\psi_1 : X^{(1)} \rightarrow X^{(3)}$ ,  $\psi_2 : X^{(2)} \rightarrow X^{(3)}$  be fibrations. Then the fiber-product  $X^{(1)} \times_{X^{(3)}} X^{(2)} := \{(x_1, x_2) \in X^{(1)} \times X^{(2)} : \psi_1(x_1) = \psi_2(x_2)\}$  is a compact sub-nilspace<sup>3</sup>  $X^{(1)} \times X^{(2)}$ .*

*Proof.* Let  $Q = X^{(1)} \times_{X^{(3)}} X^{(2)}$ . We have to check that, if for each  $n \geq 0$  we let  $C^n(Q)$  consist of the  $Q$ -valued cubes in  $C^n(X^{(1)} \times X^{(2)})$ , then these cube sets  $C^n(Q)$  satisfy the nilspace axioms. The composition and ergodicity axioms are easily verified. Let us check the corner-completion axiom. Let  $\Delta(c'_1, c'_2) \in \text{Cor}^n(Q)$ , which implies that  $c'_1 \in \text{Cor}^n(X^{(1)})$  and  $c'_2 \in \text{Cor}^n(X^{(2)})$ . Let  $c_2 \in C^n(X^{(2)})$  be a completion of  $c'_2$ . By definition of  $Q$  we have  $\psi_1 \circ c'_1(v) = \psi_2 \circ c_2(v)$  for all  $v \neq 1^n$ . Therefore  $\psi_2 \circ c_2$  is a completion of the corner  $\psi_1 \circ c'_1$ , so, since  $\psi_1$  is a fibration, there exists  $c_1 \in C^n(X_1)$  that completes  $c'_1$  such that  $\psi_1 \circ c_1 = \psi_2 \circ c_2$ . Therefore  $\Delta(c_1, c_2)$  completes  $\Delta(c'_1, c'_2)$ .  $\square$

**Lemma 6.17.** *Let  $X$  be a  $k$ -step compact nilspace, let  $\psi_1 : X \rightarrow Y$  be a fibration, let  $\psi_2 : X \rightarrow W$  be a fibration that factors through  $\pi_{k-1, X}$ , let  $\psi_3 : W \rightarrow Y_{k-1}$  be a fibration such that  $\pi_{k-1, Y} \circ \psi_1 = \psi_3 \circ \psi_2$ , and let  $\psi := \Delta(\psi_1, \psi_2)$ . Then  $\psi$  is a fibration  $X \rightarrow Y \times_{Y_{k-1}} W$ . Moreover  $(\psi)_{(k-1)} \approx (\psi_2)_{(k-1)}$ , and if  $W$  and  $Y$  are of finite rank then so is  $\psi(X)$ .*

<sup>3</sup>The definition of a product nilspace may be recalled from [9, Definition 3.1.2].

The following diagram illustrates the assumptions:



*Proof.* Let  $Q$  denote the fiber-product nilspace  $Y \times_{Y_{k-1}} W$  for the fibrations  $\pi_{k-1, Y}, \psi_3$ . We claim that  $\psi(X) = Q$ . The inclusion  $\psi(X) \subseteq Q$  is clear since  $\pi_{k-1, Y} \circ \psi_1 = \psi_3 \circ \psi_2$ . For the opposite inclusion, let  $(a, b) \in Q$  and  $x \in X$  be any element with  $\psi_2(x) = b$  (such an  $x$  exists by the surjectivity of the fibration  $\psi_2$ ). Letting  $Z_k(X)$  denote the  $k$ -th structure group of  $X$ , for every  $z \in Z_k(X)$  we have  $\psi_2(x + z) = \psi_2(x)$ , since  $\psi_2$  factors through  $\pi_{k-1, X}$ . Now  $\pi_{k-1}(a) = \psi_3(b) = \psi_3(\psi_2(x)) = \pi_{k-1}(\psi_1(x))$ . Thus there exists  $z' \in Z_k(Y)$  such that  $a = \psi_1(x) + z' = \psi_1(x + z)$  for some  $z \in Z_k(X)$ , where the last equality follows from the fiber-surjectivity of  $\psi_1$ . Hence  $\psi(x + z) = (a, b)$ , and the inclusion follows.

Note that from the definitions it is clear that  $\psi$  is a morphism  $X \rightarrow Q$ . We now prove that  $\psi$  is a fibration. Let  $c' \in \text{Cor}^n(X)$ , and let  $\tilde{c} \in C^n(Q)$  be a completion of  $\psi \circ c'$ , thus  $\tilde{c} = \Delta(c_1, c_2)$  for  $c_1 \in C^n(Y)$ ,  $c_2 \in C^n(W)$  completing  $\psi_1 \circ c'$ ,  $\psi_2 \circ c'$  respectively, and satisfying  $\psi_3 \circ c_2 = \pi_{k-1, Y} \circ c_1$ . Since  $\psi_2$  is a fibration, we can complete  $c'$  to  $c_3 \in C^n(X)$  with  $\psi_2 \circ c_3 = c_2$ . Now  $\pi_{k-1, Y} \circ \psi_1 \circ c_3 = \psi_3 \circ \psi_2 \circ c_3 = \psi_3 \circ c_2 = \pi_{k-1, Y} \circ c_1$ , so  $\psi_1 \circ c_3$  and  $c_1$  are in the same  $\pi_{k-1, Y}$ -fiber, so there is  $c'' \in C^n(\mathcal{D}_k(Z_k(Y)))$  such that  $\psi_1 \circ c_3 + c'' = c_1$ . Since  $\psi_1$  is a fibration, its  $k$ -th structure morphism<sup>4</sup>  $Z_k(X) \rightarrow Z_k(Y)$  is surjective, whence there is  $c_4 \in C^n(\mathcal{D}_k(Z_k(X)))$  such that  $\psi_1 \circ (c_3 + c_4) = \psi_1 \circ c_3 + c'' = c_1$ , and since  $\psi_2$  factors through  $\pi_{k-1, X}$  we still have  $\psi_2 \circ (c_3 + c_4) = c_2$ , so  $c_3 + c_4$  completes  $c'$  as required.

To prove the remaining claims in the lemma, it is useful first to give a more precise description of  $Q$  in terms of  $Y$  and  $W$ . We first show that  $Q_{k-1}$  is isomorphic to  $W$  as a compact nilspace. The isomorphism is given by the map  $\varphi : W \rightarrow Q_{k-1}$  defined by  $\varphi(b) = \pi_{k-1, Q}(a, b)$ , for any  $a \in Y$  such that  $\pi_{k-1}(a) = \psi_3(b)$ . This is well-defined because if  $a, a' \in Y$  satisfy  $\pi_{k-1}(a) = \pi_{k-1}(a')$  then  $a' = a + z$  for some  $z \in Z_k(Y)$ , and then from basic properties of the relation  $\sim_{k-1}$  (see [9, Lemma 3.2.4, Remark 3.2.12]) it

<sup>4</sup>The notion of the *structure morphisms* of a nilspace morphism may be recalled from [9, Definition 3.3.1].

follows that  $\pi_{k-1,Q}(a, b) = \pi_{k-1,Q}(a + z, b)$ . The map  $\varphi$  is injective, because if  $\varphi(b) = \varphi(b')$  then the definition of  $\sim_{k-1}$  on  $Q$  and the fact that  $W$  is  $(k-1)$ -step imply that  $b = b'$ . By definition of  $\varphi$  and the fact that  $\pi_{k-1,Q}$  is surjective, we also have that  $\varphi$  is surjective. Let us now check that  $\varphi$  and  $\varphi^{-1}$  are both morphisms. To see that  $\varphi$  is a morphism, note that if  $c \in C^n(W)$  then  $\psi_3 \circ c \in C^n(Y_{k-1})$  and there exists  $c' \in C^n(Y)$  such that  $\pi_{k-1} \circ c' = \psi_3 \circ c$ , whence  $\varphi \circ c = \pi_{k-1,Q} \circ (\Delta(c', c)) \in C^n(Q_{k-1})$ . That  $\varphi^{-1}$  is a morphism follows from the definition of  $\varphi$  and  $Q$  and the fact that  $\pi_{k-1,Q}$  is a fibration. Let us show that  $\varphi^{-1}$  is continuous. Let  $p : Q \rightarrow W$  be the projection  $(a, b) \mapsto b$ , which is continuous and satisfies  $\varphi^{-1} \circ \pi_{k-1,Q} = p$ . Then for any open set  $U \subset Q_{k-1}$ , we have  $\pi_{k-1,Q}^{-1}(\varphi(U)) = p^{-1}(U)$ , and since  $\pi_{k-1,Q}$  is surjective we have  $\varphi(U) = \pi_{k-1,Q}(p^{-1}(U))$ . Since  $p$  is continuous and  $\pi_{k-1,Q}$  is open (see [10, Remark 2.1.7]), we have that  $\varphi(U)$  is open, and the continuity of  $\varphi^{-1}$  follows. We thus have a continuous bijection  $\varphi^{-1}$  between compact metric spaces, so  $\varphi$  is a homeomorphism. Having shown that  $Q_{k-1}$  is isomorphic to  $W$ , let us now complete the description of  $Q$  by describing  $Z_k(Q)$ . We claim that  $Z_k(Q)$  is isomorphic as a compact abelian group to  $Z_k(Y)$ . To see this, it suffices to show that for any fiber  $F$  of  $\sim_{k-1}$  on  $Q$ , as a compact sub-nilspace of  $Q$  this fiber is isomorphic to  $\mathcal{D}_k(Z_k(Y))$  (the isomorphism of the structure groups then follows from known theory; see for instance the end of the proof of [10, Proposition 2.1.9]). Fix  $(a_0, b_0) \in F$  and note that by definition of  $\sim_{k-1}$  on  $Q$  we have that every  $(a, b) \in F$  is  $(a_0 + z, b_0)$  for some unique  $z \in Z_k(Y)$ . Let  $\tau : F \rightarrow Z_k(Y)$  be the map sending  $(a, b)$  to this unique  $z$ . Using that  $Q$  is a sub-nilspace of  $Y \times W$ , it is checked in a straightforward way that  $\tau$  is a compact nilspace isomorphism  $F \rightarrow \mathcal{D}_k(Z_k(Y))$  ( $\tau$  is clearly a bijection, and the cube-preserving properties can be checked using [9, (2.9)]).

We can now prove the last claims in the lemma. From the definition of the isomorphism  $\varphi$  above and the assumption  $\pi_{k-1,Y} \circ \psi_1 = \psi_3 \circ \psi_2$ , it follows that  $(\psi)_{(k-1)} \circ \pi_{k-1,X} = \varphi \circ \psi_2$ , and from this it is easily deduced that  $(\psi)_{(k-1)} \approx (\psi_2)_{(k-1)}$ . Finally, by the above description of  $Q$  it is clear that if  $W$  and  $Y$  are of finite rank then all the structure groups of  $Q$  are Lie groups, so  $Q$  is also of finite rank.  $\square$

For a map  $f : A \rightarrow B$  we write  $a \sim_f a'$  if  $f(a) = f(a')$ . Our proof of Theorem 6.6 uses the next fact.

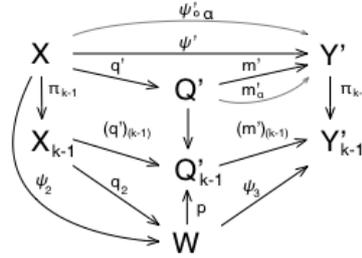
**Lemma 6.18.** *Let  $\psi : X \rightarrow Y$  and  $R : X \rightarrow Y'$  be fibrations with  $\psi \lesssim R$ , let  $\phi_k$  be the  $k$ -th structure morphism of  $\psi$ , and let  $\varphi = \Delta(\psi, (R)_{(k-1)}) \circ \pi_{k-1,X}$ .*

If  $x \sim_\varphi y$  then  $x \sim_R y + z$  for some  $z \in \ker(\phi_k)$ .

*Proof.* If  $x \sim_\varphi y$  then  $\psi(x) = \psi(y)$  and (since  $(R)_{(k-1)} \circ \pi_{k-1,X} = \pi_{k-1,Y'} \circ R$ ),  $R(x) \sim_{k-1} R(y)$ . Then, since  $R$  is a fibration, there exists  $z \in Z_k(X)$  such that  $R(x) = R(y + z)$ . Since  $\psi \lesssim R$ , we deduce that  $\psi(x) = \psi(y + z) = \psi(x) + \phi_k(z)$ . Hence  $z \in \ker(\phi_k)$ .  $\square$

*Proof of Theorem 6.6.* We argue by induction on  $k$ . The result is trivial for  $k = 0$ . Let  $k > 0$  and assume that the result holds for  $k - 1$ .

By Lemma 6.15, there is a finite-rank nilspace  $Q'$ , fibrations  $q' : X \rightarrow Q'$ ,  $m' : Q' \rightarrow Y'$ , and  $m'_\alpha : Q' \rightarrow Y'$  for each  $\alpha \in H$ , with  $\psi' = m' \circ q'$  and  $\psi' \circ \alpha = m'_\alpha \circ q'$  for each  $\alpha$ . Note that  $x \sim_{q'} x'$  implies that  $x \sim_{\psi' \circ \alpha} x'$  for each  $\alpha$ . Let  $H' = \{(\alpha)_{(k-1)} : \alpha \in H\}$ . Let  $q_2 : X_{k-1} \rightarrow W$  be an  $H'$ -consistent fibration on  $X_{k-1}$  obtained by applying the inductive hypothesis to  $(q')_{(k-1)} : X_{k-1} \rightarrow Q'_{k-1}$  (in particular  $q_2 \gtrsim (q')_{(k-1)}$ ), and let  $p : W \rightarrow Q'_{k-1}$  be the fibration such that  $p \circ q_2 = (q')_{(k-1)}$ . Let  $\psi_3$  denote the map  $(m')_{(k-1)} \circ p : W \rightarrow Y'_{k-1}$  (thus, in this inductive application of Theorem 6.6, the objects  $\psi, Y$  from the conclusion of the theorem are denoted here by  $q_2, W$  respectively). Let  $\psi_2 := q_2 \circ \pi_{k-1,X}$ . Note that for each  $\alpha$ , since  $q_2$  is  $(\alpha)_{(k-1)}$ -consistent and  $\pi_{k-1,X}$  is  $\alpha$ -consistent, we have that  $\psi_2$  is  $\alpha$ -consistent. The following diagram illustrates the situation:



We now claim that  $\psi := \Delta(\psi', \psi_2)$  satisfies the required conclusion. We know that  $\psi$  is a fibration, by Lemma 6.17 applied with  $\psi_1 = \psi'$  and  $\psi_2, \psi_3$  defined above. We also know by that lemma that, since  $W$  and  $Y'$  are of finite rank, so is  $\psi(X)$ .

Let us check that  $\psi$  is  $H$ -consistent. Fix any  $\alpha \in H$  and suppose that  $x \sim_\psi y$ . We have to show that  $\alpha(x) \sim_\psi \alpha(y)$ . Firstly we claim that  $\alpha(x) \sim_{\psi'} \alpha(y)$ . To see this, note that since  $(q')_{(k-1)} \lesssim q_2$ , we have  $\Delta(\psi', (q')_{(k-1)} \circ \pi_{k-1,X}) \lesssim \Delta(\psi', q_2 \circ \pi_{k-1,X}) = \psi$ , and then by Lemma 6.18 applied to  $\psi'$  and  $R = q'$ , it follows that  $q'(x) = q'(y+z)$  for some  $z \in \ker(\phi_k)$

(where  $\phi_k$  is the  $k$ -th structure morphism of  $\psi'$ ). Applying  $m'_\alpha$  to both sides of the last equality, we deduce that  $\psi'(\alpha(x)) = \psi'(\alpha(y + z))$ . We now use basic properties of  $k$ -step nilspaces, namely that translations commute with the action of  $Z_k$  [9, Lemma 3.2.37], and the equivariance property involving  $\phi_k$  given by [9, Proposition 3.3.2 and Definition 3.3.1 (ii)], to deduce that  $\psi'(\alpha(y + z)) = \psi'(\alpha(y) + z) = \psi'(\alpha(y)) + \phi_k(z) = \psi'(\alpha(y))$ , so  $\alpha(x) \sim_{\psi'} \alpha(y)$  as claimed. Then, the  $\alpha$ -consistency of  $\psi_2$  (seen above) implies  $\alpha(x) \sim_{\Delta(\psi', \psi_2)} \alpha(y)$ , so  $\psi$  is  $\alpha$ -consistent. Since this holds for all  $\alpha \in H$ , the result follows.  $\square$

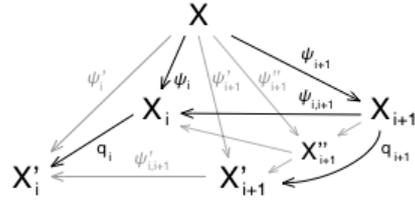
## 6.5 An inverse limit theorem for nilspace systems

As recalled in the introduction, one of the main results in nilspace theory is the inverse limit theorem, which states that every compact nilspace is an inverse limit of compact finite-rank nilspaces. In this section we prove the following stronger version of this result.

**Theorem 6.8.** *Let  $X$  be a compact nilspace and let  $H$  be a finite subset of  $\Theta(X)$ . Then there is a strict inverse system  $(\psi_{i,j} : X_j \rightarrow X_i)_{i,j \in \mathbb{N}, i \leq j}$  of compact finite-rank nilspaces  $X_i$  such that  $X = \varprojlim X_i$  and such that the limit maps  $\psi_i : X \rightarrow X_i$  are all  $\langle H \rangle$ -consistent.*

*Proof.* Recall that by the inverse limit theorem [10, Theorem 2.7.3] there is a strict inverse system  $\{\psi'_{i,j} : X'_j \rightarrow X'_i\}$  such that  $X = \varprojlim X'_i$ . We use the following inductive argument to upgrade this inverse system gradually. Starting with the limit map  $\psi'_1 : X \rightarrow X'_1$ , we use Theorem 6.6 to obtain a finite-rank nilspace  $X_1$ , an  $H$ -consistent fibration  $\psi_1 : X \rightarrow X_1$  and a fibration  $q_1 : X_1 \rightarrow X'_1$  with  $\psi'_1 = q_1 \circ \psi_1$ . Suppose now that we have upgraded the system up to  $i$ , thus we have  $H$ -consistent fibrations  $\psi_j : X \rightarrow X_j$ , fibrations  $q_j : X_j \rightarrow X'_j$ ,  $j \in [i]$ , and also fibrations  $\psi_{j,k} : X_k \rightarrow X_j$  for  $1 \leq j \leq k \leq i$ . Then we apply Lemma 6.15 to  $\psi_i$  and  $\psi'_{i+1}$  to obtain a fibration  $\psi''_{i+1} : X \rightarrow X''_{i+1}$  through which  $\psi_i$  and  $\psi'_{i+1}$  both factor. Then we apply Theorem 6.6 to  $\psi''_{i+1}$  to refine it to an  $H$ -consistent fibration  $\psi_{i+1} : X \rightarrow X_{i+1}$ . Continuing this way, the result follows.  $\square$

The following diagram illustrates the inductive step:



Recall that a measure-preserving action of a countable discrete group  $G$  on a probability space  $(\Omega, \mathcal{A}, \mu)$  is *ergodic* if  $\forall A \in \mathcal{A}, (\forall g \in G, \mu((g \cdot A) \Delta A) = 0) \Rightarrow \mu(A) \in \{0, 1\}$ .

We obtain the following consequence of Theorem 6.8.

**Theorem 6.19.** *Let  $X$  be a  $k$ -step compact nilspace and let  $H$  be a finitely generated subgroup of  $\Theta(X)$  acting ergodically on  $X$  (relative to the Haar probability measure on  $X$ ). Then the nilspace system  $(X, \mu, H)$  is an inverse limit of  $k$ -step nilsystems.*

This follows immediately by combining Theorem 6.8 with the following basic lemma.

**Lemma 6.20.** *Let  $Y$  be a  $k$ -step compact finite-rank nilspace, and let  $H$  be a finitely generated subgroup of  $\Theta(Y)$  acting ergodically on  $Y$ . Then the  $k$ -step nilpotent Lie group  $\langle \Theta(Y)^0, H \rangle$  acts transitively on  $Y$ .*

*Remark 6.21.* Note that no assumption on  $Y$  is made other than that it is of finite rank, hence no additional assumption on  $X$  is needed in Theorem 6.19. In Lemma 6.20 the ergodicity of the action of  $H$  indeed suffices to deduce the claimed transitivity, but to show this we use a deep result, namely the transitivity of the action of the identity component  $\Theta(Y)^0$  on each connected component of  $Y$ , established in [1, Corollary 3.3].

*Proof.* By [1, Corollary 3.3] (see also [10, Corollary 2.9.12]), if there is only one component in  $Y$  then we are done. Suppose, then, that there are at least two components. It suffices to prove the claim that for every two components  $C, C' \subset Y$  there is  $g \in H$  such that  $\mu(g(C) \cap C') > 0$ . Indeed, if this holds then for any  $y, y' \in Y$  there is  $g' \in H$ , and some  $x$  in the component  $C(y)$  containing  $y$ , such that  $g' \cdot x \in C(y')$ . Then, by the transitivity of  $\Theta(Y)^0$  on  $C(y), C(y')$ , there are  $\beta, \beta' \in \Theta(Y)^0$  with  $\beta(y) = x$  and  $\beta' \cdot g' \cdot x = y'$ , so the element  $g = \beta' g' \beta$  satisfies  $g \cdot y = y'$ , and the transitivity of  $\langle \Theta(Y)^0, H \rangle$  follows.

To prove the claim, note first that since the compact nilspace  $Y$  has finite rank, it is a finite-dimensional manifold (see [10, Lemma 2.5.3]) and is therefore locally connected, so each of its connected components is an open set [65, Theorem 25.3]. Since the Haar measure  $\mu$  on  $Y$  is strictly positive [10, Proposition 2.2.11], every component has positive measure. Let  $C, C'$  be any two such components, and suppose for a contradiction that for every  $g \in H$  we have  $\mu(g(C) \cap C') = 0$ . Then the  $H$ -invariant set  $\cup_{g \in H} g \cdot C$  is disjoint from  $C'$  up to a  $\mu$ -null set, so it is an  $H$ -invariant set of measure strictly between 0 and 1, contradicting the ergodicity of  $H$ .  $\square$

*Remark 6.22.* As mentioned in the introduction, the results in this section are related to a result of Gutman, Manners and Varjú, namely the version of [42, Theorem 1.30] for nilspace systems mentioned in their paper after their Theorem 1.30. We obtain Theorem 6.19 as a swift consequence of the fundamental factorization results for morphisms from previous sections, and this makes our proof markedly different from the arguments in [42]. Moreover, Theorem 6.19 is a special case of Theorem 6.8, which is a direct generalization of the inverse limit theorem [1, Theorem 4], and which concerns arbitrary (not just ergodic) finitely generated nilspace systems, whereas [42, Theorem 1.30] concerns minimal group actions. Thus the results in this section and [42, Theorem 1.30] are complementary. We also remark that it would be possible to obtain Theorem 6.19 from [42, Theorem 1.30] if an adequate equivalence between ergodicity (in the measure-theoretic setting) and minimality (in the topological setting) were established for nilspace systems, but this is beyond the scope of this chapter.

# Chapter 7

## A note on the bilinear Bogolyubov theorem: transverse and bilinear sets

First published in Proceedings of the American Mathematical Society in 2019, published by American Mathematical Society. This work was written in collaboration with Pierre-Yves Bienvenu and Ángel D. Martínez. For the original publication, see [6].

### 7.1 Introduction

A simple exercise shows that any nonempty subset  $A \subset \mathbb{F}_p^n$  that is closed under addition is a linear subspace, that is, the zero set of a family of linear forms. Indeed, denoting as usual

$$A \pm A = \{a \pm b : (a, b) \in A^2\},$$

this amounts to the claim that  $A + A = A \neq \emptyset$  if and only if  $A$  is a subspace (and analogously for  $A - A$ ). Considering a large number of summands, if  $0 \in A$ , one will eventually get  $\text{span}(A)$ , the linear subspace generated by  $A$ . This may require an unbounded number of summands as the dimension  $n$  or the prime  $p$  tends to infinity.

The following classical result states that a bounded number of summands already suffices to produce a rather large subspace of  $\text{span}(A)$  if  $A$  has positive density.

**Theorem 7.1** (Bogolyubov). *Let  $A \subset \mathbb{F}_p^n$  be a subset of density  $\alpha > 0$ , that is,  $|A| = \alpha p^n$ . Then  $2A - 2A$  contains a vector space of codimension  $c(\alpha) = O(\alpha^{-2})$ .*

Bogolyubov’s original paper [8] deals with  $\mathbb{Z}/N\mathbb{Z}$ , but the ideas translate to finite  $\mathbb{F}_p$ -vector spaces. Note that if  $A$  is a vector space, its codimension is  $\log_p \alpha^{-1}$ . As a consequence,  $c(\alpha) \geq \log_p \alpha^{-1}$ . Sanders [79] improved the bound in the statement to a nearly optimal  $c(\alpha) = O(\log^4 \alpha^{-1})$ . Recently, bilinear versions of this result by Bienvenu and Lê [5] and, independently, Gowers and Milićević [33] have appeared. Let us now state this bilinear Bogolyubov theorem. We need to introduce a piece of useful notation (cf. [5]).

Given a set  $A \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  we define the vertical sum or difference as

$$A \overset{V}{\pm} A := \{(x, y_1 \pm y_2) : (x, y_1), (x, y_2) \in A\}.$$

The set  $A \overset{H}{\pm} A$  is defined analogously but fixing the second coordinate. Then we define  $\phi_V$  as the operation

$$A \mapsto (A \overset{V}{+} A) \overset{V}{-} (A \overset{V}{+} A)$$

and  $\phi_H$  similarly. The theorem proved in [5] is the following.

**Theorem 7.2** (Bienvenu and Lê, [5]). *Let  $\delta > 0$ , then there is  $c(\delta) > 0$  such that the following holds. For any  $A \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  of density  $\delta$ , there exists  $W_1, W_2 \subseteq \mathbb{F}_p^n$  subspaces of codimension  $r_1$  and  $r_2$  respectively and bilinear forms  $Q_1, \dots, Q_{r_3}$  on  $W_1 \times W_2$  such that  $\phi_H \phi_V \phi_H(A)$  contains*

$$\{(x, y) \in W_1 \times W_2 : Q_1(x, y) = \dots = Q_{r_3}(x, y) = 0\} \tag{7.1}$$

where  $\max\{r_1, r_2, r_3\} \leq c(\delta)$ .

The rather weak bound obtained in [5] and [33] was improved recently by Hosseini and Lovett [47] to the nearly optimal  $c(\delta) = O(\log^{O(1)} \delta^{-1})$ , at the cost of replacing  $\phi_H \phi_V \phi_H$  by a slightly longer sequence of operations.

We call a set  $A \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  *transverse* if it satisfies  $A \overset{V}{+} A = A \overset{H}{+} A = A$ . In connection with the result above the following natural problem arose: characterise transverse sets. Note that  $A \overset{V}{+} A = A$  if and only if there exist

a set  $B$  and for each  $x \in B$  a subspace  $V_x$  such that  $A = \bigcup_{x \in B} \{x\} \times V_x$ ; similarly  $A \overset{H}{+} A = A$  if and only if there exist a set  $C$  and for each  $y \in C$  a subspace  $W_y$  such that  $A = \bigcup_{y \in C} W_y \times \{y\}$ . Although nothing more may be said about a set admitting either of these decompositions (the assignment  $x \mapsto V_x$  may be perfectly random), their simultaneous validity could result in strong structural properties.

The most natural examples of transverse sets are what we call *bilinear* sets, that is, zero sets of linear and bilinear forms as in (7.1). In view of the linear case, it is tantalizing to suspect that they are the only possible examples. Theorem 7.2 only shows that any transverse set  $A$  of density  $\alpha$  contains a bilinear subset defined by  $c(\alpha)$  linear and bilinear forms.

In this chapter, we find transverse, non-bilinear sets  $A \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  for any  $(p, n)$  except  $p = 2$  and  $n = 2$  where it is possible to list all transverse sets and check that they are bilinear. Thus the analogy to the linear case breaks down.

For any transverse set  $P \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$ , let  $P_x = \{y \in \mathbb{F}_p^n : (x, y) \in P\}$  be the vertical *fiber* above  $x \in \mathbb{F}_p^n$ . Notice that a non-empty fiber is a subspace. We now state our main result.

**Theorem 7.3.** *Let  $p$  be a prime and  $n$  a positive integer.*

1. *For any prime  $p \geq 5$  and dimension  $n \geq 2$ , there exists a transverse, non-bilinear set  $P \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  for which  $P_x$  contains a hyperplane for any  $x$ .*
2. *For all but finitely many primes  $p$  and dimensions  $n$ , we can find transverse, non-bilinear sets  $P \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  where  $P_x$  is a space of dimension 1 for any  $x$ .*

It remains to address  $p = 3$ , which we are able to do with an explicit, algebraic counter-example.

**Proposition 7.4.** *Let  $P \subset \mathbb{F}_3^2 \times \mathbb{F}_3^2$  be the set of  $((x_1, x_2), (y_1, y_2))$  satisfying*

$$\begin{cases} x_1 y_1^2 + x_2 y_2^2 = 0 \\ x_1^2 y_1 + x_2^2 y_2 = 0 \end{cases} \quad (7.2)$$

*is transverse but not bilinear.*

Nevertheless, we show that transversity together with an extra largeness hypothesis implies bilinearity for small characteristics.

**Theorem 7.5.** *Let  $P \subset \mathbb{F}_p^n \times \mathbb{F}_p^n$  be a transverse set such that  $P_x$  contains a hyperplane for any  $x$ . Then it is bilinear provided that the prime  $p = 2$  or  $3$ .*

We point out that in the above theorem, the number of bilinear forms required to write  $P$  as a bilinear set may not be bounded, whereas the density is bounded below. An example will appear in Proposition 7.9. This in sharp contrast to Theorem 7.2, which asserts that  $P$  contains a bilinear set defined with a bounded number of bilinear forms.

A question that remains open, however, is whether Theorem 7.2 may be quantitatively improved, or proven in a simpler way, for transverse sets. Note that the single hypothesis  $P \overset{V}{+} P = P$  (“partial transversity”) does not seem to lead to such an improvement, since most of the difficulty in the three known proofs [5, 33, 47] consists in handling such a set. In addition, note that for any  $A \subset \mathbb{F}_p^n$ , the set  $P = A \times \mathbb{F}_p^n$  has the same density in  $\mathbb{F}_p^n \times \mathbb{F}_p^n$  as  $A$  in  $\mathbb{F}_p^n$  and it is a “partial transverse” set, so the bilinear Bogolyubov theorem for such sets is equivalent to the linear Bogolyubov, where Sanders’ aforementioned bound is nearly optimal.

The chapter is organized as follows. In Section 7.2 we study the explicit algebraic counterexample. In Section 7.3 we provide a qualitative classification of transverse sets  $P$  for which  $P_x$  contains a hyperplane; this entails a proof for Theorem 7.5 and the basis for the proof Theorem 7.3, which can be finally found in Section 7.4.

## 7.2 Proof of proposition 7.4

Consider  $P \subset \mathbb{F}_3^2 \times \mathbb{F}_3^2$  to be the set defined by the system (7.2). We want to show that we cannot have

$$P = \{(x, y) \in W_1 \times W_2 : Q_1(x, y) = \dots = Q_{r_3}(x, y) = 0\}$$

for any subspaces  $W_1, W_2$  and any bilinear forms  $Q_1, \dots, Q_{r_3}$  so by contradiction suppose that it is the case.

The set  $P$  is easy to describe: indeed, if  $(x, y) \in P$ , then either  $x_1y_1 = x_2y_2 = 0$  or  $x_1y_1x_2y_2 \neq 0$ . Let

$$P_0 = \{(x_1, x_2, y_1, y_2) \in \mathbb{F}_3^2 \times \mathbb{F}_3^2 : x_1y_1 = 0 \text{ and } x_2y_2 = 0\}$$

and

$$P_1 = \{(x_1, x_2, y_1, y_2) \in \mathbb{F}_3^2 \times \mathbb{F}_3^2 : x_1 + x_2 = 0 \text{ and } y_1 + y_2 = 0\}$$

which is a subset of  $P$  and contains the set of points where  $x_1y_1x_2y_2 \neq 0$  since  $z^2 \equiv 1 \pmod{3}$  provided  $z \not\equiv 0 \pmod{3}$ . Therefore  $P = P_0 \cup P_1$ .

Let us check that this set satisfies both conditions  $P \overset{V}{+} P = P$  and  $P \overset{H}{+} P = P$ . By symmetry it is enough to check that  $P \overset{H}{+} P = P$ . The cases where the points  $(x_1, x_2, y_1, y_2), (x'_1, x'_2, y_1, y_2)$  are both in  $P_0$  or  $P_1$  are easily verified and if one is in  $P_0$  and the other in  $P_1$  then  $(x_1+x'_1)y_1^2 + (x_2+x'_2)y_2^2 = 0$  by the first equation in (7.2) and

$$(x_1 + x'_1)^2y_1 + (x_2 + x'_2)^2y_2 = 2(x_1x'_1y_1 + x_2x'_2y_2) = 0$$

using the fact that either  $(x_1, x_2, y_1, y_2)$  or  $(x'_1, x'_2, y_1, y_2)$  is in  $P_0$ .

The fact that  $P_1 \subset P$  shows that  $W_1, W_2$  are at least one dimensional but this is not enough. Indeed, suppose they are one dimensional, then  $W_1$  and  $W_2$  should be precisely  $\{(x_1, x_2) : x_1 + x_2 = 0\}$  and  $\{(y_1, y_2) : y_1 + y_2 = 0\}$  but, for example,  $(1, 0, 0, 0) \notin W_1 \times \mathbb{F}_3^2$  and  $(0, 0, 1, 0) \notin \mathbb{F}_3^2 \times W_2$  and they belong to  $P$ . As a consequence  $W_1 = W_2 = \mathbb{F}_3^2$ . Let us show that no bilinear form other than the trivial one can vanish on this  $P$ . Suppose

$$xQy = \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 0$$

for all  $(x, y) \in P$  or, alternatively,

$$xQy = a_{11}x_1y_1 + a_{12}x_1y_2 + a_{21}x_2y_1 + a_{22}x_2y_2 = 0.$$

On  $P_0 \subset P$ , this equation boils down to

$$a_{12}x_1y_2 + a_{21}x_2y_1 = 0$$

but now  $(0, 1, 1, 0), (1, 0, 0, 1) \in P_0$  imply  $a_{12} = a_{21} = 0$ . On the other hand  $(1, 2, 1, 2) \in P_1$  imply  $a_{11} + a_{22} = 0$ . This implies that if  $P$  is a bilinear

set then it must be the zero set of  $Q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  (or equivalently,  $-Q$ ). But this is impossible because  $(x, y) = (1, 1, 1, 1) \notin P$  and yet  $xQy = 0$ . So the only option left is that  $P = \mathbb{F}_3^2 \times \mathbb{F}_3^2$  and this is not the case either. As an aside, note that  $\dim P_x$  is not constant on  $\mathbb{F}_p^2 \setminus \{0\}$ , so this example is different from the generic ones mentioned in Theorem 7.3.

### 7.3 Proof of proposition 7.5

In this section, we prove Theorem 7.5. Let  $V_1$  and  $V_2$  be two  $\mathbb{F}_p$ -vector spaces, and we slightly generalise the above discussion to transverse sets of  $V_1 \times V_2$ . Let  $P \subset V_1 \times V_2$  be a set. Write  $P_x = \{y \in V_2 : (x, y) \in P\}$  and  $P_y = \{x \in V_1 : (x, y) \in P\}$  for the vertical and horizontal fibers, respectively, borrowing the notation from [33]. We now characterise transversity by some rigidity property of the map  $x \mapsto P_x$ .

**Lemma 7.6.** *A set  $P \subset V_1 \times V_2$  is transverse if, and only if, the map  $x \mapsto P_x$  satisfies the following properties.*

1. For any  $x$ , the set  $P_x$  is the empty set or a subspace and  $P_x \subset P_0$ .
2. For any  $x \neq 0$ , the set  $P_x$  depends only on the class  $[x] \in \mathbb{P}(V_1) = V_1^*/\mathbb{F}_p^*$  of  $x$  in the projective space.
3. If  $[z]$  is on the projective line spanned by  $[x]$  and  $[y]$ , we have  $P_z \supset P_x \cap P_y$ .

*Proof.* Let  $P \subset V_1 \times V_2$  be transverse. Let  $x \in V_1$ . Because  $P + P = P$ , we find that  $P_x + P_x = P_x$ , so  $P_x$  is empty or a subspace. Similarly  $P_y$  is empty or a subspace. Let  $y \in P_x$ . Then  $x \in P_y$  which implies  $0 \in P_y$ , hence  $y \in P_0$ , which proves the first point. Further,  $(\lambda x, y) \in P$  for any  $\lambda \neq 0$  as well, thus  $y \in P_{\lambda x}$ ; this shows the second point. To prove the third point, suppose without loss of generality that  $z = x + \lambda y$  for some  $\lambda \in \mathbb{F}_p$ . Let  $w \in P_x \cap P_y$ . Thus both  $x$  and  $y$  belong to the subspace  $P_w$ , so that  $z \in P_w$  too, which means that  $w \in P_z$ , concluding the proof.

We now prove the converse. Let a set  $P \subset V_1 \times V_2$  satisfy the three properties. The first point means that  $P + P = P$ . The horizontal stability follows from the second and third points.  $\square$

We will need another lemma. Recall the notation  $\mathbb{P}(V) = V^*/\mathbb{F}^*$  for the projective space of an  $\mathbb{F}$ -vector space  $V$ . We will often omit the distinction between  $x \in V$  and its class  $[x] \in \mathbb{P}(V)$ . It will be convenient to use the language of projective geometry, of which we assume some basic facts, such as the fact that any two (projective) lines of a (projective) plane intersect.

**Lemma 7.7.** *Suppose that  $\xi : \mathbb{P}(V_1) \rightarrow \mathbb{P}(V_2)$  has the property that for any  $x, y, z$  in  $V_1$  such that  $z \in \text{span}(x, y)$ , we have  $\xi(z) \in \text{span}(\xi(x), \xi(y))$ . Then  $\xi$  is either constant or injective.*

*Proof.* First we deal with the case where  $\mathbb{P}(V_1)$  is a projective line (i.e.  $\dim V_1 = 2$ ). Suppose  $\xi$  is not injective, thus there exists two non-collinear vectors  $x$  and  $y$  of  $V_1$  such that  $\xi(x) = \xi(y)$ . Now  $(x, y)$  is a basis of  $V_1$ , so for any  $z \in \mathbb{P}(V_1)$ , by the defining property of  $\xi$ , we have  $\xi(z) = \xi(x) = \xi(y)$ . So  $\xi$  is constant.

Now suppose  $\dim V_1 \geq 3$ . We already know that  $\xi$  is either injective or constant on any projective line. Assume that overall  $\xi$  is neither injective nor constant. This means that there exist two distinct points  $x, y$  such that  $\xi(x) = \xi(y)$ , and a third point  $z$  satisfying  $\xi(z) \neq \xi(x)$ . This implies that  $x, y, z$  are not (projectively) aligned, so they span a projective plane. The reader may now wish to follow the proof on Figure 7.1. Take a point  $w \notin \{y, z\}$  on the line  $(yz)$  spanned by  $y$  and  $z$ . Because  $\xi$  is a bijection on both lines  $(yz)$  and  $(xz)$ , and the image of both lines under  $\xi$  being the same namely  $(\xi(y)\xi(z))$ , we can find  $w' \notin \{x, z\}$  on  $(xz)$  such that  $\xi(w) = \xi(w') \neq \xi(x)$ . Now consider the intersection  $u = (ww') \cap (xy)$  in the projective plane  $\text{span}(x, y, z)$ . Then we have  $\xi(u) = \xi(x) = \xi(y) \neq \xi(w)$ , so that on the line  $(ww')$  the map  $\xi$  is neither constant nor injective, a contradiction. □

Finally, we recall the fundamental theorem [77, Théorème 7] of projective geometry.

**Theorem 7.8.** *Suppose that  $\xi : \mathbb{P}(V_1) \rightarrow \mathbb{P}(V_2)$  is injective and has the property that for any  $x, y, z$  in  $V_1$  such that  $z \in \text{span}(x, y)$ , we have  $\xi(z) \in \text{span}(\xi(x), \xi(y))$  (i.e. it maps points on a line to points on a line). Further, suppose that  $\dim V_1 \geq 3$ . Then  $\xi$  is a projective map, that is, there exists a linear injection  $f : V_1 \rightarrow V_2$  such that  $\xi([x]) = [f(x)]$  for any  $x \in V_1$ .*

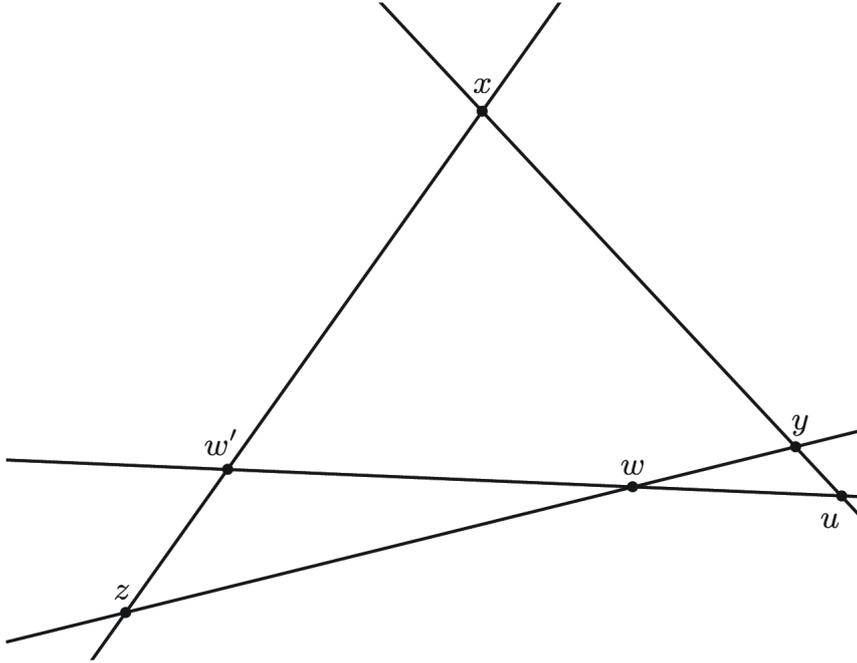


Figure 7.1: Proof of Lemma 7.7.

Here we require the field  $\mathbb{F}_p$  to be a prime field; on a non prime finite field  $\mathbb{F}_q$ , we would need to incorporate Frobenius field automorphisms.

Note that the result holds even if  $\dim V_1 = 2$  in the case where  $p = 2$  or  $3$ . Indeed, the number of bijections between two projective lines is  $(p + 1)!$ . On the other hand, since there are  $(p^2 - 1)(p^2 - p)$  linear bijections between any two given planes, the number of projective bijections is  $(p^2 - 1)(p^2 - p)/(p - 1) = (p + 1)p(p - 1)$ . These two numbers are equal when  $p \in \{2, 3\}$  which forces any bijection to be projective.

Now we state this section’s main result.

**Proposition 7.9.** *Let  $P \subset V_1 \times V_2$  be a transverse set. Suppose that  $\text{codim}_{V_2} P_x \leq 1$  for any  $x \in V_1$ . Then one of the three alternatives holds.*

1. *There exist a subset  $W \subset V_1$  which is empty or a subspace, and a hyperplane  $H \leq V_2$ , such that  $P = W \times V_2 \cup V_1 \times H$ .*
2. *There exists a bilinear form  $b$  on  $V_1 \times V_2$  such that  $P = \{(x, y) \in V_1 \times V_2 : b(x, y) = 0\}$ .*

3. We have  $p \geq 5$  and the minimal codimension of a subspace  $W \leq V_1$  such that  $W \times V_2 \subset P$  is exactly 2.

Observe that this implies Theorem 7.5, since the first two alternatives correspond to bilinear sets. This is obvious for the second one. For the first one, if  $W$  is empty, it is clear; otherwise, let  $a_1, \dots, a_k$  be linearly independent linear forms such that  $W$  is the intersection of their kernels, and  $\ell$  be a linear form that defines  $H$ . Then

$$P = \{(x, y) \in V_1 \times V_2 : a_1(x)\ell(y) = \dots = a_k(x)\ell(y) = 0\}.$$

One can check that one can not write  $P$  as in (7.1) with  $W_1$  and  $W_2$  other than  $V_1$  and  $V_2$  and with  $r_3 \neq k$ , and  $k$  may tend to infinity with  $\dim V_1$ , while the density is bounded below by  $1/p$ , but this is not a contradiction with Theorem 7.2, since  $P$  contains (but may not be equal to) the Cartesian product  $V_1 \times H$ . As for the last alternative, Theorem 7.3 (ii) indicates that it is not necessarily a bilinear set.

*Proof.* Without loss of generality suppose that  $P_0 = V_2$ . Indeed, otherwise  $P_0$  is a hyperplane  $H$  and Lemma 7.6 (i) shows that  $P = V_1 \times H$ . Let  $(y, \phi) \mapsto y \cdot \phi$  be a bilinear form of full rank on  $V_2 \times V_2$ . For  $\phi \in V_2$  let  $\phi^\perp = \{y \in V_2 : y \cdot \phi = 0\}$ . The hypothesis allows us to write  $P_x = \xi(x)^\perp$  for some vector  $\xi(x) \in V_2$  that is defined uniquely up to homothety. The proof consists in deriving rigidity properties for  $\xi$  which will eventually make it linear or constant.

With this new notation, the assumption just made implies that  $\xi(0) = 0$ . Further, the second point of Lemma 7.6 means that  $\xi(x)$  depends only on  $[x]$  for  $x \neq 0$  and the third point of that lemma yields that whenever  $[z]$  is on the projective line spanned by  $x$  and  $y$ , we have  $\xi(z) \in \text{span}(\xi(x), \xi(y))$ . Using Lemma 7.6 (iii), one can see that the set

$$W := \{x \in V_1 : P_x = V_2\}$$

is a vector subspace. If  $W = V_1$ , we have  $P = V_1 \times V_2$  so the first alternative holds. Otherwise  $W \neq V_1$ . Let  $V'_1 = V_1/W$  and observe that for any given  $x - y = w \in W$ , we have  $\xi(x) \in \text{span}(\xi(y), \xi(w)) = \text{span}(\xi(y))$ , that is,  $\xi(x) = \xi(y)$  up to homothety, so that  $\xi$  descends to a map  $\xi' : \mathbb{P}(V_1/W) \rightarrow \mathbb{P}(V_2)$ . Thus  $\xi'$  is a map  $\mathbb{P}(V'_1) \rightarrow \mathbb{P}(V_2)$  that maps aligned points to aligned points. If  $\text{codim } W = 1$ , it follows that  $[\xi(x)]$  is a nonzero constant vector  $\phi$

for  $x \in V \setminus W$  so the first alternative is true with  $H = \phi^\perp$ . In the following we assume that  $\text{codim } W \geq 2$ .

By construction  $\xi'$  satisfies the hypothesis of Lemma 7.7, therefore it should be either constant or injective. If  $\xi'$  is constant on  $\mathbb{P}(V'_1)$ , we can take  $\xi(x)$  to be a nonzero constant vector  $\phi \in V_2$  for all  $x \in W^\perp$ , while  $\xi(x) = 0$  on  $W$ . Let  $H$  denote the subspace orthogonal to  $\phi$ . Then  $P = W \times V_2 \cup V_1 \times H$ , which is the first alternative. We suppose now that  $\xi'$  is injective. If  $\dim V'_1 = 2$  and  $p \geq 5$ , the third alternative is true. Now suppose that  $\dim V'_1 \geq 3$  or that  $\dim V'_1 = 2$  and  $p \in \{2, 3\}$ . Theorem 7.8 and the remark following it imply that  $\xi$  comes from an injective linear map  $V'_1 \rightarrow V_2$ , which we extend to a linear map  $f : V_1 \rightarrow V_2$  with kernel  $W$ . In the particular case  $p \in \{2, 3\}$  this proves proposition 7.5. Then  $P$  is the zero set of the bilinear form  $(x, y) \mapsto f(x) \cdot y$ , which concludes the proof of Proposition 7.9.  $\square$

## 7.4 Proof of proposition 7.3

First we introduce a new notation and a characterisation of bilinear sets. For a set  $P \subset V_1 \times V_2$  satisfying  $P_{0.} = V_2$  and  $P_{.0} = V_1$ , let  $\text{Ann}(P)$  be the subspace of the space  $\mathcal{B}(V_1, V_2)$  of bilinear forms on  $V_1 \times V_2$  that consist of the forms that vanish on  $P$ . For a set  $M \subset \mathcal{B}(V_1, V_2)$ , let  $\text{Orth}(M)$  be the (bilinear) subset  $V_1 \times V_2$  where all the forms of  $M$  vanish simultaneously. Thus in general  $P \subset \text{Orth}(\text{Ann}(P))$ , while the equality holds if and only if  $P$  is a bilinear set.

Now we prove Theorem 7.3 (i), that is, we show that some transverse sets satisfying the third alternative of Proposition 7.9 are not bilinear. Let  $W$  be a subspace of codimension 2 in  $V_1$ . Let  $V'_1 = V_1/W$  and  $\xi' : \mathbb{P}(V'_1) \rightarrow \mathbb{P}(V_2)$  be a non-projective bijection onto a projective line; as observed after Theorem 7.8, this is possible when  $p \geq 5$  since there are  $(p+1)!$  bijection between any two projective lines but only  $(p+1)p(p-1)$  projective maps between them. Extend naturally  $\xi'$  to a map  $\xi : V_1 \rightarrow V_2$  that induces  $\xi'$  by projection and let  $P = \bigcup_{x \in V_1} \{x\} \times \xi(x)^\perp$ . Thanks to the characterization from Lemma 7.6, we see that  $P$  is transverse.

Let  $b \in \text{Ann}(P)$ , one can write  $b(x, y) = f(x) \cdot y$  where  $f$  is a linear map  $V_1 \rightarrow V_2$  vanishing on  $W$ ; thus it induces a linear map  $f' : V'_1 \rightarrow V_2$  satisfying  $f'(x) \in \text{span}(\xi'(x))$  for  $x \in V'_1 \setminus \{0\}$ . Recall that  $W$  has codimension two

$x$	(1, 0, 0)	(0, 1, 0)	(0, 0, 1)	(1, 1, 0)	(1, 0, 1)	(0, 1, 1)	(1, 1, 1)
$\sigma(x)$	(1, 0, 0)	(0, 1, 0)	(0, 0, 1)	(1, 1, 0)	(0, 1, 1)	(1, 1, 1)	(1, 0, 1)

 Figure 7.2: Table defining the permutation  $\sigma$ .

and therefore  $f'$  has either rank 2, 1 or 0 respectively. In the first case  $f'$  does not vanish on  $V_1' \setminus \{0\}$  and we get  $\xi'(x) = [f'(x)]$  for any  $x \neq 0$ . As a consequence  $\xi'$  is projective, which is false. The second possibility can be ruled out too. Indeed, in this case the image of  $f'$  is a line  $\ell$ , i.e. a vector space of dimension one. As a consequence  $\xi'([x])$  will have the same constant value for any  $x \in V_1' \setminus \ker f'$  which contradicts the fact that it is injective by construction. The only possibility left is  $f' = 0$ . This proves that  $\text{Ann}(P) = \{0\}$  and so  $\text{Orth}(\text{Ann}(P)) = V_1 \times V_2 \neq P$ , which means that  $P$  is not bilinear, concluding the proof of Theorem 7.3 (i).

We now show Theorem 7.3 (ii). Here we think of  $V_1$  and  $V_2$  as two  $n$ -dimensional  $\mathbb{F}_p$ -vector spaces. Recall the characterisation of transverse sets obtained in Lemma 7.6. In particular, if  $P_x \cap P_y = \{0\}$  for any  $[x] \neq [y]$ , the third property of that Lemma 7.6 is vacuous. As a consequence the characterization of transverse sets it provides is easier to satisfy. One can achieve this, for instance, by taking a bijection  $\sigma : \mathbb{P}(V_1) \rightarrow \mathbb{P}(V_2)$  and letting  $P$  be the transverse set

$$P_\sigma = \{0\} \times V_2 \cup \bigcup_{x \in \mathbb{P}(V_1)} \text{span}(x) \times \text{span}(\sigma(x))$$

where  $\text{span}$  denotes the linear span in  $V_1$  or  $V_2$ .

With the assistance of a computer, it is possible to find  $\sigma$  such that  $P_\sigma \neq \text{Orth}(\text{Ann}(P_\sigma))$  for small  $p$  and  $n$ . For instance, for  $p = 2$  and  $n = 3$  one can let  $\sigma$  be the permutation of  $\mathbb{P}(\mathbb{F}_2^3) = \mathbb{F}_2^3 \setminus \{(0, 0, 0)\}$  defined in Figure 2. The above characterization implies that  $P_\sigma$  is not a bilinear set. Indeed, we find that

$$\text{Ann}(P) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \right\}$$

so that  $\text{Orth}(\text{Ann}(P))$  contains  $((1, 0, 0), (0, 1, 0))$ , an element which does not belong to  $P$ , so  $P$  is not bilinear.

For general  $p$  and  $n$ , the following non-constructive counting argument shows that there exists a permutation  $\sigma$  such that  $P_\sigma$  is not bilinear. On the one hand, the number of points in a projective space can be bounded from below, i.e.

$$|\mathbb{P}(V_1)| = \frac{p^n - 1}{p - 1} \geq p^{n-1}.$$

Thus there are at least

$$p^{n-1}! \geq \left(\frac{p^{n-1}}{e}\right)^{p^{n-1}}$$

transverse sets  $P_\sigma$ , where we used the inequality  $e^m \geq m^m/(m!)$  valid for any positive integer  $m$ . On the other hand, the number of subspaces  $M$  of  $\mathcal{B}(V_1, V_2)$  can be bounded from above as follows. The space of bilinear forms  $\mathcal{B}(V_1, V_2)$  has dimension  $n^2$  and contains  $p^{n^2}$  elements. The number of subspaces of dimension  $k$  can be bounded by  $p^{kn^2}$ . Recall that there exists the same number of spaces of dimension  $k$  and  $n^2 - k$  so the total number of subspaces can be bounded above by  $\sum_{k=0}^{n^2} |\{H \subset \mathcal{B}(V_1, V_2) : \dim(H) = k\}| \leq 2 \frac{p^{n^4/2+n^2}-1}{p^{n^2}-1}$  (if  $n$  is even this is clear and if it is odd the number of subspaces of dimension  $(n^2 + 1)/2$  is only counted once and the bound obtained is smaller than the one given). Now we argue by contradiction. The absence of counterexamples would force  $(p, n \geq 2)$

$$\left(\frac{p^{n-1}}{e}\right)^{p^{n-1}} \leq p^{n-1}! \leq 2 \frac{p^{n^4/2+n^2}-1}{p^{n^2}-1} \leq \frac{32}{15} p^{n^4/2}$$

which provides the contradiction we were seeking for  $n \geq n_0(p)$ . Indeed, we can take  $n_0(p) = 11$  for all  $p$  but this estimate can be improved if we allow  $p$  to be large enough and for instance  $n_0(p) = 2$  is enough for  $p \geq 13$ .

# Appendix A

## Auxiliary structures and results for nilspaces

We are going to present some structures and results that are useful to prove some statements of Chapter 5. Just as in Chapter 5, in this appendix, most of the results are not original, and the original parts will be clearly stated at the beginning of each section.

### A.1 Algebraic aspects

This section presents some auxiliary results needed to prove some algebraic facts about nilspaces. There are no new original results but there are new proofs of known facts.

In some cases, some concepts like Definition A.1, Definition A.5, or Corollary A.13 appear only implicitly in [9].

The only original part is the treatment of the concept of tricube, Definition A.18; and tricube composition, Definition A.19. Those definitions, together with Proposition A.20, Lemma A.22, and the proof of Proposition A.23 are alternative ways to prove the results from [9, 3.1.3 Tricubes and tricube composition].

### A.1.1 Complementary definitions and examples

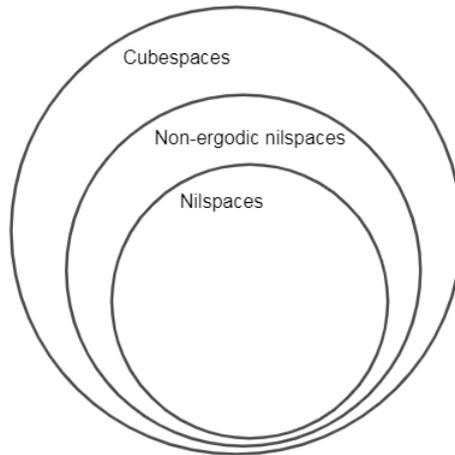
First, let us define some structures closely related to nilspaces. These are non-ergodic nilspaces and cubespaces.

**Definition A.1** (Non-ergodic nilspace). A set  $X$  is a non-ergodic nilspace if it satisfies Definition 5.7 except for maybe the Ergodicity Axiom. Instead we require also that  $C^0(X) = X$ .

A further weakening of this definition is the concept of cubespace:

**Definition A.2** (Cubespace). A cubespace  $X$  is a set together with a set of cubes  $C^n(X) \subset X^{\llbracket n \rrbracket}$  for every  $n \geq 0$  such that  $C^0(X) = X$  and the cubes satisfy the Composition axiom of Definition 5.7.

It is clear that nilspace  $\Rightarrow$  non-ergodic nilspace  $\Rightarrow$  cubespace. In general, the converse implications are false.



**Definition A.3** (Morphism and isomorphism). Let  $X$  and  $Y$  be cubespaces. A function  $\phi : X \rightarrow Y$  is a morphism if for every cube  $c \in C^n(X)$ , we have that  $\phi \circ c \in C^n(Y)$ . If in addition  $\phi$  is invertible and the inverse is a morphism we say that it is an isomorphism. We will denote by  $\text{hom}(X, Y)$  the set of morphisms from  $X$  to  $Y$ .

*Remark A.4.* Note that this is consistent with Definition 5.9.

Let us now give an example of a non-ergodic nilspace that is not a nilspace in general.

**Definition A.5.** Let  $X$  be a non-ergodic nilspace and fix some  $k \geq 0$ . Then define the cubespace  $Y := C^k(X)$  with the following set of cubes. For all  $n \geq 0$ , we will say that  $c \in C^n(Y)$  if and only if the function  $c^* : \llbracket n+k \rrbracket \rightarrow X$  defined by the formula  $c^*(\underline{v}) := c(v(k+1), \dots, v(k+n))(v(1), \dots, v(k))$  is in  $C^{n+k}(X)$ .

This definition is very natural in many contexts. Here the elements of  $Y$  are cubes of dimension  $k$  of the nilspace  $X$ .

**Proposition A.6.** *The cubespace  $Y$  along with the set of cubes defined as above is a non-ergodic nilspace. Furthermore,  $X$  is  $(k+l)$ -fold ergodic if and only if  $Y$  is  $l$ -fold ergodic and  $X$  is  $k$ -fold ergodic.*

*Proof.* Most of the things we have to check follow from the definitions. The Completion axiom is the only non-trivial part, and it follows from (the proof of) [9, Lemma 3.1.5].  $\square$

This construction enables us to create many non-ergodic nilspaces. For example, take any group nilspace  $X = G$  (constructed as explained in Definition 5.12) that is not  $k$ -fold ergodic (for some  $k \geq 1$ , see Proposition 5.14) and take  $Y := C^k(X)$ .

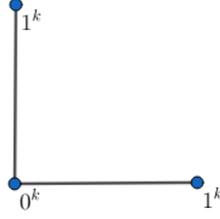
To conclude this subsection, let us give two examples of cubespaces that are not non-ergodic nilspaces in general.

**Definition A.7** (Subcubespaces). Fix any  $k \geq 0$  and consider any subset  $Q \subset \llbracket k \rrbracket$ . We will say that  $c \in C^n(Q)$  if  $c$  is a discrete-cube morphism  $c : \llbracket n \rrbracket \rightarrow \llbracket k \rrbracket$  and  $c(\llbracket n \rrbracket) \subset Q$ .

**Proposition A.8.** *The set  $Q \subset \llbracket k \rrbracket$  with this set of cubes defined as above is a cubespace.*

*Proof.* The composition axiom is almost trivial to check. To see that  $C^0(Q) = Q$ , note that given any  $\underline{x} \in Q$ , the function  $c : \llbracket 0 \rrbracket \rightarrow \llbracket k \rrbracket$  such that  $0 \mapsto \underline{x}$  is a discrete-cube morphism.  $\square$

This cubespace does not satisfy the Completion axiom (unless  $k = 0$ ). For a larger  $k$ , the following 2-corner does not have a completion:



Now let us define another cubespace that will be very useful in the next subsection:

**Definition A.9** (Simplicial cubespaces). Let  $n \geq 0$  and  $l \geq 1$  be integers, and let  $F_1, \dots, F_l \subset \llbracket n \rrbracket$  be lower faces. Define  $S := \cup_{i=1}^l F_i$ . We say that  $c \in C^m(S)$  if  $c$  is a discrete-cube morphism such that its image lies inside  $F_i$  for some  $i \in \{1, \dots, l\}$ .

The proof that this definition gives a cubespace is similar to the proof of Proposition A.8.

Note that the two latter definitions are not the same in general. For example, let  $Q = Q^* = \llbracket 2 \rrbracket \setminus \{(1, 1)\}$  but let us equip  $Q$  with the sub-cubespace structure (Definition A.7) and  $Q^*$  with the simplicial cubespace structure (Definition A.9). Now note that the discrete-cube morphism  $c : \llbracket 1 \rrbracket \rightarrow \llbracket 2 \rrbracket$  defined by  $v(1) \mapsto (1 - v(1), v(1))$  is an element of  $C^1(Q)$  but it is not an element of  $C^1(Q^*)$ . This is because, on the one hand,  $c$  is a discrete-cube morphism such that its image is contained in  $Q$ . Hence, it satisfies Definition A.7. On the other hand,  $c$  does not satisfy Definition A.9 because its image does not lie inside  $\{\underline{v} \in \llbracket 2 \rrbracket : v(1) = 0\}$  or  $\{\underline{v} \in \llbracket 2 \rrbracket : v(2) = 0\}$  (the two lower faces of  $\llbracket 2 \rrbracket \setminus \{(1, 1)\}$ ). However, in the next subsection we will see how these two cubespaces are closely related via the Completion axiom.

*Remark A.10.* If  $Q = \llbracket k \rrbracket$  then the cubespaces on  $Q$  given by Definition A.7 and Definition A.9 are equal. Thus, if we refer to the cubespace structure of  $\llbracket k \rrbracket$ , it will always be the one given by either of those definitions.

### A.1.2 Concatenation and tricubes.

Now we are going to introduce some tools and concepts that will be useful later. Let  $Q \subset P$  be two cubespaces.

**Definition A.11** (Extension property). Let  $Q \subset P$  be two cubespaces. We say that  $Q$  has the extension property in  $P$  if for every non-ergodic nilspace  $X$  and every morphism  $f : Q \rightarrow X$ , there exists a morphism  $f' : P \rightarrow X$  such that  $f'|_Q = f$ .

Note that this differs from [9, Definition 3.1.3], because here we only require  $X$  to be a non-ergodic nilspace. The reason for doing so is that in many applications, it is enough to work with the axioms of non-ergodic nilspaces.

**Proposition A.12.** *Let  $S \subset \llbracket n \rrbracket$  be a simplicial cubespace (see Definition A.9). Then  $S$  has the extension property in  $\llbracket n \rrbracket$ .*

*Proof.* See [9, Lemma 3.1.5]. The idea is that given a morphism  $f : S \rightarrow X$ , take a vertex  $\underline{v} \in \llbracket n \rrbracket \setminus S$  such that for any other vertex  $\underline{w} \in \llbracket n \rrbracket$ ,  $\underline{w} \neq \underline{v}$ , and  $w(i) \leq v(i)$  for all  $i = 1, \dots, n$ , we have  $\underline{w} \in S$ . Then the set of vertices  $\{\underline{w} \in \llbracket n \rrbracket : w(i) \leq v(i) \text{ for all } i\}$  is a  $(\sum_{i=1}^n v(i))$ -corner. Using the Completion axiom with  $f$  restricted to the previous set, we can assign a value to  $v$  and thus we would have defined a morphism  $f' : S \cup \{\underline{v}\} \rightarrow X$  (with  $S \cup \{\underline{v}\}$  being a simplicial cubespace). We can repeat this process until we have a morphism from  $\llbracket n \rrbracket$  to  $X$ .  $\square$

This result connects Definition A.9 with Definition A.7 in the following way:

**Corollary A.13.** *Let  $Q \subset \llbracket k \rrbracket$  be the union of some lower faces. Let  $Q_1$  be the cubespace over  $Q$  given by Definition A.7 (subcubespace) and let  $Q_2$  be the cubespace over  $Q$  given by Definition A.9 (simplicial cubespace). Then for any non-ergodic nilspace  $Y$  we have  $\text{hom}(Q_1, Y) = \text{hom}(Q_2, Y)$ .*

*Proof.* One inclusion is clear. For the other, take any  $f \in \text{hom}(Q_2, Y)$  and apply Proposition A.12 to extend it to an element  $f' \in \text{hom}(\llbracket k \rrbracket, Y)$ . Now, given any  $c \in C^n(Q_1)$  we have that  $f \circ c = f' \circ c \in C^n(Y)$ .  $\square$

Having this idea in mind, we can define an operation between cubes called concatenation. To do so, we need some more notation. Let  $f : \llbracket n \rrbracket \rightarrow X$ , for some  $n \geq 1$  and some non-ergodic nilspace  $X$ , be any map. Define

$$f(\cdot, v(i) = l) : \begin{array}{ccc} \llbracket n-1 \rrbracket & \rightarrow & X \\ (v(1), \dots, v(n-1)) & \mapsto & f(v(1), \dots, v(i-1), l, v(i), \dots, v(n)) \end{array}$$

for some  $l \in \{0, 1\}$  and some  $i \in \{1, \dots, n\}$ .

**Definition A.14** (Adjacent maps and concatenation). Let  $X$  be a non-ergodic nilspace and let  $f_1, f_2 : \llbracket n \rrbracket \rightarrow X$  be functions. We say that they are  $i$ -adjacent (for some  $i = 1, \dots, n$ ) if  $f_1(\cdot, v(i) = 1) = f_2(\cdot, v(i) = 0)$ . If  $f_1$  and  $f_2$  are  $i$ -adjacent, we define their  $i$ -concatenation, denoted by  $f_1 \prec_i f_2$  as the function from  $\llbracket n \rrbracket$  to  $X$  such that

$$\underline{w} \mapsto \begin{cases} f_1(\cdot, v(i) = 0)(w(1), \dots, w(i-1), w(i+1), \dots, w(n)) & \text{if } w(i) = 0 \\ f_2(\cdot, v(i) = 1)(w(1), \dots, w(i-1), w(i+1), \dots, w(n)) & \text{if } w(i) = 1. \end{cases}$$

**Lemma A.15.** *Let  $X$  be a non-ergodic nilspace,  $n \geq 1$  and  $i \in \{1, \dots, n\}$ . If  $c_1, c_2 \in C^n(X)$  are  $i$ -adjacent, then  $c_1 \prec_i c_2 \in C^n(X)$ .*

*Proof.* The proof of this lemma is very similar to the proof of [9, Lemma 3.1.7] and indeed, by the Composition axiom, it is enough to prove it for  $i = n$ . We reproduce here the proof because it is very illustrative of how we can work with nilspaces. Suppose that we want to  $n$ -concatenate two cubes  $c_1, c_2 \in C^n(X)$  that are  $n$ -adjacent for some fixed  $n \geq 1$ . We can construct a simplicial cubespace (Definition A.9)  $S := F_1 \cup F_2 \subset \llbracket n+1 \rrbracket$  where  $F_1 := \{\underline{v} \in \llbracket n+1 \rrbracket : v(n+1) = 0\}$  and  $F_2 := \{\underline{v} \in \llbracket n+1 \rrbracket : v(n) = 0\}$ . Define the morphism  $f : S \rightarrow X$  as

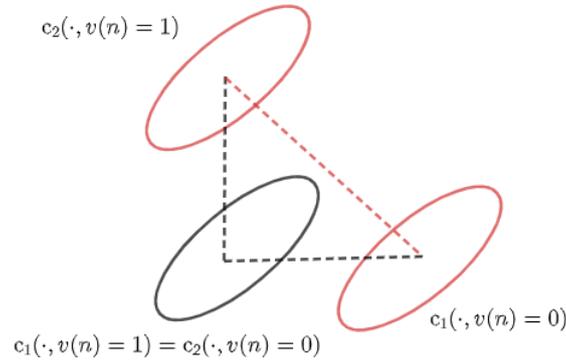
$$\underline{w} \mapsto \begin{cases} c_1(w(1), \dots, w(n-1), 1 - w(n)) & \text{if } w(n+1) = 0 \\ c_2(w(1), \dots, w(n-1), w(n+1)) & \text{if } w(n) = 0. \end{cases}$$

Note that as  $c_1$  and  $c_2$  are  $n$ -adjacent,  $f$  is well defined and  $f \in \text{hom}(S, X)$ .

Now, let  $S^* = S$  be the corresponding subcubespace (Definition A.7). By Corollary A.13, we have that  $f \in \text{hom}(S^*, X)$ . Then consider the discrete-cube morphism  $\phi : \llbracket n \rrbracket \rightarrow \llbracket n+1 \rrbracket$  defined by  $\underline{w} \mapsto (w(1), \dots, w(n-1), 1 - w(n), w(n))$ . We know that  $\phi \in C^n(S^*)$ . Hence  $f \circ \phi \in C^n(X)$ , but this is precisely  $c_1 \prec_n c_2$ .  $\square$

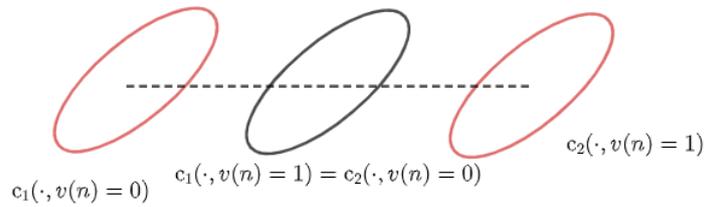
*Remark A.16.* To simplify the notation in the future, note that we can define the concatenation as an operation  $\prec_i : \cup_{n=i}^{\infty} \{(c_1, c_2) \in (C^n(X))^2 : c_1, c_2 \text{ are } i\text{-adjacent}\} \rightarrow \cup_{n=i}^{\infty} C^n(X)$ .

Graphically, what we are doing is to prove that we can *take diagonals* in the following sense. Represent the morphism  $f$  of the previous proof as:



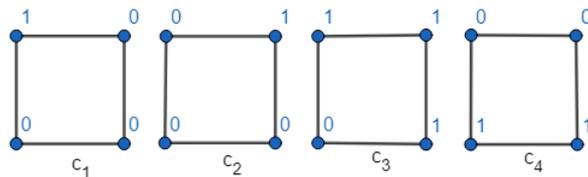
Here, the horizontal direction is the  $n$ -th direction and the vertical direction is the  $(n + 1)$ -th direction. The ellipses represent the remaining  $n - 1$  dimensions. The two ellipses joined by the horizontal dotted line represent  $c_1$  (with the last coordinate inverted, on the right we have  $c_1(\cdot, v(n) = 0)$ ), the vertical ellipses represent  $c_2$ , and the two ellipses in red, joined by the red dotted line, represent  $c_1 \prec_n c_2$ .

Typically, instead of adding another dimension, we will write the previous diagram as:

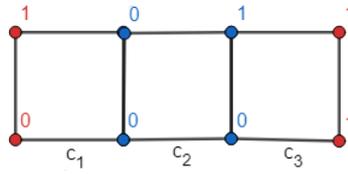


This has the advantage also that we can see  $c_1$  as the first two ellipses,  $c_2$  as the last two, and  $c_1 \prec_n c_2$  as the red ones. For examples where the dimension is small, we will emphasize the values at the vertices with dots of different colors as in the following example:

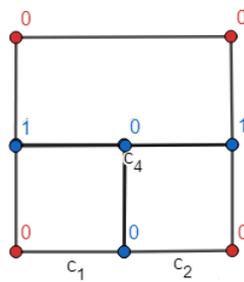
Suppose that  $n = 2$ ,  $X = \mathcal{D}_2(\mathbb{Z}_2)$ , and define the following cubes:



We can see that  $c_1$  and  $c_2$  are 1-adjacent, and  $c_2$  and  $c_3$  are also 1-adjacent. We can see graphically the result of (say)  $(c_1 \prec_1 c_2) \prec_1 c_3$  as the cube consisting of the extremes (in red) of

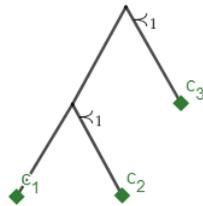


We can also concatenate cubes in a way that involves  $i$ -concatenations for different values of  $i$ 's. For instance,  $(c_1 \prec_1 c_2) \prec_2 c_4$  can be represented as:

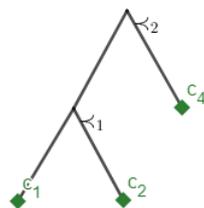


Note that  $c_2$  and  $c_4$  are not 2-adjacent, so we cannot 2-concatenate them.

Another way of representing these operations with concatenations is by using trees. For example, the operation  $(c_1 \prec_1 c_2) \prec_1 c_3$  can be seen as



and  $(c_1 \prec_1 c_2) \prec_2 c_4$  can be represented as



Thus, we can see concatenation as an operation between certain pairs of cubes. For any non-ergodic nilspace  $X$  and any cubes  $c_1, c_2, c_3 \in C^m(X)$  the following holds. If  $c_1$  and  $c_2$  are  $i$ -adjacent and  $c_2$  and  $c_3$  are  $i$ -adjacent then  $c_1 \prec_i c_2$  is  $i$ -adjacent to  $c_3$  and  $c_1$  is  $i$ -adjacent to  $c_2 \prec_i c_3$ . Moreover, the  $i$ -concatenation is associative in this case,  $(c_1 \prec_i c_2) \prec_i c_3 = c_1 \prec_i (c_2 \prec_i c_3)$ . However, if  $c_1$  and  $c_2$  are  $i$ -adjacent and  $c_1 \prec_i c_2$  is  $j$ -adjacent to  $c_3$  for  $i \neq j$ , in general it may be not even possible to say that  $c_2$  and  $c_3$  are  $j$ -adjacent.

*Remark A.17.* Let  $X$  be a non-ergodic nilspace and  $n \geq 1$  an integer. Suppose that we have cubes  $c_i \in C^n(X)$  for  $i = 1, 2, 3$  such that  $c_1 \prec_l c_2 = c_3$ , for some  $l \in \{1, \dots, n\}$ . Then, we can recover any cube  $c_i$ , for  $i \in \{1, 2, 3\}$ , from the other two,  $\{c_j : j \neq i\}$ , by the following observation. Let  $\phi_l : \llbracket n \rrbracket \rightarrow \llbracket n \rrbracket$  be the discrete-cube morphism that inverts the  $l$ -th coordinate, i.e.,  $\phi_l(\underline{v})(j) = v(j)$  if  $j \neq l$  and  $\phi_l(\underline{v})(l) = 1 - v(l)$ . Then  $c_1 = c_3 \prec_l (c_2 \circ \phi_l)$  and  $c_2 = (c_1 \circ \phi_l) \prec_l c_3$ .

Next, we are going to explain a very useful construction involving concatenations that we will call tricube. This part gives an alternative point of view of the results of [9, 3.1.3 Tricubes and tricube composition].

**Definition A.18** (Tricube). Let  $n \geq 0$  and  $m \geq n$  be integers, and let  $X$  be a non-ergodic nilspace. A set of cubes  $c_{\underline{v}} \in C^m(X)$  for  $\underline{v} \in \llbracket n \rrbracket$  is called a  $(n, m)$ -tricube if it satisfies the following property:

- For all  $i = 1, \dots, n$  and all  $\underline{v}_1, \underline{v}_2 \in \llbracket n \rrbracket$ , if  $v_1(j) = v_2(j)$  for all  $j \neq i$  and  $v_1(i) \neq v_2(i)$  then  $c_{\underline{v}_1}$  and  $c_{\underline{v}_2}$  are  $i$ -adjacent.

The idea is that with this definition, we will be able to concatenate all the elements of a  $(n, m)$ -tricube in a precise way.

**Definition A.19** (Tricube composition). Let  $n \geq 0$  and  $m \geq n$  be integers,  $X$  a non-ergodic nilspace and let  $c_{\underline{v}} \in C^m(X)$  for  $\underline{v} \in \llbracket n \rrbracket$  be a  $(n, m)$ -tricube. Then define the tricube composition  $T_n((c_{\underline{v}})_{\underline{v} \in \llbracket n \rrbracket})$  recursively as follows.

- $T_0((c_{\underline{v}})_{\underline{v} \in \llbracket 0 \rrbracket}) = c_0$ .
- For  $n \geq 1$  define  $T_n((c_{\underline{v}})_{\underline{v} \in \llbracket n \rrbracket})$  as

$$T_{n-1}((c_{(v(1), \dots, v(n-1), 0)} \prec_n c_{(v(1), \dots, v(n-1), 1)})_{(v(1), \dots, v(n-1)) \in \llbracket n-1 \rrbracket}).$$

**Proposition A.20.** *Let  $n \geq 0$ ,  $m \geq n$ , and  $X$  a non-ergodic nilspace. Let also  $c_{\underline{v}} \in C^n(X)$  for  $v \in \llbracket n \rrbracket$  be a  $(n, m)$ -tricube. Then the tricube composition  $T_n((c_{\underline{v}})_{\underline{v} \in \llbracket n \rrbracket})$  is well defined.*

*Remark A.21.* The definitions of tricube and tricube composition will be particularly useful when  $n = m$ . In this case, and when  $n$  can be inferred from the context, we will call them tricubes instead of  $(n, n)$ -tricubes.

*Proof.* We are going to prove this by induction on  $n$ . The base case is a  $(0, m)$ -tricube for any  $m \geq 0$ , and it is clear that in this case, everything works.

By induction, assume that if we have a  $(n-1, m)$ -tricube for any  $m \geq n-1$ , then  $T_{n-1}((c_{\underline{v}})_{\underline{v} \in \llbracket n-1 \rrbracket})$  is well defined. To prove the desired result, we have to check that the set  $(c_{(v(1), \dots, v(n-1), 0)} \prec_n c_{(v(1), \dots, v(n-1), 1)})_{(v(1), \dots, v(n-1)) \in \llbracket n-1 \rrbracket}$  is a  $(n-1, m)$ -tricube. To prove this, by definition, take two elements  $\underline{v}, \underline{w} \in \llbracket n-1 \rrbracket$  such that they are equal in all but one coordinate. Without loss of generality suppose that  $v(i) = w(i)$  for all  $i \in \{1, \dots, n-2\}$ ,  $v(n-1) = 0$ , and  $w(n-1) = 1$ . We have to prove then that the  $(n-1)$ -upper face of  $(c_{(v(1), \dots, v(n-2), 0, 0)} \prec_n c_{(v(1), \dots, v(n-2), 0, 1)})$  is equal to the  $(n-1)$ -lower face of  $(c_{(v(1), \dots, v(n-2), 1, 0)} \prec_n c_{(v(1), \dots, v(n-2), 1, 1)})$ . Consider  $\underline{t}_1 := (t(1), \dots, t(n-2), 1, t(n), \dots, t(m))$  and  $\underline{t}_2 := (t(1), \dots, t(n-2), 0, t(n), \dots, t(m))$ . We have to check that

$$\begin{aligned} (c_{(v(1), \dots, v(n-2), 0, 0)} \prec_n c_{(v(1), \dots, v(n-2), 0, 1)}) (\underline{t}_1) \\ = (c_{(v(1), \dots, v(n-2), 1, 0)} \prec_n c_{(v(1), \dots, v(n-2), 1, 1)}) (\underline{t}_2). \end{aligned}$$

There are two possibilities:

**If  $t(n) = 0$ :** Then

$$\begin{aligned} (c_{(v(1), \dots, v(n-2), 0, 0)} \prec_n c_{(v(1), \dots, v(n-2), 0, 1)}) (\underline{t}_1) \\ = c_{(v(1), \dots, v(n-2), 0, 0)} (t(1), \dots, t(n-2), 1, 0, t(n+1), \dots, t(m)). \end{aligned}$$

And

$$\begin{aligned} (c_{(v(1), \dots, v(n-2), 1, 0)} \prec_n c_{(v(1), \dots, v(n-2), 1, 1)}) (\underline{t}_2) \\ = c_{(v(1), \dots, v(n-2), 1, 0)} (t(1), \dots, t(n-2), 0, 0, t(n+1), \dots, t(m)). \end{aligned}$$

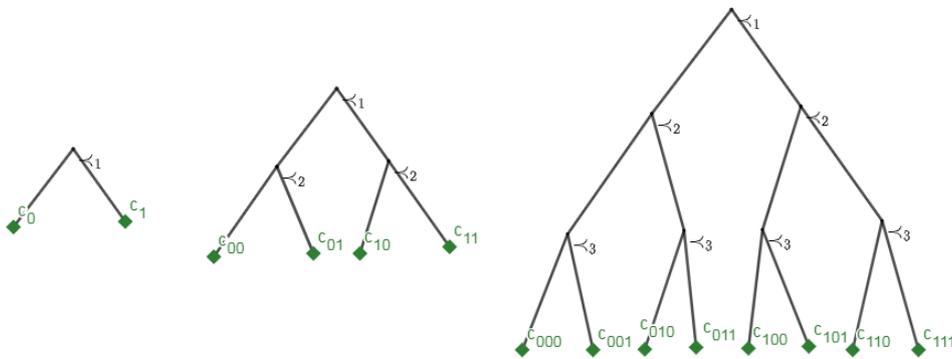
And the latter are equal by definition of tricube.

**If  $t(n) = 1$ :** Essentially the same.

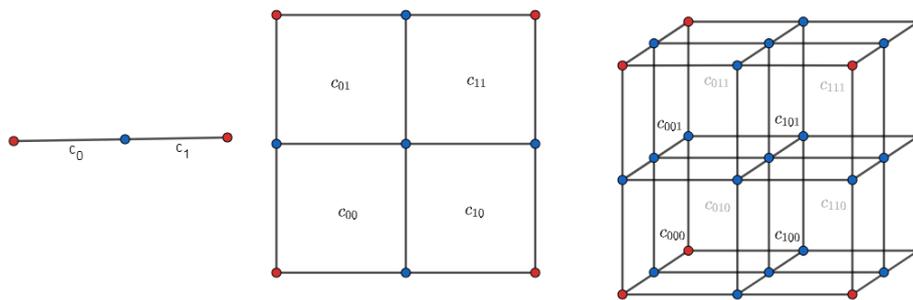
Thus we have proved that  $(c_{(v,0)} \prec_n c_{(v,1)})_{v \in \llbracket n-1 \rrbracket}$  is a  $(n-1, m)$ -tricube, and the result follows.  $\square$

Let us put some examples and represent them graphically to understand better this construction.

For  $n = 1, 2$  and  $3$ , the expressions are  $c_0 \prec_1 c_1$ ,  $(c_{00} \prec_2 c_{01}) \prec_1 (c_{10} \prec_2 c_{11})$ , and  $((c_{000} \prec_3 c_{001}) \prec_2 (c_{010} \prec_3 c_{011})) \prec_1 ((c_{100} \prec_3 c_{101}) \prec_2 (c_{110} \prec_3 c_{111}))$  respectively. The trees representing these concatenations are:



As we mentioned before, it is particularly useful in the case of  $(n, n)$ -tricubes. In this case, for  $n = 1, 2$  and  $3$ , the diagram representing the concatenations is:



The reason why they are useful is the following:

**Lemma A.22.** *Let  $n \geq 0$  be an integer and consider a  $(n, n)$ -tricube  $(c_{(\underline{v})})_{\underline{v} \in \llbracket n \rrbracket}$ . Then*

$$T_n((c_{(\underline{v})})_{\underline{v} \in \llbracket n \rrbracket})(\underline{t}) = c_{\underline{t}}(\underline{t})$$

for all  $\underline{t} \in \llbracket n \rrbracket$ .

*Proof.* It can be proved by induction on  $n$  a slightly more general result: Given any  $(n, m)$ -tricube we have

$$T_n((c_{(\underline{v})})_{\underline{v} \in \llbracket n \rrbracket})(\underline{t}, \underline{l}) = c_{\underline{t}}(\underline{t}, \underline{l})$$

where  $\underline{t} \in \llbracket n \rrbracket$  and  $\underline{l} \in \llbracket m - n \rrbracket$ . We leave this proof to the reader. The proof of the lemma then follows.  $\square$

**Proposition A.23.** *Let  $X$  be a non-ergodic nilspace and let  $k \geq 0$  be an integer. Define the following relation:*

- We say  $x \sim_k y$  for  $x, y \in X$  if there exist cubes  $c_1, c_2 \in C^{k+1}(X)$  such that  $c_1(v) = c_2(v)$  for all  $v \neq 0^{k+1}$ ,  $c_1(0^{k+1}) = x$  and  $c_2(0^{k+1}) = y$ .

*Then this is an equivalence relation.*

*Proof.* The only non-trivial part is to check the transitivity property. Let  $x \sim_k y$  for  $x, y \in X$ . Let  $c_1, c_2 \in C^{k+1}(X)$  be such that  $c_1(v) = c_2(v)$  for all  $v \neq 0^{k+1}$ ,  $c_1(0^{k+1}) = x$  and  $c_2(0^{k+1}) = y$ . We are going to check that this implies that there exists a cube  $c_3 \in C^{k+1}(X)$  such that  $c_3(v) = y$  for all  $v \neq 0^{k+1}$  and  $c_3(0^{k+1}) = x$ .

For every  $\underline{w} \in \llbracket k + 1 \rrbracket$  let us define the discrete-cube morphism  $\phi_{\underline{w}} : \llbracket k + 1 \rrbracket \rightarrow \llbracket k + 1 \rrbracket$  as

$$(\phi_{\underline{w}}(\underline{t}))(i) := \begin{cases} t(i) & \text{if } w(i) = 0 \\ 1 - t(i) & \text{if } w(i) = 1, \end{cases}$$

for any  $i \in \{1, \dots, k + 1\}$  and any  $\underline{t} \in \llbracket k + 1 \rrbracket$ .

Now let us define the tricube  $(c_{(\underline{w})})_{\underline{w} \in \llbracket k+1 \rrbracket}$  as:  $c_{0^{k+1}} := c_1 \circ \phi_{0^{k+1}} = c_1$  and  $c_{\underline{w}} := c_2 \circ \phi_{\underline{w}}$  if  $\underline{w} \neq 0^{k+1}$ . Let us check that this is indeed a tricube. Let  $\underline{w}' \in \llbracket k \rrbracket$  be any element. Without loss of generality, by the Composition

axiom, it is enough to check that  $c_{(0,\underline{w}')} (1, \underline{t}') = c_{(1,\underline{w}')} (0, \underline{t}')$  for any  $\underline{t}' \in \llbracket k \rrbracket$ . First of all, let us compute

$$\phi_{(0,\underline{w}')} (1, \underline{t}') = \left( 1, \left\{ \begin{array}{ll} t'(1) & \text{if } w'(2) = 0 \\ 1 - t'(1) & \text{if } w'(2) = 1 \end{array} \right\}, \dots, \left\{ \begin{array}{ll} t'(k) & \text{if } w'(2) = 0 \\ 1 - t'(k) & \text{if } w'(2) = 1 \end{array} \right\} \right).$$

And similarly,

$$\phi_{(1,\underline{w}')} (0, \underline{t}') = \left( 1, \left\{ \begin{array}{ll} t'(1) & \text{if } w'(2) = 0 \\ 1 - t'(1) & \text{if } w'(2) = 1 \end{array} \right\}, \dots, \left\{ \begin{array}{ll} t'(k) & \text{if } w'(2) = 0 \\ 1 - t'(k) & \text{if } w'(2) = 1 \end{array} \right\} \right).$$

Note now that  $c_{(0,\underline{w}')} (1, \underline{t}') = c_j \circ \phi_{(0,\underline{w}')} (1, \underline{t}')$  where  $j \in \{1, 2\}$  and  $c_{(1,\underline{w}')} (0, \underline{t}') = c_2 \circ \phi_{(1,\underline{w}')} (0, \underline{t}')$ . But regardless of the value of  $j$ , as we are evaluating in an upper face, those two quantities are equal.

Now, consider the tricube composition  $T_{k+1}((c_{\underline{w}})_{\underline{w} \in \llbracket k+1 \rrbracket})$  which by Proposition A.20 is an element of  $C^{k+1}(X)$ . We just have to check its values using Lemma A.22. In  $\underline{t} = 0^{k+1}$ ,

$$T_{k+1}((c_{\underline{w}})_{\underline{w} \in \llbracket k+1 \rrbracket})(0^{k+1}) = c_{0^{k+1}}(0^{k+1}) = c_1(0^{k+1}) = x.$$

And for any  $\underline{t} \neq 0^{k+1}$ ,

$$T_{k+1}((c_{\underline{w}})_{\underline{w} \in \llbracket k+1 \rrbracket})(\underline{t}) = c_{\underline{t}}(\underline{t}) = (c_2 \circ \phi_{\underline{t}})(\underline{t}) = c_2(0^{k+1}) = y.$$

The only non-trivial equality is to check that  $\phi_{\underline{t}}(\underline{t}) = 0^{k+1}$ , and this is easily seen from the definition of  $\phi_{\underline{t}}$ .

Thus,  $c_3 := T_{k+1}((c_{\underline{w}})_{\underline{w} \in \llbracket k+1 \rrbracket})$  is an element of  $C^{k+1}(X)$  that satisfies the required properties.

Therefore, to prove that this relation is transitive, let  $x, y, z \in X$  be such that  $x \sim_k y$  and  $y \sim_k z$ . Using the fact that we have just proved, there exists a cubes  $c_3, c'_3 \in C^{k+1}(X)$  such that  $c_3(0^{k+1}) = x$  and  $c_3(v) = y$  for all  $v \neq 0^{k+1}$ , and  $c'_3(0^{k+1}) = z$  and  $c_3(v) = y$  for all  $v \neq 0^{k+1}$ . Hence,  $x \sim_k z$ .  $\square$

### A.1.3 More on abelian bundles

**Definition A.24** (Restricted morphism). Let  $P \subset \llbracket n \rrbracket$  be a cubespace with the extension property in  $\llbracket n \rrbracket$ ,  $S \subset P$  a cubespace with the extension

property in  $P$ , and  $X$  a  $k$ -step nilspace. Let also  $f : S \rightarrow X$  be a morphism. We denote by  $\text{hom}_f(P, X)$  the set of morphisms  $g : P \rightarrow X$  such that  $g|_S = f$ .

**Lemma A.25.** *Let  $P, S, X$  and  $f$  be as above. Then  $\text{hom}_f(P, X)$  is a  $k$ -fold abelian bundle with factors  $\text{hom}_{\pi_i \circ f}(P, X_i)$ . Moreover, its structure groups are  $\text{hom}_{S \rightarrow 0}(P, \mathcal{D}_i(Z_i))$  for all  $i = 0, 1, \dots, k$ , where  $Z_i$  is the  $i$ -th structure group of  $X$ .*

*Proof.* See [9, Lemma 3.3.11]. □

*Remark A.26.* In particular, if  $P = \llbracket n \rrbracket$  and  $S = \emptyset$  then  $\text{hom}_f(P, X) = C^n(X)$ . Thus we can see  $C^n(X)$  as an abelian bundle with structure groups  $C^n(\mathcal{D}_i(Z_i))$  for all  $i = 0, 1, \dots, k$  where  $Z_i$  is the  $i$ -th structure group of  $X$ .

## A.2 Topological and measure-theoretic aspects

The following short section contains a result that is used in the proof of Lemma 5.108, and we have included it here for completeness. It is entirely non-original.

### A.2.1 Probability spaces of restricted morphisms

Let us recall that by Proposition 5.55, we can define a Haar measure on any compact abelian bundle. By Lemma A.25 we know that the set  $\text{hom}_f(P, X)$  is a  $k$ -fold abelian bundle where  $P, f$ , and  $X$  are defined as in Definition A.24. It can be proved that if  $X$  is a  $k$ -step compact nilspace then  $\text{hom}_f(P, X)$  is a  $k$ -fold compact abelian bundle (see [10, Lemma 2.2.12]). Hence, we can define a Haar measure on it. In the study of both nilspaces and cubic couplings it will be important to study these spaces, and there is an important concept that it is worth mentioning [10, Definition 2.2.13]:

**Definition A.27** (Good pair). Let  $P \subset \llbracket n \rrbracket$  be a cubespace, and let  $P_1, P_2 \subset P$  be subcubespaces of  $P$ . We say that  $P_1, P_2$  is a good pair if:

- $P_1$  and  $P_1 \cap P_2$  both have the extension property in  $P$ .
- For every abelian group  $Z$ , every positive integer  $k$  and every morphism  $f' : P_2 \rightarrow \mathcal{D}_k(Z)$  with  $f'|_{P_1 \cap P_2} = 0$ , there exists an extension  $f : P \rightarrow \mathcal{D}_k(Z)$  such that  $f|_{P_1} = 0$ .

To motivate this definition, see Lemma 5.108. Meanwhile, we have this important result:

**Lemma A.28.** *Let  $P \subset \llbracket n \rrbracket$  be a cubespace, and let  $P_1, P_2 \subset P$  be a good pair in  $P$ . Let  $X$  be a  $k$ -step nilspace and  $f_1 : P_1 \rightarrow X$  be a morphism. Then the restriction*

$$\varphi : \text{hom}_f(P, X) \rightarrow \text{hom}_{f|_{P_1 \cap P_2}}(P_2, X)$$

*is a continuous totally-surjective bundle morphism.*

*Remark A.29.* In particular,  $\varphi$  preserves the Haar measure.

*Proof.* See [10, Lemma 2.2.14]. □

# Bibliography

- [1] Antolín Camarena O.; Szegedy B., *Nilspaces, nilmanifolds and their morphisms*, Preprint. [arXiv:1009.3825](https://arxiv.org/abs/1009.3825).
- [2] Auslander L.; Green L.; Hahn F., *Flows on homogeneous spaces*, Annals of Mathematics Studies, No. 53, Princeton University Press, Princeton, N.J. (1963).
- [3] Baltz A.; Hegarty P.; Knape J.; Larsson U.; Schoen T., *The structure of maximum subsets of  $\{1, \dots, n\}$  with no solutions to  $a + b = kc$* , Electron. J. Combin., Volume 12 (2005), Paper No. R19, 16pp.
- [4] Bergelson V.; Host B.; Kra B., *Multiple recurrence and nilsequences with an appendix by Imre Ruzsa*, Invent. Math., Volume 160, (2005), Number 2, pp. 261-303.
- [5] Bienvenu P.-Y.; Lê T.H., *A bilinear Bogolyubov theorem*. European J. Combin., Volume 77 (2019), pp. 102-113.
- [6] Bienvenu P.-Y.; González-Sánchez D., Martínez A. D., *A note on the bilinear Bogolyubov theorem: Transverse and bilinear sets* Proceedings of the AMS, Volume 148, (2020), pp. 23-31.
- [7] Bloom T. F., *A quantitative improvement for Roth's theorem on arithmetic progressions*, J. Lond. Math. Soc., Volume 93, (2016), Issue 3, pp. 643-663.
- [8] Bogoliouboff N., *Sur quelques propriétés arithmétiques des presque-périodes*. Ann. Chaire Phys. Math. Kiev, Volume 4 (1939), pp. 185-205.
- [9] Candela P., *Notes on nilspaces: algebraic aspects*, Discrete Analysis, (2017), Paper No. 15, 59 pp.

- [10] Candela P., *Notes on compact nilspaces*, Discrete Analysis, (2017), Paper No. 16, 57pp.
- [11] Candela P.; González-Sánchez D.; de Roton A., *A Plünnecke-Ruzsa inequality in compact abelian groups*, Revista Matemática Iberoamericana, Volume 35, (2019), Issue 7, pp. 2169-2186.
- [12] Candela P.; González-Sánchez D.; Gryniewicz D. J., *A step towards the  $3k - 4$  conjecture in  $\mathbb{Z}/p\mathbb{Z}$  and an application to  $m$ -sum-free sets*, Acta Mathematica Universitatis Comenianae, Volume 88, (2019), Issue 3, pp. 521-525.
- [13] Candela P.; González-Sánchez D.; Szegedy B., *On nilspace systems and their morphisms*, Ergodic Theory and Dynamical Systems, (2019), 15pp.
- [14] Candela P.; de Roton A., *On sets with small sumset in the circle*, Q. J. Math., Volume 70, (2019), Issue 1, pp. 49-69.
- [15] Candela P.; Serra O.; Spiegel C., *A step beyond Freiman's theorem for set addition modulo a prime*, to appear in Journal de Theorie des Nombres de Bordeaux.
- [16] Candela P.; Sisask O., *On the asymptotic maximal density of a set avoiding solutions to linear equations modulo a prime*, Acta Math. Hungar., Volume 132 (2011), Issue 3, pp. 223-243.
- [17] Candela P.; Szegedy B., *Nilspace factors for general uniformity seminorms, cubic exchangeability and limits*, Preprint. [arXiv:1803.08758](https://arxiv.org/abs/1803.08758).
- [18] Candela P.; B. Szegedy, *Regularity and inverse theorems for uniformity norms on compact abelian groups and nilmanifolds*, (2019), Preprint [arxiv:1902.01098](https://arxiv.org/abs/1902.01098).
- [19] Candela P.; Szegedy B.; Vena L., *On linear configurations in subsets of compact abelian groups, and invariant measurable hypergraphs*, Ann. Comb., Volume 20, (2016), Issue 3, pp. 487-524.
- [20] Choquet G., *Theory of Capacities*, Annales de l'Institut Fourier, Tome 5, (1954), pp. 131-295.

- [21] Chung F. R. K.; Goldwasser J. L., *Integer sets containing no solutions to  $x+y = 3z$* , in: Graham R.L. and Nešetřil J. (eds.), *The Mathematics of Paul Erdős I. Algorithms and Combinatorics*, Volume 13, (1997), pp. 218-227.
- [22] Chung F. R. K.; Goldwasser J. L., *Maximum subsets of  $(0, 1]$  with no solutions to  $x + y = kz$* , *Electron. J. Combin.* Volume 3 (1996), Issue 1, Research Paper 1.
- [23] Ciesielski K.; Fejzić H.; Freiling C., *Measure zero sets with non-measurable sum*, *Real Anal. Exchange*, Volume 27, (2001/02), Number 2, pp. 783-794.
- [24] Cohn D. L., *Measure Theory, Second edition*, Birkhäuser Advanced Texts: Basel Textbooks, Birkhäuser/Springer, New York, (2013).
- [25] Erdős P.; Stone A. H., *On the sum of two Borel sets*, *Proc. Amer. Math. Soc.*, Volume 25, (1970), Issue 2, pp. 304-306.
- [26] Erdős P.; Turán P., *On some sequences of integers*, *Journal of the London Mathematical Society*. Volume s1-11 (1936), Issue 4, pp. 261-264.
- [27] Freiman G., *Inverse problems in additive number theory. Addition of sets of residues modulo a prime*, In *Dokl. Akad. Nauk SSSR*, Volume 141, (1961), Number 3, pp. 571-573.
- [28] Fremlin D. H., *Čech-analytic spaces*, Note of 8 December 1980, unpublished.
- [29] Furstenberg H., *Strict ergodicity and transformation of the torus*, *Amer. J. Math.*, Volume 83, (1961), Number 4, pp. 573-601.
- [30] Furstenberg H., *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, *Journal d'Analyse Math.*, Volume 31, (1977), Issue 1, pp. 204-256.
- [31] Glasner E.; Gutman Y.; Ye X., *Higher order regionally proximal equivalence relations for general minimal group actions*, *Adv. Math.*, Volume 333, (2018), pp. 1004-1041.
- [32] Gowers W. T., *A new proof of Szemerédi's theorem*, *Geom. funct. anal.* Volume 11, (2001), Issue 3, pp. 465-588.

- [33] Gowers W. T.; Milićević L., *A bilinear version of Bogolyubov's theorem*. Preprint, [arxiv:1712.00248](https://arxiv.org/abs/1712.00248).
- [34] Gowers W. T.; Wolf J., *The true complexity of a system of linear equations* Proceedings of the London Mathematical Society, Volume 100, (2010), Issue 1, pp. 155-176.
- [35] Green B.; Ruzsa I. Z., *Sets with small sumset and rectification*, Bull. Lond. Math. Soc., Volume 38, (2006), Issue 1, pp. 43-52.
- [36] Green B.; Tao T., *The primes contain arbitrarily long arithmetic progressions*. Annals of Mathematics, Volume 167, (2008), Issue 2, pp. 481-547.
- [37] Green B.; Tao T., *An inverse theorem for the Gowers  $U^3$ -norm, with applications*, Proc. Edinburgh Math. Soc., Volume 51 (2008), Issue 1, pp. 73-153.
- [38] Green B.; Tao T., *New bounds for Szemerédi's theorem, I: progressions of length 4 in finite field geometries*. Proceedings of the London Mathematical Society, Volume 98, (2009), Issue 2, pp. 365-392.
- [39] Gryniewicz D. J., *Structural additive theory*, Developments in Mathematics, Volume 30, (2013) xii+426 pp.
- [40] Gutman Y.; Manners F.; Varjú P. P., *The structure theory of nilspaces I*, to appear in J. Anal. Math.
- [41] Gutman Y.; Manners F.; Varjú P. P., *The structure theory of nilspaces II: Representation as nilmanifolds*, Trans. Amer. Math. Soc., Volume 371, (2019), pp. 4951-4992.
- [42] Gutman Y.; Manners F.; Varjú P. P., *The structure theory of nilspaces III: Inverse limit representations and topological dynamics*, Advances in Mathematics 365, (2020), 107059.
- [43] Hansell R. W., *Descriptive topology*, Recent progress in general topology, (1991), pp. 275-315.
- [44] Hofmann K. H.; Morris S. A., *The structure of compact groups. A primer for the student—a handbook for the expert*, Second revised and augmented edition, De Gruyter Studies in Mathematics 25, Walter de Gruyter & Co., Berlin, (2006).

- [45] Holický P., *Čech-analytic and almost  $K$ -descriptive spaces*, Czechoslovak Math. J., Volume 43, (1993), Issue 3, pp. 451-466.
- [46] Holický P., *Descriptive classes of sets in nonseparable spaces*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math., Volume 104, (2010), Issue 2, pp. 257-282.
- [47] Hosseini K.; Lovett S.. *A bilinear Bogolyubov-Ruzsa lemma with polynomial bounds*, Preprint [arxiv:1808.04965](https://arxiv.org/abs/1808.04965).
- [48] Host B.; Kra B., *Nilpotent structures in ergodic theory*, Mathematical Surveys and Monographs Volume: 236, (2018), 427 pp.
- [49] Host B.; Kra B., *Parallelepipeds, nilpotent groups and Gowers norms*, Bulletin de la société mathématique de France, Tome 136, (2008) Number 3, pp. 405-437.
- [50] Host B.; Kra B., *Nonconventional ergodic averages and nilmanifolds*, Ann. of Math., Volume 161, (2005), Issue 1, pp. 397-488.
- [51] Host B.; Kra B.; Maass A., *Nilsequences and a structure theorem for topological dynamical systems*, Adv. Math., Volume 224, (2010), Number 1, pp. 103-129.
- [52] Jayne J. E., *Structure of analytic Hausdorff spaces*, Mathematika, Volume 23, (1976), Issue 2, pp. 208-211.
- [53] Jayne J. E.; Namioka I.; Rogers C. A., *Topological properties of Banach spaces*, Proc. London Math. Soc., Volume s3-66, (1993), Issue 3, pp. 651-672.
- [54] Kechris A. S., *Classical descriptive set theory*, Graduate Texts in Mathematics, Volume 156, Springer-Verlag, New York, (1995).
- [55] Kemperman J. H. B., *On products of sets in a locally compact group*, Fund. Math., Volume 56, (1964), Issue 1, pp. 51-68.
- [56] Kleppner A., *Measurable homomorphisms of locally compact groups* Proceedings of the American Mathematical Society, Volume 106, (1989), Number 2, pp. 391-395.
- [57] Kneser M., *Summenmengen in lokalkompakten abelschen Gruppen*, Math. Z., Volume 66, (1956/57), pp. 88-110.

- [58] Kysiak M., *Bernstein sets with algebraic properties*, Cent. Eur. J. Math., (2009), 7: 725.
- [59] Lev V. F., *Distribution of points on arcs*, Integers: Electronic Journal of Combinatorial Number Theory 5(2), (2005).
- [60] Lusin N., *Sur la classification de M. Baire*, C. R. Acad. Sci. Paris, Volume 164, (1917), pp. 91-94.
- [61] Macbeath A. M., *On the measure of sum sets, II. The sum-theorem for the torus*, Math. Proc. Cambridge Phil. Soc., Volume 49, (1953), Issue 1, pp. 40-43.
- [62] Mal'cev A. I., *On a class of homogeneous spaces*, Izv. Akad. Nauk. SSSR. Ser. Mat., Volume 13, (1949), Issue 1, pp. 9-32.
- [63] Manners F., *Quantitative bounds in the inverse theorem for the Gowers  $U^{s+1}$ -norms over cyclic groups*, preprint. [arXiv:1811.00718](https://arxiv.org/abs/1811.00718).
- [64] Matolcsi M.; Ruzsa I. Z., *Sets with no solutions to  $x+y = 3z$* , European J. Combin., Volume 34, (2013), Number 8, pp. 1411-1414.
- [65] Munkres J. R., *Topology* (Second Edition), Prentice Hall, (2000).
- [66] Parry W., *Ergodic properties of affine transformations and flows on nilmanifolds*, Amer. J. Math., Volume 91, (1969), Number 3, pp. 757-771.
- [67] Petridis G., *New Proofs of Plünnecke-type Estimates for Product Sets in Groups*, Combinatorica, Volume 32, (2012), Number 6, pp. 721-733.
- [68] Petridis G., *The Plünnecke-Ruzsa inequality: an overview*, Combinatorial and additive number theory—CANT, Volume 101, (2014) pp. 229-241.
- [69] Plagne A.; de Roton A., *Maximal sets with no solution to  $x + y = 3z$* , Combinatorica, Volume 36, (2016), Number 2, pp. 229-248.
- [70] Plünnecke H., *Eine zahlentheoretische anwendung der graphtheorie*, J. Reine Angew. Math., Volume 243, (1970), pp. 171-183.
- [71] Raikov D., *On the addition of point-sets in the sense of Schnirelmann*, Rec. Math. [Mat. Sbornik] N.S., Volume 5(47), (1939), Number 2, pp. 425-440.

- [72] Rødseth Ø. J., *On Freiman's 2.4-theorem*, Skr. K. Nor. Vidensk. Selsk, Volume 4, (2006), pp. 11-18.
- [73] Rogers, C. A.; Jayne, J. E.; Dellacherie, C.; Topsoe, F.; Hoffman-Jorgensen, J.; Martin, D. A.; Kechris, A. S.; Stone, A. H., *Analytic sets*, Academic Press, London-New York, (1980), 499 pp.
- [74] Roth K. F., *On certain sets of integers* J. London Math. Soc., Volume s1-28, (1953), Issue 1, pp. 104-109.
- [75] Rudin W., *Fourier analysis on groups*, Interscience Tracts in Pure and Applied Mathematics, Number 12, Interscience Publishers, New York-London, (1962).
- [76] Ruzsa I. *An application of graph theory to additive number theory*, Sci., Ser. A Math. Sci. (N. S.), 3 (1989), pp. 97-109.
- [77] Samuel. P., *Géométrie projective*, Presses Universitaires de France, Paris, (1986).
- [78] Sanders T., *On Roth's theorem on progressions*, Ann. of Math., Volume 174, (2011), Issue 1, pp. 619-636.
- [79] Sanders. T., *On the Bogolyubov-Ruzsa lemma*. Anal. PDE, Volume 5, (2012), Number 3, pp. 627-655.
- [80] Sepanski, M.R., *Compact Lie Groups*, Graduate Texts in Mathematics, vol 235. Springer, New York (2007).
- [81] Serra O.; Zémor G., *Large sets with small doubling modulo  $p$  are well covered by an arithmetic progression*, Ann. Inst. Fourier (Grenoble), Volume 59, (2009), Issue 5, pp. 2043-2060.
- [82] Schoen T., *Linear equations in  $\mathbb{Z}_p$* , Bull. London Math. Soc., Volume 37, (2005), Issue 4, pp. 495-501.
- [83] Sierpiński W., *Sur la question de la mesurabilité de la base de M. Hamel*, Fund. Math., Volume 1, (1920), Issue 1, pp. 105-111.
- [84] Sion M., *Topological and Measure Theoretic Properties of Analytic Sets*, Proc. Amer. Math. Soc., Volume 11, (1960), Number 5, pp. 769-776.

- [85] Souslin M., *Sur une définition des ensembles mesurables  $B$  sans nombres transfinis*, C. R. Acad. Sci. Paris, Volume 164, (1917), pp. 88-91.
- [86] Szegedy B., *On higher order Fourier analysis*, preprint 2012. [arXiv:1203.2260](https://arxiv.org/abs/1203.2260).
- [87] Szemerédi E., *On sets of integers containing no  $k$  elements in arithmetic progression*, Acta Arithmetica., Volume 27, (1975), pp. 199-245.
- [88] Tao T., *Product set estimates for non-commutative groups*, Combinatorica, Volume 28, (2008), Issue 5, pp. 547-594.
- [89] Vosper G., *The critical pairs of subsets of a group of prime order*, J. London Math. Soc., Volume s1-31, (1956), Issue 2, pp. 200-205.
- [90] Ziegler T., *Universal characteristic factors and Furstenberg averages*, J. Amer. Math. Soc., Volume 20, (2007), Number 1, pp. 53-97.