Condensation and densification for sets of large diameter

Trevor D. Wooley

Department of Mathematics, Purdue University, 150 N. University Street, West Lafayette, IN 47907-2067, USA,
twooley@purdue.edu

Abstract. Consider a set of integers $\mathscr{A}$ having finite diameter X, and a system of simultaneous polynomial equations to be solved over $\mathscr{A}$. In many circumstances, it is known that the number of solutions of this system is $O(X^\varepsilon|\mathscr{A}|^\theta)$ for a suitable $\theta > 0$ and any $\varepsilon > 0$. These estimates become worse than trivial when the diameter X is very large compared to $|\mathscr{A}|$, or equivalently, when the set $\mathscr{A}$ is very sparse. This motivates the problem of seeking a new set of integers $\mathscr{B}$, in a certain sense isomorphic to $\mathscr{A}$, having the property that the diameter X' of $\mathscr{B}$ is smaller than X, and at the same time the set $\mathscr{B}$ preserves the salient features of the solution set of the system of equations in question. We report on our speculative investigations concerning this problem closely associated with the topic of Freiman homomorphisms.

1 Introduction

Given a system of polynomial equations having integral coefficients, the investigation of solution sets with variables restricted to a given finite set of integers $\mathscr{A}$ is of basic interest in arithmetic combinatorics. Even for a fixed system of equations, comprehensive knowledge concerning such solution sets seems a goal far too ambitious to be realised, for the sets $\mathscr{A}$ to which variables are restricted may contain extraordinarily complicated constellations of arbitrarily large size. In this paper we seek to understand such solution sets in terms of related sets of integers, every element of which is bounded purely in terms of the cardinality of $\mathscr{A}$ and the data associated with the system of polynomials in question. Thus, in a certain sense, our conclusions derive faithful models of solution sets in arithmetic combinatorics. Any model of this type having elements of least size might reasonably be interpreted as a minimal model. The interest in such models lies in the hope that a minimal model might be more easily understood than a non-minimal and potentially very sparse counterpart. There are close parallels with the concept of Freiman homomorphisms and isomorphisms (see [4], [5] and, for example, [14, Definition 5.21]) in the situation wherein these mappings take one set of integers to another. Although we comment further on such considerations in due course, we emphasise for now the importance for us of remaining within the same ring rather than mapping to a finite field. We express the hope that, despite our investigations on these matters being rudimentary in nature, they may provide a stimulus for further work.

Further discussion requires the introduction of some notation. We are interested primarily in finite sets of integers $\mathscr{A} \subset \mathbb{Z}$. We write A for $\mathrm{card}(\mathscr{A})$. Two notions of the size of the elements of $\mathscr{A}$ play a role in our discussions. First, there is the *diameter* of $\mathscr{A}$, namely

$$\mathrm{diam}(\mathscr{A}) = \max \mathscr{A} - \min \mathscr{A} + 1.$$

Second, there is the *enveloping radius* of $\mathscr{A}$, by which we mean

$$\mathrm{env}(\mathscr{A}) = \max\{|a| : a \in \mathscr{A}\} + 1.$$

It is apparent that $\mathrm{diam}(\mathscr{A})$ and $\mathrm{env}(\mathscr{A})$ provide very crude measures of the complexity of the set $\mathscr{A}$ in wide generality[1]. One focus of interest for us concerns translation-dilation invariant (TDI) systems of equations, such as the familiar linear equation $x_1 + x_2 = x_3 + x_4$. When considering the solutions of such an equation with $\mathbf{x} \in \mathscr{A}^4$, it is apparent that no information concerning the solution set is lost if one translates the elements of $\mathscr{A}$ by a fixed integer b to obtain a new set $\mathscr{A}' = \{a - b : a \in \mathscr{A}\}$. Consequently, there is no loss of generality in assuming that $\min \mathscr{A} = 0$, and in such circumstances it is more natural to measure the complexity of the set $\mathscr{A}$ by means of its diameter rather than its enveloping radius.

The measures $\mathrm{env}(\mathscr{A})$ and $\mathrm{diam}(\mathscr{A})$ play a critical role in the best available upper bounds for certain mean values of additive number theory. For example, when s and k are natural numbers and $\mathscr{A} \subset \mathbb{Z}$ is finite, let $J_{s,k}(\mathscr{A})$ denote the number of solutions of the system of equations

$$x_1^j + \ldots + x_s^j = x_{s+1}^j + \ldots + x_{2s}^j \quad (1 \leqslant j \leqslant k),$$

with $x_i \in \mathscr{A}$ $(1 \leqslant i \leqslant 2s)$. Likewise, when $\varphi_j \in \mathbb{Z}[t]$ $(1 \leqslant j \leqslant k)$, denote by $J_{s,k}(\mathscr{A}; \boldsymbol{\varphi})$ the number of solutions of the system of equations

$$\varphi_j(x_1) + \ldots + \varphi_j(x_s) = \varphi_j(x_{s+1}) + \ldots + \varphi_j(x_{2s}) \quad (1 \leqslant j \leqslant k),$$

with $x_i \in \mathscr{A}$ $(1 \leqslant i \leqslant 2s)$. We begin by recalling a consequence of recent work resolving the main conjecture in Vinogradov's mean value theorem.

[1] The presence of the additional term 1 in these definitions may seem mysterious, but is designed to align with a subsequent definition appropriate for the situation in algebraic number fields.

Theorem 1.1. *Let $\mathscr{A} \subset \mathbb{Z}$ be finite.*

(i) Suppose that $\varphi_j \in \mathbb{Z}[t]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials with

$$\det\left(\frac{\mathrm{d}^i \varphi_j(t)}{\mathrm{d}t^i}\right)_{1\leqslant i,j\leqslant k} \neq 0.$$

Also, let s and k be natural numbers with $s \leqslant k(k+1)/2$. Then for each $\varepsilon > 0$, one has

$$J_{s,k}(\mathscr{A};\boldsymbol{\varphi}) \ll \mathrm{env}(\mathscr{A})^{\varepsilon} A^s. \tag{1.1}$$

(ii) For all natural numbers s and k, and each $\varepsilon > 0$, one has

$$J_{s,k}(\mathscr{A}) \ll \mathrm{diam}(\mathscr{A})^{\varepsilon}(A^s + A^{2s-k(k+1)/2}). \tag{1.2}$$

In each asymptotic bound, the constants implicit in Vinogradov's notation $\ll$ may depend on ε, s, k and the coefficients of $\boldsymbol{\varphi}$.

Both of the conclusions of Theorem 1.1 are immediate consequences of Wooley [17, Theorem 1.1], as we explain in §9 below, and the conclusion (ii) is also immediate from the work of Bourgain, Demeter and Guth [3]. The motivating observation we wish to highlight here is that both estimates (1.1) and (1.2) are worse than trivial when the set $\mathscr{A}$ is extremely sparse. Suppose, for example, that

$$\mathrm{diam}(\mathscr{A}) \asymp \exp(\exp(A)).$$

Then the estimates (1.1) and (1.2) are inferior to the trivial bounds $J_{s,k}(\mathscr{A};\boldsymbol{\varphi}) \leqslant A^{2s}$ and $J_{s,k}(\mathscr{A}) \leqslant A^{2s}$. This observation remains valid for the improved estimates for $J_{3,2}(\mathscr{A})$ and $J_{6,3}(\mathscr{A})$ made available, respectively in the very recent work reported in [8], [9] and [13]. It seems reasonable to speculate that the extremal situation is that in which $\mathscr{A}$ consists of A consecutive integers.

Conjecture 1. Suppose that $\mathscr{A} \subset \mathbb{Z}$ is finite and $s, k \in \mathbb{N}$. Then

$$J_{s,k}(\mathscr{A}) \leqslant J_{s,k}(\{1,2,\ldots,A\}).$$

Moreover, for each $\varepsilon > 0$, one has

$$J_{s,k}(\mathscr{A}) \ll_{\varepsilon,s,k} A^{s+\varepsilon} + A^{2s-k(k+1)/2}. \tag{1.3}$$

By elimination, one finds that the bound $J_{s,k}(\mathscr{A}) \ll A^s + A^{2s-k}$ is essentially trivial. When $k \geqslant 2$, this estimate remains very far from that asserted in Conjecture 1. The only other non-trivial bound of which the author is aware is an estimate very slightly stronger than

$$J_{s,2}(\mathscr{A}) \ll A^{2s-3+2^{2-s}} \quad (s \geqslant 3)$$

due to Mudgal [12, Theorem 1.1]. With progress towards Conjecture 1 in mind, it would be desirable to have available a set $\mathscr{C}$ associated with a sparse set $\mathscr{A}$ having the property that

$$J_{s,k}(\mathscr{A}) = J_{s,k}(\mathscr{C}),$$

or even merely

$$J_{s,k}(\mathscr{A}) \ll J_{s,k}(\mathscr{C}),$$

and, moreover, having much smaller diameter than $\mathscr{A}$. Were one to have the upper bound $\mathrm{diam}(\mathscr{C}) \leqslant A^c$, for some fixed $c > 0$, for example, then the conjecture (1.3) would follow from Theorem 1.1(ii). Although such cannot be true in general, one is led to the broader problem of determining the extent to which such compressions might be achieved in practice. This problem concerning *condensations* is formalised in §2, and explored in §§3, 4 and 5. We direct the reader to Theorem 5.1 for our most general conclusions concerning condensations associated with systems of polynomial equations. Write c_1 and c_2 for suitable positive constants. Then a very rough idea of these conclusions can be surmised if we note, first, that we are forced to work in a number field of degree as large as $\exp_2(c_1 A)$, and second, that our condensations contain elements roughly of size $\exp_4(c_2 A)$. Here, and throughout, we use $\exp_m(\cdot)$ to denote the m-fold iterated exponential function. Thus

$$\exp_1(x) = e^x, \quad \exp_2(x) = e^{e^x},$$

and so on.

An alternate strategy for obtaining bounds of the shape (1.3) has a very different flavour. One might surmise that the difficulty in applying Theorem 1.1 to establish the estimate (1.3) of Conjecture 1 stems from the awkward nature of ultra-sparse sets $\mathscr{A}$ having very large diameter compared to their cardinality A. One might therefore seek to obtain a much denser set $\mathscr{D}$ associated with $\mathscr{A}$, having the property that for some large integer N one has

$$\mathrm{card}(\mathscr{D}) = (\mathrm{card}(\mathscr{A}))^N \quad \text{and} \quad J_{s,k}(\mathscr{A}) = J_{s,k}(\mathscr{D})^{1/N},$$

while at the same time $\operatorname{diam}(\mathscr{D})$ is not much larger than $\operatorname{diam}(\mathscr{A})$. This set $\mathscr{D}$ would be a much denser analogue of $\mathscr{A}$ with the potential that $\operatorname{diam}(\mathscr{D}) \leqslant (\operatorname{card}(\mathscr{D}))^c$, for some fixed $c > 0$. In these circumstances, the conjectured estimate (1.3) would again follow from Theorem 1.1(ii). We formalise this problem of *densification* in §6 and explore it in §7.

It seems worth remarking that the concepts of condensation and densification possess interpretations also in the scenario wherein sets of integers are replaced by finite sets of real numbers, or even finite subsets of a characteristic zero integral domain. We make some remarks in this direction in §8.

We view both the strategies of condensation and densification of sets of large diameter as being of interest in their own right. We emphasise that our conclusions do not achieve the level whereby application to Conjecture 1 can reasonably be envisioned.

Acknowledgements: This work was supported in its initial phases by a European Research Council Advanced Grant under the European Union's Horizon 2020 research and innovation programme via grant agreement No. 695223. The bulk of the work reported here was obtained while the author was supported by the National Science Foundation via Grant No. DMS-1854398 and DMS-2001549. The author wishes to express his gratitude to Julia Wolf for some early discussions on the topic of this paper, and to Ben Barber for discussion concerning an idea that led to Theorem 2.1.

We write $X \asymp Y$ when, in Vinogradov's notation, we have

$$X \ll Y \ll X.$$

Also, when θ is a real number, we write $\lceil \theta \rceil$ for the least integer m with $m \geqslant \theta$, and likewise $\lfloor \theta \rfloor$ for the largest integer m with $m \leqslant \theta$. In addition, we write $\|\theta\|$ for $\min\{|\theta - m| : m \in \mathbb{Z}\}$. Finally, we make frequent use of vector notation in the form $\mathbf{x} = (x_1, \ldots, x_r)$. Here, the dimension r depends on the course of the argument.

2 Condensations of sets

The informal introduction of condensations in §1 provides a framework insufficient for the more serious discussion on which we now embark. We begin by introducing a notion generalising that of a Freiman isomorphism.

Definition 2.1. *Let $\mathscr{A}$ and $\mathscr{B}$ be finite sets of integers, and suppose that we are given polynomials $P_1, \ldots, P_r \in \mathbb{Z}[x_1, \ldots, x_s]$. We say that a* *bijection* $\psi : \mathscr{A} \to \mathscr{B}$ *is a Freiman* $\mathbf{P}$*-isomorphism if, whenever one has* $(x_1, \ldots, x_s) \in \mathscr{A}^s$*, then*

$$P_i(x_1, \ldots, x_s) = 0 \quad (1 \leqslant i \leqslant r)$$

if and only if

$$P_i(\psi(x_1), \ldots, \psi(x_s)) = 0 \quad (1 \leqslant i \leqslant r).$$

We emphasise here that a Freiman $\mathbf{P}$-isomorphism is specific to a particular polynomial tuple $\mathbf{P}$, since our focus will lie on the solution set of a fixed polynomial system. This is in contrast with a similar definition given in work of Grosu (see the preamble to the statement of [7, Theorem 1.3]). Moreover, also in contrast to the latter and indeed other sources concerning Freiman isomorphisms, we shall only be interested in situations wherein both $\mathscr{A}$ and $\mathscr{B}$ lie in the same ring. This restriction permits iterative approaches in which one composes a sequence of Freiman $\mathbf{P}$-isomorphisms $\psi_1, \psi_2, \ldots, \psi_n$ to obtain a new Freiman $\mathbf{P}$-isomorphism $\psi_n \circ \psi_{n-1} \circ \ldots \circ \psi_1$.

A few words of explanation seem warranted concerning our interest in Freiman $\mathbf{P}$-isomorphisms. We are interested in the structure of the solutions of the system of polynomials

$$P_i(x_1, \ldots, x_s) = 0 \quad (1 \leqslant i \leqslant r), \tag{2.1}$$

with $\mathbf{x} \in \mathscr{A}^s$. This is described precisely by the hypergraph $\mathit{\Gamma}(\mathscr{A}; \mathbf{P})$ with the elements of $\mathscr{A}$ as vertices, and having hyperedges defined by the s-tuples $\mathbf{x}$ from $\mathscr{A}^s$ satisfying the system of equations (2.1). With this characterisation of the structure of the solution set of (2.1) in mind, it is apparent that the mapping

$$\mathit{\Psi} : \mathit{\Gamma}(\mathscr{A}; \mathbf{P}) \to \mathit{\Gamma}(\mathscr{B}; \mathbf{P}),$$

induced by a Freiman $\mathbf{P}$-isomorphism $\psi : \mathscr{A} \to \mathscr{B}$, delivers a bijection that preserves every feature of the solution set of (2.1) as one replaces $\mathscr{A}$ by $\mathscr{B} = \psi(\mathscr{A})$.

Given a finite set of integers $\mathscr{A}$ and a system of polynomials $\mathbf{P} \in \mathbb{Z}[\mathbf{x}]^r$, our interest lies in finding a set $\mathscr{B}$ Freiman $\mathbf{P}$-isomorphic to $\mathscr{A}$ with $\mathscr{B}$ having elements intrinsically smaller than those of $\mathscr{A}$. Since $\mathit{\Gamma}(\mathscr{B}; \mathbf{P})$ is in bijective correspondence with $\mathit{\Gamma}(\mathscr{A}; \mathbf{P})$, one may expect that the salient features of the solution structure of the system (2.1) with $\mathbf{x} \in \mathscr{A}^s$ may be more easily determined by instead considering solutions $\mathbf{x} \in \mathscr{B}^s$. This motivates the next definition.

Definition 2.2. *We say that a mapping $\psi : \mathscr{A} \to \mathscr{C}$ is a $\mathbf{P}$-condenser of $\mathscr{A}$ if it is a Freiman $\mathbf{P}$-isomorphism for which $\mathit{env}(\mathscr{C}) \leqslant \mathit{env}(\mathscr{A})$. When the latter inequality is strict, we refer to ψ as a strict $\mathbf{P}$-condenser of $\mathscr{A}$. In either case, we refer to $\mathscr{C}$ as being a $\mathbf{P}$-condensation of $\mathscr{A}$.*

We make an observation here concerning TDI systems of polynomials $\mathbf{P}$. Suppose that $\min \mathscr{A} = b$. Then by considering the mapping $\psi : \mathscr{A} \to \mathbb{Z}$ defined by $a \mapsto a - b$, we see that $\mathscr{A}$ possesses a $\mathbf{P}$-condensation $\mathscr{B}$ with $\mathrm{env}(\mathscr{B}) = \mathrm{diam}(\mathscr{B})$.

Of particular interest are the $\mathbf{P}$-condensations $\mathscr{B}$ of $\mathscr{A}$ distinguished by the property that $\mathrm{env}(\mathscr{B})$ is minimal.

Definition 2.3. *The $\mathbf{P}$-essential enveloping radius of $\mathscr{A}$ is*

$$\mathit{env}^*(\mathscr{A}; \mathbf{P}) = \min\{\mathit{env}(\psi(\mathscr{A})) : \psi \text{ is a } \mathbf{P}\text{-condenser of } \mathscr{A}\},$$

and the $\mathbf{P}$-essential diameter of $\mathscr{A}$ is

$$\mathit{diam}^*(\mathscr{A}; \mathbf{P}) = \min\{\mathit{diam}(\psi(\mathscr{A})) : \psi \text{ is a } \mathbf{P}\text{-condenser of } \mathscr{A}\}.$$

The notion of the $\mathbf{P}$-essential enveloping radius of a finite set $\mathscr{A} \subset \mathbb{Z}$ provides a measure of the complexity of $\mathscr{A}$ with respect to the system of equations (2.1), for it describes the minimal footprint of a set $\mathscr{B}$ for which the hypergraph $\mathit{\Gamma}(\mathscr{B}; \mathbf{P})$ associated with the solution set faithfully describes that of interest, namely $\mathit{\Gamma}(\mathscr{A}; \mathbf{P})$.

In general, the sharpest conclusions concerning $\mathrm{env}^*(\mathscr{A}; \mathbf{P})$ of which the author is aware are the trivial ones recorded in the following theorem.

Theorem 2.1. *Let $\mathbf{P} \in \mathbb{Z}[x_1, \dots, x_s]^r$ be a polynomial system, and let $\mathscr{A} \subset \mathbb{Z}$ be a finite set of integers having cardinality A. Then one has*

$$\lceil (A+1)/2 \rceil \leqslant \mathrm{env}^*(\mathscr{A}; \mathbf{P}) \ll_{A,\mathbf{P}} 1$$

and

$$A \leqslant \mathrm{diam}^*(\mathscr{A}; \mathbf{P}) \ll_{A,\mathbf{P}} 1.$$

We emphasise here that the upper bounds recorded in this theorem indicate that the $\mathbf{P}$-essential enveloping radius (respectively, the $\mathbf{P}$-essential diameter) of $\mathscr{A}$ depends at most on $A = \mathrm{card}(\mathscr{A})$ and the polynomials comprising $\mathbf{P}$, but not on the specific identity of the elements of $\mathscr{A}$. A few moments of reflection should disabuse the puzzled reader that this conclusion might be in any sense non-trivial.

Proof (of Theorem 2.1). The solution set of the polynomial system

$$P_i(x_1,\dots,x_s)=0\quad (1\leqslant i\leqslant r),$$

with $\mathbf{x}\in\mathscr{A}^s$, defines the hypergraph $\Gamma(\mathscr{A};\mathbf{P})$. Let $\mathscr{C}\subset\mathbb{Z}$ be any set of integers of cardinality A having smallest enveloping radius for which $\Gamma(\mathscr{C};\mathbf{P})$ is isomorphic to $\Gamma(\mathscr{A};\mathbf{P})$. Denote by ψ the mapping from $\mathscr{A}$ to $\mathscr{C}$ induced by this hypergraph isomorphism, and note that one possibility is that ψ is the identity mapping. The definitions of $\Gamma(\mathscr{C};\mathbf{P})$ and $\Gamma(\mathscr{A};\mathbf{P})$ ensure that $\psi:\mathscr{A}\rightarrow\mathscr{C}$ is a bijection satisfying the property that whenever $(x_1,\dots,x_s)\in\mathscr{A}^s$, then

$$P_i(x_1,\dots,x_s)=0\quad (1\leqslant i\leqslant r)$$

if and only if

$$P_i(\psi(x_1),\dots,\psi(x_s))=0\quad (1\leqslant i\leqslant r).$$

Hence, we see that ψ is a Freiman $\mathbf{P}$-isomorphism and also a $\mathbf{P}$-condenser of $\mathscr{A}$ with $\mathscr{C}=\psi(\mathscr{A})$.

The set of all hypergraphs on A vertices with hyperedges defined by s-tuples of vertices is finite in number. Indeed, the number of such hypergraphs depends at most on s and A. Thus, since $\mathscr{C}$ depends at most on the hypergraph isomorphism class of $\Gamma(\mathscr{A};\mathbf{P})$ and the polynomial system $\mathbf{P}$, one sees that $\mathrm{env}(\mathscr{C})$ depends at most on s, $\mathbf{P}$ and A. Since $\mathscr{C}=\psi(\mathscr{A})$ with ψ a $\mathbf{P}$-condenser of $\mathscr{A}$, it follows that $\mathrm{env}^*(\mathscr{A};\mathbf{P})\ll_{A,\mathbf{P}}1$. A similar conclusion is apparent also for $\mathrm{diam}^*(\mathscr{A};\mathbf{P})$ by arguing mutatis mutandis.

The lower bounds $\mathrm{env}^*(\mathscr{A};\mathbf{P})\geqslant\lceil(A+1)/2\rceil$ and $\mathrm{diam}^*(\mathscr{A};\mathbf{P})\geqslant A$ follow by considering sets $\mathscr{A}$ containing A consecutive integers.

3 Condensations for linear systems of equations

There is one class of polynomial systems for which the quantitative aspects of condensations are explicit, and for which the underlying methods possess familiar themes. Thus, the analysis of systems of linear polynomials $\mathbf{P}(\mathbf{x})$ is both simple and instructive, and serves as a warm-up for the analysis of the next two sections concerning polynomial systems. We focus in this section on such linear systems in order to motivate the more general discussion of the next section.

In order to fix ideas, suppose that $s\geqslant 2$, $r\geqslant 1$, and for $1\leqslant i\leqslant r$ fix $b_i\in\mathbb{Z}$ and $c_{ij}\in\mathbb{Z}$ $(1\leqslant j\leqslant s)$. We ignore the trivial situation in which for some index i one has $c_{ij}=0$ for $1\leqslant j\leqslant s$, since this will correspond to a case in which r is smaller. The system of polynomials of interest to us in this section is

$$P_i(\mathbf{x})=\sum_{j=1}^s c_{ij}x_j-b_i\quad (1\leqslant i\leqslant r).$$

When $\mathscr{A}\subset\mathbb{Z}$ is a finite set of integers, we write $S(\mathscr{A};\mathbf{P})$ for the set of solutions of the system of equations $P_i(\mathbf{x})=0$ $(1\leqslant i\leqslant r)$, with $\mathbf{x}\in\mathscr{A}^s$. Also, we define the integer $\Lambda=\Lambda(\mathbf{c},\mathbf{b})$ by putting

$$\Lambda=\max_{1\leqslant i\leqslant r}\biggl(|b_i|+\sum_{j=1}^s|c_{ij}|\biggr).$$

Thus, the quantity Λ provides a measure of the height of the coefficient matrix defining $\mathbf{P}$. Finally, it is convenient both here and elsewhere to introduce an integer that encapsulates both distinctness of the elements of $\mathscr{A}$, and also whether or not an s-tuple $\mathbf{a}$ lies in $S(\mathscr{A};\mathbf{P})$. Thus, we define

$$\Upsilon=\biggl(\prod_{\substack{a_1,a_2\in\mathscr{A}\\ a_1\neq a_2}}|a_1-a_2|\biggr)\biggl(\prod_{\substack{\mathbf{a}\in\mathscr{A}^s\\ \mathbf{a}\notin S(\mathscr{A};\mathbf{P})}}\sum_{i=1}^r|P_i(\mathbf{a})|\biggr).\tag{3.1}$$

Theorem 3.1. *Consider a system* $\mathbf{P}$ *of linear polynomials as described in the preamble, and consider a finite set of integers* $\mathscr{A}$*. Then provided that* $A=\mathrm{card}(\mathscr{A})$ *is sufficiently large in terms of* r *and* s*, one has*

$$\mathrm{env}^*(\mathscr{A};\mathbf{P})<\exp\left(3(\Lambda+1)^A\right).\tag{3.2}$$

Proof. A moment of reflection reveals that there is no loss of generality in supposing that $\Lambda\geqslant 2$ and $s\geqslant 2$. Write $X=\mathrm{env}(\mathscr{A})-1$. Our strategy is to find an integer h with $\Lambda<h<2X$ having the following three properties:

(i) when $a_1,a_2\in\mathscr{A}$ satisfy $a_1\neq a_2$, then $a_1\not\equiv a_2 \pmod h$;
(ii) when $\mathbf{a}\notin S(\mathscr{A};\mathbf{P})$, then there is an index i with $1\leqslant i\leqslant r$ for which one has $P_i(\mathbf{a})\not\equiv 0\pmod h$;
(iii) for every $a\in\mathscr{A}$, one has $\|a/h\|<1/\Lambda$.

If such an integer h can be found, then we may define the map $\psi:\mathscr{A}\to\mathbb{Z}$ by putting

$$\psi(a)=[a\ (\mathrm{mod}\ h)]\,,$$

where $[a \pmod h]$ denotes the numerically least residue of a modulo h. To be clear, the numerically least residue of a modulo h is the integer m with $-h/2 < m \leqslant h/2$ for which $a \equiv m \pmod h$. Property (i) then ensures that the set $\mathscr{B} = \psi(\mathscr{A})$ is in bijective correspondence with $\mathscr{A}$. Also, property (ii) ensures that whenever $\mathbf{a} \notin S(\mathscr{A};\mathbf{P})$, then for some index i with $1 \leqslant i \leqslant r$, one has

$$P_i(\psi(\mathbf{a})) \equiv P_i(\mathbf{a}) \not\equiv 0 \pmod h,$$

whence $P_i(\psi(\mathbf{a})) \neq 0$. However, when $\mathbf{a} \in \mathcal{S}(\mathscr{A};\mathbf{P})$, one has

$$P_i(\psi(\mathbf{a})) \equiv P_i(\mathbf{a}) \equiv 0 \pmod h \quad (1 \leqslant i \leqslant r).$$

At the same time, in view of property (iii), one has

$$|P_i(\psi(\mathbf{a}))| < \biggl(|b_i| + \sum_{j=1}^{s} |c_{ij}|\biggr)\frac{h}{\Lambda} \leqslant h,$$

whence $P_i(\psi(\mathbf{a})) = 0$ $(1 \leqslant i \leqslant r)$. We therefore infer that the map ψ is a Freiman $\mathbf{P}$-isomorphism from $\mathscr{A}$ to $\mathscr{B}$. Consequently, since

$$\mathrm{env}(\mathscr{B}) - 1 \leqslant h/2 < X = \mathrm{env}(\mathscr{A}) - 1,$$

we have confirmed the existence of a strict $\mathbf{P}$-condenser of $\mathscr{A}$.

We establish the existence of a suitable integer h by modifying very slightly an argument employed by Baker and Harman (see [1, Proposition 1]). Recall the definition (3.1) of the integer Υ. A crude estimate delivers the bounds

$$1 \leqslant \Upsilon \leqslant (2X)^{A^2-A}(r\Lambda X)^{A^s} \leqslant \tfrac{1}{3}(r\Lambda X)^{2A^s}. \tag{3.3}$$

The number of prime divisors of Υ exceeding $\log(3\Upsilon)$ cannot exceed

$$\frac{\log(3\Upsilon)}{\log\log(3\Upsilon)}.$$

Thus, an application of the prime number theorem reveals that whenever Y is large and $Y \geqslant 2\log(3\Upsilon)$, then in any interval $(Y, 2Y)$, there exists a prime π with $\pi \nmid \Upsilon$. It therefore follows from (3.3) that we may choose a prime π with $\pi \nmid \Upsilon$ for which

$$\pi < 4\log(3\Upsilon) \leqslant 8A^s \log(r\Lambda X). \tag{3.4}$$

We put

$$L = \mathrm{lcm}[1, 2, \ldots, (\varLambda + 1)^A]$$

and note that an elementary application of the prime number theorem ensures that, when A is large, one has $L \leqslant \exp(2(\varLambda + 1)^A)$. Next, by applying the multidimensional version of Dirichlet's box principle to the real numbers $a/(\pi L)$ $(a \in \mathscr{A})$, it follows that for some $\rho \in \mathbb{N}$ satisfying $1 \leqslant \rho \leqslant (\varLambda + 1)^A$, one has

$$\left\| \frac{\rho a}{\pi L} \right\| \leqslant \frac{1}{\varLambda + 1} \quad (a \in \mathscr{A}).$$

Since $\rho | L$, we may therefore define the integer $h = \pi L/\rho$, and then we see that

$$\|a/h\| \leqslant (\varLambda + 1)^{-1} \quad (a \in \mathscr{A}). \tag{3.5}$$

By construction, the integer h is divisible by π. We now exploit the fact that $\pi \nmid \varUpsilon$ using the definition (3.1). Thus, when $a_1, a_2 \in \mathscr{A}$ satisfy $a_1 \neq a_2$, one has $a_1 \not\equiv a_2 \pmod{\pi}$. Moreover, when $\mathbf{a} \in \mathscr{A}^s$ one sees that $P_i(\mathbf{a}) \equiv 0 \pmod{\pi}$ $(1 \leqslant i \leqslant r)$ if and only if $\mathbf{a} \in S(\mathscr{A}; \mathbf{P})$. In combination with (3.5), therefore, it is apparent that the properties (i), (ii) and (iii) above all hold for the integer h that we have constructed. In particular, the map $\psi : \mathscr{A} \to \mathbb{Z}$ defined by putting $\psi(a) = [a \pmod{h}]$ gives a Freiman $\mathbf{P}$-isomorphism from $\mathscr{A}$ to $\mathscr{B} = \psi(\mathscr{A})$ in which, on recalling (3.4), we see that

$$\mathrm{env}(\mathscr{B}) - 1 \leqslant h/2 \leqslant \pi L/2 < 4A^s \log(r\varLambda X)\exp(2(\varLambda + 1)^A).$$

We may summarise our deliberations thus far in the following form. Whenever $\mathscr{A}$ is a finite subset of $\mathbb{Z}$ with cardinality A and enveloping radius $X + 1$, then $\mathscr{A}$ possesses a $\mathbf{P}$-condensation $\mathscr{A}_1 = \psi(\mathscr{A})$ with enveloping radius at most $X_1 + 1$, where

$$X_1 = 4A^s \log(r\varLambda X)\exp\left(2(\varLambda + 1)^A\right).$$

When A is large in terms of r and s, and $X + 1 \geqslant \exp(3(\varLambda + 1)^A)$, we have

$$4A^s \left(\log(r\varLambda) + \log X\right) \leqslant \tfrac{1}{2} X^{1/3}.$$

Thus, under the same conditions on A and X, it follows that

$$X_1 \leqslant \tfrac{1}{2} X^{1/3}(X + 1)^{2/3} < X,$$

and consequently one has $\mathrm{env}(\mathscr{A}_1) < \mathrm{env}(\mathscr{A})$. Provided that

$$\mathrm{env}(\mathscr{A}_1) \geqslant \exp\left(3(\varLambda + 1)^A\right),$$

we may apply this process again, next showing that $\mathscr{A}_1$ has a $\mathbf{P}$-condensation $\mathscr{A}_2$ with $\mathrm{env}(\mathscr{A}_2) < \mathrm{env}(\mathscr{A}_1)$. Since $\mathbf{P}$-condensers may be composed, it follows that $\mathscr{A}$ also has a $\mathbf{P}$-condensation $\mathscr{A}_2$ with enveloping radius smaller than $\mathrm{env}(\mathscr{A}_1)$. By iterating this process repeatedly, with each iteration reducing the enveloping radius of the condensation of $\mathscr{A}$, we ultimately obtain a condensation $\mathscr{A}^*$ of $\mathscr{A}$ for which

$$\mathrm{env}(\mathscr{A}^*) < \exp\left(3(\mathit{\Lambda}+1)^A\right).$$

This establishes the bound (3.2), and the proof of the theorem is complete.

In the situation in which $\mathbf{b} = \mathbf{0}$, so that all of the linear polynomials are homogeneous, there is more freedom to apply changes of variable to advantage. Here the arguments are reminiscent of those employed in the proof of versions of Freiman's theorem (see, for example, the proof of [2, Theorem 2.1]).

Theorem 3.2. *Consider a system* $\mathbf{P}$ *of linear polynomials with* $\mathbf{b} = \mathbf{0}$*, as described in the preamble to the statement of Theorem 3.1. Also, consider a finite set of integers* $\mathscr{A}$*. Then provided that* $A = \mathrm{card}(\mathscr{A})$ *is sufficiently large in terms of* r *and* s*, one has*

$$\mathrm{env}^*(\mathscr{A};\mathbf{P}) \leqslant (\mathit{\Lambda}+1)^A. \tag{3.6}$$

Proof. We proceed much as in the proof of Theorem 3.1, though with a twist en route. First, writing $X = \mathrm{env}(\mathscr{A}) - 1$ and defining the integer $\mathit{\Upsilon}$ as in (3.1), we again obtain the bound (3.3), and conclude that there exists a prime number π with $\pi \nmid \mathit{\Upsilon}$ satisfying the property that

$$(\mathit{\Lambda}+1)^A < \pi < 2\max\{(\mathit{\Lambda}+1)^A, 4A^s\log(r\mathit{\Lambda}X)\}. \tag{3.7}$$

By applying the multidimensional version of Dirichlet's approximation theorem to the real numbers a/π $(a \in \mathscr{A})$, it follows that for some $\rho \in \mathbb{N}$ with $1 \leqslant \rho \leqslant (\mathit{\Lambda}+1)^A$, one has

$$\left\|\frac{\rho a}{\pi}\right\| \leqslant \frac{1}{\mathit{\Lambda}+1} \quad (a \in \mathscr{A}).$$

We fix any such integer ρ, noting that since $\pi > \rho$, one has $(\rho, \pi) = 1$. It follows that:

(i) whenever $a_1, a_2 \in \mathscr{A}$ satisfy $a_1 \neq a_2$, then $\rho a_1 \not\equiv \rho a_2 \pmod{\pi}$;

(ii) whenever $\mathbf{a} \notin S(\mathscr{A};\mathbf{P})$, then there is an index i with $1 \leqslant i \leqslant r$ for which one has $P_i(\rho\mathbf{a}) \not\equiv 0 \pmod{\pi}$;

(iii) for every $a \in \mathscr{A}$, one has $\|\rho a/\pi\| < 1/\varLambda$.

We now define the map $\psi : \mathscr{A} \to \mathbb{Z}$ by putting

$$\psi(a) = [\rho a \ (\mathrm{mod}\ \pi)].$$

Property (i) then ensures that the set $\mathscr{C} = \psi(\mathscr{A})$ is in bijective correspondence with $\mathscr{A}$. Also, property (ii) ensures that whenever $\mathbf{a} \notin S(\mathscr{A};\mathbf{P})$, then for some index i with $1 \leqslant i \leqslant r$, one has

$$P_i(\psi(\mathbf{a})) \equiv \rho P_i(\mathbf{a}) \not\equiv 0 \ (\mathrm{mod}\ \pi),$$

whence $P_i(\psi(\mathbf{a})) \neq 0$. However, when $\mathbf{a} \in S(\mathscr{A};\mathbf{P})$, one has

$$P_i(\psi(\mathbf{a})) \equiv \rho P_i(\mathbf{a}) \equiv 0 \ (\mathrm{mod}\ \pi) \quad (1 \leqslant i \leqslant r).$$

At the same time, in view of property (iii), one has

$$|P_i(\psi(\mathbf{a}))| < \frac{\pi}{\varLambda} \sum_{j=1}^{s} |c_{ij}| \leqslant \pi,$$

whence $P_i(\psi(\mathbf{a})) = 0$ $(1 \leqslant i \leqslant r)$. We therefore infer that ψ is a Freiman $\mathbf{P}$-isomorphism from $\mathscr{A}$ to $\mathscr{C}$. Consequently, provided that $\pi < 2X$, we see that

$$\mathrm{env}(\mathscr{C}) - 1 \leqslant \pi/2 < X = \mathrm{env}(\mathscr{A}) - 1,$$

and thus we have established the existence of a strict $\mathbf{P}$-condenser of $\mathscr{A}$.

Notice here that in view of (3.7), one has

$$\mathrm{env}(\mathscr{C}) - 1 \leqslant \pi/2 < \max\{(\varLambda+1)^A, 4A^s \log(r\varLambda X)\},$$

and we again have available an iterative process for reducing the enveloping radius of $\mathbf{P}$-condensations of $\mathscr{A}$ similar to that made available in the concluding stages of the proof of Theorem 3.1. When A is sufficiently large in terms of r and s, and $X \geqslant (\varLambda+1)^A$, we have

$$4A^s(\log(r\varLambda) + \log X) < X.$$

In this instance, therefore, under the same conditions on A and X, we discern from (3.7) that $\pi < 2X$ and hence that $\mathrm{env}(\mathscr{C}) < \mathrm{env}(\mathscr{A})$. Thus, our iteration continues until we obtain a $\mathbf{P}$-condensation $\mathscr{A}^*$ of $\mathscr{A}$ for which $\mathrm{env}(\mathscr{A}^*) - 1 < (\varLambda+1)^A$. This confirms the bound (3.6), and thus the proof of the theorem is complete.

The problem of obtaining lower bounds on $\mathrm{env}^*(\mathscr{A};\mathbf{P})$ has been considered in special cases such as that in which the system $\mathbf{P}$ consists of the single polynomial $x_1+x_2=x_3+x_4$. Here, it is apparent that the set $\mathscr{A}=\{0,1,2,4,\dots,2^{A-2}\}$ cannot be condensed into a fundamentally smaller set (see [10, §5]). Thus, in this special case, one has $\mathrm{env}^*(\mathscr{A};\mathbf{P})\gg 2^A$, and it is apparent that the upper bound on $\mathrm{env}^*(\mathscr{A};\mathbf{P})$ provided by Theorem 3.2 cannot in general be replaced by a quantity subexponential in A.

4 Condensations for non-linear systems of equations, I

Equipped with the discussion of §3 applicable to linear equations, we move on in this section to consider the corresponding situation for the solubility of polynomial equations of degree exceeding one over a finite subset $\mathscr{A}$ of the integers. Here, any attempt to merely mimic the proofs of Theorems 3.1 and 3.2 must plainly be abandoned. Suppose, for example, that we seek to analyse the solubility with $\mathbf{x}\in\mathscr{A}^4$ of the equation $x_1^2+x_2^2=x_3^2+x_4^2$ by utilising the map $\psi:\mathbb{Z}\to\mathbb{Z}/h\mathbb{Z}$ defined by putting $\psi(a)=[a\ (\mathrm{mod}\ h)]$ for a suitable positive integer h. The optimistic notion that the congruence

$$\psi(a_1)^2+\psi(a_2)^2\equiv\psi(a_3)^2+\psi(a_4)^2\ (\mathrm{mod}\ h)$$

might imply that

$$\psi(a_1)^2+\psi(a_2)^2=\psi(a_3)^2+\psi(a_4)^2$$

would seem to demand a choice for h ensuring that $|\psi(a)|<\frac{1}{4}h^{1/2}$ for all $a\in\mathscr{A}$. Such an eventuality cannot reasonably be countenanced for any but very special sets $\mathscr{A}$. However, a means of mapping subsets of finite fields into subsets of $\mathbb{C}$, while preserving associated solution structures, has been made available in work of Grosu [7]. With care, this approach can be wrought to yield a $\mathbf{P}$-condenser of sorts in the non-linear situation currently of interest to us.

The discussion of this section and the next requires the introduction of notions somewhat more flexible than those defined in §2. We have in mind now that the sets of integers under consideration will be replaced by elements of some algebraic number field. For the sake of simplicity, we shall restrict the polynomial equations under consideration to have coefficients lying in $\mathbb{Z}$, though it is straightforward to relax this condition so that the coefficient ring $\mathbb{Z}$ is replaced by the ring of integers from some other number field.

Definition 4.1. *Let $\mathscr{A}$ and $\mathscr{B}$ be finite sets of algebraic numbers. Suppose that $P_1, \ldots, P_r \in \mathbb{Z}[x_1, \ldots, x_s]$. We say that a bijection $\psi : \mathscr{A} \to \mathscr{B}$ is an algebraic Freiman* **P***-isomorphism if, whenever $(x_1 \ldots, x_s) \in \mathscr{A}^s$, then*

$$P_i(x_1, \ldots, x_s) = 0 \quad (1 \leqslant i \leqslant r)$$

if and only if

$$P_i(\psi(x_1), \ldots, \psi(x_s)) = 0 \quad (1 \leqslant i \leqslant r).$$

Notice here that we have not insisted that $\mathscr{A}$ and $\mathscr{B}$ lie in the same number field. Thus, for example, it is possible that one has $\mathscr{A} \subset \mathbb{Z}[\sqrt{-1}]$ and $\mathscr{B} \subset \mathbb{Z}[\sqrt[3]{2}]$. Given this flexibility in the choice of the image set, an appropriate definition of the analogue of a **P**-condenser takes some care. First, when $\mathscr{C} = \{c_1, \ldots, c_n\}$ is a finite set of algebraic numbers, we define the number field $K = \mathbb{Q}(\mathscr{C})$ by putting $K = \mathbb{Q}(c_1, \ldots, c_n)$. We then put

$$d(\mathscr{C}) = [K : \mathbb{Q}] \quad \text{and} \quad D(\mathscr{C}) = \mathrm{Disc}(K : \mathbb{Q}).$$

Rather than become entangled with a coordinate basis for K over $\mathbb{Q}$, we instead work with minimal polynomials associated with each element $c \in \mathscr{C}$. Here, by the minimal polynomial $m_c \in \mathbb{Z}[x]$ of $c \in \mathscr{C}$, we mean the irreducible polynomial in $\mathbb{Z}[x]$ with content 1 and positive leading coefficient satisfying the condition that $m_c(c) = 0$. Note that if m_c has leading coefficient l, then $l^{-1} m_c$ is the conventional minimal polynomial of c over $\mathbb{Q}$. Given a polynomial $f \in \mathbb{Z}[x]$ with $f(x) = f_0 + f_1 x + \ldots + f_d x^d$, we define

$$\|f\|_q = (|f_0|^q + |f_1|^q + \ldots + |f_d|^q)^{1/q} \quad (q = 1, 2).$$

Then, as a measure of the enveloping radius of the set $\mathscr{C}$, we work with the *algebraic enveloping radius*

$$\mathrm{Env}(\mathscr{C}) = \max\{\|m_c\|_1 : c \in \mathscr{C}\}.$$

If $\mathscr{C}$ is a set of rational integers, then it is apparent that $\mathrm{Env}(\mathscr{C}) = \mathrm{env}(\mathscr{C})$. Notice that $\mathrm{Env}(\mathscr{C})$ is independent of any particular coordinate basis for $\mathbb{Q}(\mathscr{C})$.

Our goal is now to map a set of algebraic numbers $\mathscr{A}$, having a large algebraic enveloping radius $\mathrm{Env}(\mathscr{A})$, to a new set $\mathscr{B}$ having smaller algebraic enveloping radius $\mathrm{Env}(\mathscr{B})$, via an algebraic Freiman **P**-isomorphism $\psi : \mathscr{A} \to \mathscr{B}$. In this way, the size of the elements of $\mathscr{B}$ is morally speaking smaller than the corresponding size of the elements of $\mathscr{A}$, and yet

$\mathscr{B}$ preserves the salient features of the solubility of the system $\mathbf{P}(\mathbf{x})=\mathbf{0}$ exhibited by $\mathscr{A}$. This objective motivates the following analogues of Definitions 2.2 and 2.3.

Definition 4.2. *We say that a mapping $\psi:\mathscr{A}\rightarrow\mathscr{C}$ is a d-algebraic $\mathbf{P}$-condenser of $\mathscr{A}$ if it is an algebraic Freiman $\mathbf{P}$-isomorphism having the property that*

$$Env(\mathscr{C})\leqslant Env(\mathscr{A})\quad\text{and}\quad d(\mathscr{C})=d.$$

When the inequality here is strict, we refer to ψ as a strict d-algebraic $\mathbf{P}$-condenser of $\mathscr{A}$. In either case, we refer to $\mathscr{C}$ as being a d-algebraic condensation of $\mathscr{A}$.

Definition 4.3. *Let $\mathscr{A}$ be a finite set of algebraic numbers, and denote by $\Psi_{\mathbf{P}}(\delta)$ the set of all d-algebraic $\mathbf{P}$-condensers of $\mathscr{A}$ with $d\leqslant\delta$. Then the δ-limited $\mathbf{P}$-essential enveloping radius of a finite set $\mathscr{A}$ of algebraic integers is*

$$Env_\delta^*(\mathscr{A};\mathbf{P})=\min\{Env(\psi(\mathscr{A})):\psi\in\Psi_{\mathbf{P}}(\delta)\}.$$

We are now equipped to describe, in broad and rough terms, our strategy for condensing algebraic sets $\mathscr{A}$ into sets $\mathscr{C}$ establishing that $\mathrm{Env}_\delta^*(\mathscr{A};\mathbf{P})$ is bounded purely in terms of $|\mathscr{A}|$ and $\mathbf{P}$, while at the same time maintaining δ to be likewise bounded purely in terms of $|\mathscr{A}|$ and $\mathbf{P}$. The details of this process will be the subject of the next section.

Let $\mathscr{A}$ be a finite set of algebraic integers with $\mathrm{card}(\mathscr{A})=A$. In fact we shall need to consider finite sets of algebraic numbers, and this generates additional complications relative to the situation where the algebraic numbers are in fact algebraic integers. However, this simplified case allows us to sketch out the necessary argument. Put $X=\mathrm{Env}(\mathscr{A})$ and suppose that $d(\mathscr{A})=d_0$, with d_0 bounded above by some absolute constant.

Our first step is to seek a rational prime number π having the property that $\pi\nmid(a_1-a_2)$ for any distinct elements $a_1,a_2\in\mathscr{A}$, and also $\pi\nmid P_i(\mathbf{a})$ for any $\mathbf{a}\in\mathscr{A}^s$ with $P_i(\mathbf{a})\neq 0$ $(1\leqslant i\leqslant r)$. For the sake of concreteness, we shall in fact interpret these divisibility relations by taking norms of the algebraic numbers in question. It is apparent that an argument similar to that applied in §3 will deliver such a prime to us with $\pi\ll_{A,\mathbf{P}}\log X$. Unfortunately, we must ensure that this prime number behaves congenially with respect to the number field $K_0=\mathbb{Q}(\mathscr{A})$, because we intend subsequently to consider the set $\mathscr{A}$ modulo π to be a subset of the finite field $\mathbb{F}_\pi$, and thence consider the associated system of congruences

$$P_i(\mathbf{a})\equiv 0\ (\mathrm{mod}\ \pi)\quad(1\leqslant i\leqslant r).$$

We therefore seek an appropriately sized prime π having the property that a certain minimal polynomial associated with $\mathscr{A}$ splits into linear factors over $\mathbb{F}_\pi$. If we assume a certain Generalised Riemann Hypothesis, then it follows from an appropriate version of the Chebotarev density theorem that such a prime can be shown to exist with $\pi \ll_{A,\mathbf{P}} (\log X)^3$.

Having obtained a prime π with the properties just described, our second step is to apply the argument of Grosu [7] to rectify the set $\mathscr{A} \pmod{\pi}$. Provided that π is chosen large enough in terms of A and $\mathbf{P}$, this argument shows that the set $\mathscr{A} \pmod{\pi}$ can be mapped to a new set $\mathscr{B}$ algebraic Freiman $\mathbf{P}$-isomorphic to $\mathscr{A}$, and having the property that

$$\mathrm{Env}(\mathscr{B}) \ll_{A,\mathbf{P}} (\log X)^{c(A,\mathbf{P})} \quad \text{and} \quad d(\mathscr{B}) \ll_{A,\mathbf{P}} 1.$$

Here, the positive number $c(A,\mathbf{P})$ depends at most on A and $\mathbf{P}$. Notice here that, whilst the set $\mathscr{A}$ has elements of size roughly X, the elements of $\mathscr{B}$ have size roughly a power of $\log X$. This reduction in size is crucial to our condensation argument.

By iterating these two steps sufficiently many times, much as was done in §3 in the simpler linear case in the proofs of Theorems 3.1 and 3.2, we ultimately obtain a set $\mathscr{C}$ algebraically Freiman $\mathbf{P}$-isomorphic to $\mathscr{A}$, and satisfying the property that

$$\mathrm{Env}(\mathscr{C}) \ll_{A,\mathbf{P}} 1 \quad \text{and} \quad d(\mathscr{B}) \ll_{A,\mathbf{P}} 1.$$

All that remains is to take care in controlling the behaviour in these results of the implicit constants depending on A and $\mathbf{P}$.

We describe the details of the argument just outlined in the next section. For now, it suffices to say that in the setting countenanced in the above discussion, we are able to show that, subject to the validity of the Generalised Riemann Hypothesis for all Dedekind zeta functions, there is a set of algebraic numbers $\mathscr{C}$ algebraic Freiman $\mathbf{P}$-isomorphic to $\mathscr{A}$ with

$$d(\mathscr{C}) \leqslant \exp_2(\kappa_1 A) \quad \text{and} \quad \mathrm{Env}(\mathscr{C}) \leqslant \exp_4(\kappa_2 A),$$

where κ_1 and κ_2 are positive numbers depending at most on $\mathbf{P}$.

5 Condensations for non-linear systems of equations, II

Let us now put the plan of the previous section into action. It is worth stressing that our bounds will be extraordinarily weak. In consequence, it makes sense to avoid stress on detailed bounds, but instead opt for estimates somewhat weaker than might be achieved with greater attention to detail, but ones nonetheless simple to state in suitable notation.

Let s and r be natural numbers with $s \geqslant 2$, and for $1 \leqslant i \leqslant r$ consider fixed polynomials $P_i = P_i(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ of respective degrees t_i. We write $\|P_i\|_1$ for the sum of the absolute values of the coefficients of P_i, and we suppose that $t_i \leqslant t$ and $\|P_i\|_1 \leqslant k$ for $1 \leqslant i \leqslant r$. Then, in the sense of Grosu [7], the polynomial system $\mathbf{P}$ is (k,t)-bounded. Note that, in view of our work in §3, there is no loss of generality in supposing that $t \geqslant 2$. Our initial discussion will be focused on establishing the iterative step described in the previous section. Suppose then that $\mathscr{A}$ is a set of algebraic numbers with $\mathrm{card}(\mathscr{A}) = A \geqslant 2$. Our discussion will be simplified by introducing the function

$$\nu(n) = (2t)^{(2t)^{2^n}}. \tag{5.1}$$

To avoid any potential ambiguity, we note that this is a 3-fold iterated exponential function of n. Equipped with this notation, it is convenient to suppose that

$$d(\mathscr{A}) \leqslant (2t)^{2^A} \quad \text{and} \quad \mathrm{Env}(\mathscr{A}) = X. \tag{5.2}$$

In most familiar applications of algebraic number theory, analytic number theorists are used to working with a fixed number field K wherein the degree and discriminant are well-controlled. Unfortunately for us, we require discussions of field extensions of $\mathbb{Q}$ with enormous degree and discriminant, and so we are forced to pay attention to details that in normal circumstances would not delay our argument. Our initial focus lies on the non-zero algebraic number

$$\Upsilon(\mathscr{A}) = \Biggl(\prod_{\substack{a_1, a_2 \in \mathscr{A} \\ a_1 \neq a_2}} (a_1 - a_2) \Biggr) \Biggl(\prod_{i=1}^{r} \prod_{\substack{\mathbf{a} \in \mathscr{A}^s \\ P_i(\mathbf{a}) \neq 0}} P_i(\mathbf{a}) \Biggr). \tag{5.3}$$

We seek a rational prime number π with properties associated to $\Upsilon(\mathscr{A})$ outlined in the discussion of the previous section. In preparation for our application of the Chebotarev density theorem, we discuss the Galois closure K^c of $K = \mathbb{Q}(\mathscr{A})$, and some of its properties.

Lemma 5.1. *One has* $[K^c : \mathbb{Q}] \leqslant \nu(A+1)$.

Proof. By the primitive element theorem, there is some algebraic number $\theta \in K$ for which $K = \mathbb{Q}(\theta)$. The minimal polynomial m_θ of θ over $\mathbb{Z}$ has degree $[K:\mathbb{Q}] = d(\mathscr{A}) \leqslant (2t)^{2^A}$. Thus, the splitting field of m_θ, which contains K^c, has degree at most $d(\mathscr{A})!$. We therefore conclude that

$$[K^c:\mathbb{Q}] \leqslant d(\mathscr{A})^{d(\mathscr{A})} \leqslant (2t)^B,$$

where

$$B = 2^A(2t)^{2^A} \leqslant (2t)^{A+2^A} \leqslant (2t)^{2^{A+1}}.$$

Thus, on recalling the notation (5.1), we find that $[K^c:\mathbb{Q}] \leqslant \nu(A+1)$, and the proof of the lemma is complete.

Lemma 5.2. *One has* $\mathrm{Disc}(K^c:\mathbb{Q}) \leqslant (2tX)^{\nu(A+4)}$.

Proof. We begin by considering a typical element $a \in \mathscr{A}$. Suppose that $[\mathbb{Q}(a):\mathbb{Q}] = d$, whence the minimal polynomial m_a of a over $\mathbb{Z}$ has degree d. We note for future reference that $d \leqslant [K:\mathbb{Q}] = d(\mathscr{A})$. Let $S(a)$ denote the splitting field for m_a over $\mathbb{Q}$, so that $S(a) = \mathbb{Q}(\beta_1,\dots,\beta_d)$ for some distinct algebraic numbers $\beta_1,\dots,\beta_d$. We put $S_0(a) = \mathbb{Q}$, and when $1 \leqslant j \leqslant d$ we define

$$S_j(a) = \mathbb{Q}(\beta_1,\dots,\beta_j).$$

For each index j with $1 \leqslant j \leqslant d$, we have

$$\mathrm{Disc}(\mathbb{Q}(\beta_j):\mathbb{Q}) \leqslant \mathrm{Disc}(m_{\beta_j}) = \mathrm{Disc}(m_a). \tag{5.4}$$

Recall the upper bounds (5.2). Then, by considering the resultant of m_a and m_a' in terms of the determinant of the associated Sylvester matrix, noting that the coefficients of m_a are bounded in absolute value by $\mathrm{Env}(\mathscr{A})$, we see that

$$\begin{aligned}\mathrm{Disc}(m_a) &\leqslant (\deg(m_a))!\,(\mathrm{Env}(\mathscr{A}))^{2\deg(m_a)}\\ &\leqslant d(\mathscr{A})^{d(\mathscr{A})}X^{2d(\mathscr{A})}\\ &\leqslant \nu(A+1)X^{2(2t)^{2^A}}.\end{aligned} \tag{5.5}$$

Now observe that, as a consequence of a simple bound of Tôyoma [15], whenever $E:\mathbb{Q}$ and $F:\mathbb{Q}$ are two field extensions, then

$$\mathrm{Disc}(EF:\mathbb{Q}) \leqslant (\mathrm{Disc}(E:\mathbb{Q})\,\mathrm{Disc}(F:\mathbb{Q}))^{[EF:\mathbb{Q}]}. \tag{5.6}$$

Thus, for $1 \leqslant j < d$, it follows from (5.4) that

$$\begin{aligned}\mathrm{Disc}(S_{j+1}(a):\mathbb{Q}) &\leqslant (\mathrm{Disc}(S_j(a):\mathbb{Q})\,\mathrm{Disc}(\mathbb{Q}(\beta_{j+1}):\mathbb{Q}))^{[K^c:\mathbb{Q}]}\\ &\leqslant (\mathrm{Disc}(S_j(a):\mathbb{Q})\,\mathrm{Disc}(m_a))^{[K^c:\mathbb{Q}]}.\end{aligned} \tag{5.7}$$

Since it also follows from (5.4) that $\mathrm{Disc}(S_1(a):\mathbb{Q})\leqslant \mathrm{Disc}(m_a)$, we may apply the relation (5.7) inductively to derive the relation

$$\mathrm{Disc}(S_d(a):\mathbb{Q})\leqslant (\mathrm{Disc}(m_a))^{d[K^c:\mathbb{Q}]^{d-1}}. \tag{5.8}$$

We therefore deduce from (5.5) and Lemma 5.1 that

$$\mathrm{Disc}(S(a):\mathbb{Q})\leqslant \left(\nu(A+1)X^{2(2t)^{2^A}}\right)^{\nu(A+1)^{d(\mathscr{A})}}.$$

A modicum of computation confirms that

$$\nu(A+1)^{d(\mathscr{A})}\leqslant (2t)^{(2t)^{2^{A+1}}(2t)^{2^A}}\leqslant \nu(A+2),$$

whilst

$$\nu(A+1)^{\nu(A+2)}\leqslant (2t)^{\nu(A+3)}\quad \text{and}\quad 2(2t)^{2^A}\nu(A+2)\leqslant \nu(A+3).$$

Consequently, we arrive at the simplified upper bound

$$\mathrm{Disc}(S(a):\mathbb{Q})\leqslant (2tX)^{\nu(A+3)}. \tag{5.9}$$

At this point, we have bounded the discriminant associated to only one element of $\mathscr{A}$. The Galois closure K^c of $\mathbb{Q}(\mathscr{A})$, however, is the compositum of all the splitting fields $S(a)$ for $a\in\mathscr{A}$. We therefore apply the relation (5.6) as in the deduction of (5.8) to establish the bound

$$\mathrm{Disc}(K^c:\mathbb{Q})\leqslant \left(\max_{a\in\mathscr{A}}\mathrm{Disc}(S(a):\mathbb{Q})\right)^{A[K^c:\mathbb{Q}]^{A-1}}.$$

By Lemma 5.1, one has

$$A[K^c:\mathbb{Q}]^{A-1}\leqslant \nu(A+1)^A,$$

so the upper bound (5.9) yields the estimate

$$\mathrm{Disc}(K^c:\mathbb{Q})\leqslant (2tX)^B,$$

where

$$B=\nu(A+3)\nu(A+1)^A=(2t)^{A(2t)^{2^{A+1}}+(2t)^{2^{A+3}}}\leqslant (2t)^{(2t)^{2^{A+4}}}=\nu(A+4).$$

Thus we conclude that $\mathrm{Disc}(K^c:\mathbb{Q})\leqslant (2tX)^{\nu(A+4)}$, completing the proof.

We shall need to identify a rational prime number π having the property that the algebraic number $\Upsilon(\mathscr{A})$ is a unit modulo π. Let $\Upsilon_0(\mathscr{A})$ denote the least positive (rational) integer having the property that the algebraic number

$$\Upsilon_1(\mathscr{A}) = \Upsilon_0(\mathscr{A})\Upsilon(\mathscr{A})$$

is an algebraic integer. Then, by taking norms, it is evident that it suffices to arrange that π does not divide the rational integer

$$\Upsilon^*(\mathscr{A}) = |N_{K^c:\mathbb{Q}}(\Upsilon_0(\mathscr{A}))N_{K^c:\mathbb{Q}}(\Upsilon_1(\mathscr{A}))|.$$

Lemma 5.3. *One has* $1 \leqslant \Upsilon^*(\mathscr{A}) \leqslant (2kX)^{r(2A)^s\nu(A+2)}$.

Proof. We begin by taking a crude approach to bounding $|N_{K^c:\mathbb{Q}}(\Upsilon(\mathscr{A}))|$, applying bounds for the complex absolute values of the conjugates of each element of $\mathscr{A}$. Let a be a typical element of $\mathscr{A}$. Since $\mathrm{Env}(\mathscr{A}) = X$, the minimal polynomial m_a of a over $\mathbb{Z}$ satisfies the relation $\|m_a\|_1 \leqslant X$. Also, since $\deg(m_a) \leqslant d(\mathscr{A})$, we find that m_a takes the form

$$b_0(a)x^d + \ldots + b_{d-1}(a)x + b_d(a), \tag{5.10}$$

in which $d \leqslant d(\mathscr{A})$ and $|b_0(a)| \geqslant 1$. The (complex) absolute value of a therefore satisfies either the upper bound $|a| \leqslant 1$, or else is constrained by the inequality

$$|b_0(a)a^d| \leqslant |a|^{d-1}\|m_a\|_1 \leqslant |a|^{d-1}\mathrm{Env}(\mathscr{A}) = |a|^{d-1}X,$$

whence $|a| \leqslant X$. Thus, in any case, one has $|a| \leqslant X$. Since the conjugates of a are also roots of the polynomial m_a, one sees in this way that every conjugate of a in K^c has absolute value bounded above by X.

Recall the formula (5.3). It follows from our discussion thus far that the element $\Upsilon(\mathscr{A})$ of K^c satisfies the bound

$$|\Upsilon(\mathscr{A})| \leqslant (2X)^{A^2}(kX^t)^{rA^s}.$$

Here, we have made use of the observation that, since each polynomial $P_i(\mathbf{x})$ is (k,t)-bounded for $1 \leqslant i \leqslant r$, then for $\mathbf{a} \in \mathscr{A}^s$ one has

$$|P_i(\mathbf{a})| \leqslant \|P_i\|_1 \Big(\max_{1\leqslant i\leqslant s} |a_i|\Big)^{t_i} \leqslant kX^t.$$

In order to bound the norm of $\Upsilon(\mathscr{A})$, we must multiply all of the conjugates of $\Upsilon(\mathscr{A})$ together. However, since we assume that $s \geqslant 2$, the concluding remark of the preceding paragraph shows that each of these conjugates is bounded above by

$$(2X)^{A^2}(kX^t)^{rA^s} \leqslant (2kX)^{2rtA^s}.$$

Thus, multiplying all of these conjugates together, we find that

$$|N_{K^c:\mathbb{Q}}(\Upsilon(\mathscr{A}))| \leqslant \left((2kX)^{2rtA^s}\right)^{[K^c:\mathbb{Q}]}. \tag{5.11}$$

Next, we investigate the denominator $\Upsilon_0(\mathscr{A})$. Referring to the minimal polynomial (5.10) of a over $\mathbb{Z}$, we see that $b_0(a)a$ is an algebraic integer and $|b_0(a)| \leqslant X$. An inspection of (5.3) therefore shows that $\Upsilon_0(\mathscr{A})$ is a positive rational integer dividing

$$\left(\prod_{a_1,a_2\in\mathscr{A}} b_0(a_1)b_0(a_2)\right)\left(\prod_{i=1}^{r}\prod_{\mathbf{a}\in\mathscr{A}^s} b_0(a_1)^t\cdots b_0(a_s)^t\right).$$

Thus, we have

$$\Upsilon_0(\mathscr{A}) \leqslant X^{2A^2+rstA^s},$$

whence

$$|N_{K^c:\mathbb{Q}}(\Upsilon_0(\mathscr{A}))| \leqslant \left(X^{(s+2)rtA^s}\right)^{[K^c:\mathbb{Q}]}.$$

By combining this estimate together with (5.11), we therefore discern that

$$\begin{aligned}\Upsilon^*(\mathscr{A}) &= |N_{K^c:\mathbb{Q}}(\Upsilon_0(\mathscr{A}))^2 N_{K^c:\mathbb{Q}}(\Upsilon(\mathscr{A}))|\\ &\leqslant \left((2kX)^{(2s+6)rtA^s}\right)^{[K^c:\mathbb{Q}]}.\end{aligned} \tag{5.12}$$

Finally, we simplify the estimate supplied by (5.12). Observe first that, since $s \geqslant 2$, we have $2s+6 \leqslant 2^{s+2}$. Thus, on applying Lemma 5.1, we infer that

$$\Upsilon^*(\mathscr{A}) \leqslant (2kX)^{4rt(2A)^s\nu(A+1)}.$$

However, one has $4t\nu(A+1) \leqslant \nu(A+2)$. We consequently conclude that

$$\Upsilon^*(\mathscr{A}) \leqslant (2kX)^{r(2A)^s\nu(A+2)}.$$

On noting that $\Upsilon^*(\mathscr{A})$ is non-zero, by construction, the proof of the lemma is complete.

It is now time to select the rational prime number π by applying the Chebotarev density theorem. By the primitive element theorem, there exists an element $\Theta \in K^c$ having the property that $K^c = \mathbb{Q}(\Theta)$. It is apparent, moreover, that by making an appropriate choice for Θ, we may assume not only that $\mathscr{A} \subset \mathbb{Z}[\Theta]$, but also that all of the conjugates of the elements of $\mathscr{A}$ within K^c lie in $\mathbb{Z}[\Theta]$. With this choice for Θ now fixed in such a manner, we seek a rational prime number π with $\pi \nmid \Upsilon^*(\mathscr{A})$ having the property that the minimal polynomial m_Θ of Θ over $\mathbb{Z}$ splits into linear factors modulo π. This allows us to bijectively map the set $\mathscr{A}$ into a set of residues modulo π, while preserving the salient features of the solution set associated with the system of polynomial equations $\mathbf{P} = \mathbf{0}$. Throughout, we abbreviate Generalised Riemann Hypothesis to GRH.

Lemma 5.4. *There is an effectively computable positive absolute constant M_1 with the following property. Suppose that GRH holds for the Dedekind zeta function associated with the field extension $K^c : \mathbb{Q}$. In addition, assume that*

$$Y \geqslant r(2A)^s(2t)^{\nu(A+3)}\log(2kX) \tag{5.13}$$

and

$$Y \geqslant M_1(2t)^{2\nu(A+4)}(\log(2tX))^4. \tag{5.14}$$

Then there exists a rational prime number π, with $Y < \pi \leqslant 16Y$ and $\pi \nmid \Upsilon^*(\mathscr{A})$, having the property that the minimal polynomial m_Θ of Θ over $\mathbb{Z}$ splits into linear factors over $\mathbb{F}_\pi[t]$.

Proof. We work under the hypotheses (5.13) and (5.14) throughout. An effective version of the Chebotarev density theorem is provided by Lagarias and Odlyzko under the assumption of GRH for the Dedekind zeta function associated with the field extension $K^c : \mathbb{Q}$. Denote by $\pi_\Theta(x)$ the number of rational prime numbers p with $p \leqslant x$ having the property that m_Θ splits into linear factors over $\mathbb{F}_p$. Put

$$G = \mathrm{Gal}(K^c : \mathbb{Q}), \quad n = [K^c : \mathbb{Q}] \quad \text{and} \quad D = \mathrm{Disc}(K^c : \mathbb{Q}).$$

Then it follows from [11, Theorem 1.1] that there exists a positive absolute constant M_0 such that

$$\left|\pi_\Theta(x) - \frac{\mathrm{Li}(x)}{|G|}\right| \leqslant M_0\left(\frac{x^{1/2}\log(Dx^n)}{|G|} + \log D\right). \tag{5.15}$$

Here, we have written $\mathrm{Li}(x)$ for the usual logarithmic integral function.

On recalling Lemmata 5.1 and 5.2, we find that when $x \leqslant X$, we have

$$\begin{aligned}\log(Dx^n) &\leqslant \nu(A+4)\log(2tX) + \nu(A+1)\log x\\ &\leqslant 2\nu(A+4)\log(2tX).\end{aligned}$$

Moreover, it follows from a trivial upper bound for $|G|$ together with Lemma 5.1 that

$$|G| \leqslant [K^c:\mathbb{Q}]! \leqslant [K^c:\mathbb{Q}]^{[K^c:\mathbb{Q}]} \leqslant \nu(A+1)^{\nu(A+1)} \leqslant (2t)^{\nu(A+2)}, \tag{5.16}$$

whence

$$\begin{aligned}|G|\log D &\leqslant (2t)^{\nu(A+2)}\nu(A+4)\log(2tX)\\ &\leqslant (2t)^{\nu(A+3)}\log(2tX).\end{aligned}$$

Thus, we deduce from (5.15) that

$$\left|\pi_\Theta(x) - \frac{\mathrm{Li}(x)}{|G|}\right| \leqslant \frac{M_0}{|G|}\left(2x^{1/2}\nu(A+4)\log(2tX) + (2t)^{\nu(A+3)}\log(2tX)\right).$$

Suppose that M_1 is sufficiently large in terms of M_0. Then, under the hypothesis (5.14), we have

$$\begin{aligned}\pi_\Theta(16Y) &\geqslant \frac{1}{|G|}\Bigl(\frac{16Y}{\log(16Y)} - \bigl(8Y^{1/2}\nu(A+4) + (2t)^{\nu(A+3)}\bigr)M_0\log(2tX)\Bigr)\\ &\geqslant \frac{1}{|G|}\Bigl(\frac{16Y}{\log(16Y)} - \frac{4Y}{\log Y}\Bigr) \geqslant \frac{8Y}{|G|\log Y}.\end{aligned}$$

Meanwhile, in a similar manner one finds that

$$\begin{aligned}\pi_\Theta(Y) &\leqslant \frac{1}{|G|}\Bigl(\frac{2Y}{\log Y} + \bigl(2Y^{1/2}\nu(A+4) + (2t)^{\nu(A+3)}\bigr)M_0\log(2tX)\Bigr)\\ &\leqslant \frac{1}{|G|}\Bigl(\frac{2Y}{\log Y} + \frac{2Y}{\log Y}\Bigr) = \frac{4Y}{|G|\log Y}.\end{aligned}$$

Thus, we discern that

$$\pi_\Theta(16Y) - \pi_\Theta(Y) \geqslant \frac{4Y}{|G|\log Y}.$$

Let $\varPi$ denote the set of rational prime numbers p with $Y < p \leqslant 16Y$ for which m_Θ splits into linear factors over $\mathbb{F}_p$. Then

$$\prod_{p\in\varPi} p \geqslant Y^{4Y/(|G|\log Y)} = \exp\left(4Y/|G|\right).$$

Meanwhile, from Lemma 5.3 we find that

$$\log \varUpsilon^*(\mathscr{A}) \leqslant r(2A)^s \nu(A+2)\log(2kX).$$

Thus, recalling the upper bound (5.16) for $|G|$, we have

$$\prod_{p\in \varPi} p > \varUpsilon^*(\mathscr{A})$$

provided only that

$$\frac{4Y}{(2t)^{\nu(A+2)}} > r(2A)^s \nu(A+2)\log(2kX). \tag{5.17}$$

But $\nu(A+2)(2t)^{\nu(A+2)} \leqslant (2t)^{\nu(A+3)}$, and so the hypothesis (5.13) is sufficient to ensure the validity of (5.17). With this condition now satisfied, we conclude that there exists a rational prime number π with $Y < \pi \leqslant 16Y$ satisfying $\pi \nmid \varUpsilon^*(\mathscr{A})$, and such that $m_\varTheta$ splits into linear factors over $\mathbb{F}_\pi$. The conclusion of the lemma follows.

We are now in a position to move on to the second step in the inductive phase of the argument, applying the method of Grosu [7]. The conclusion of Lemma 5.4 shows that there is a rational prime number π with

$$\pi \leqslant 16M_1 r(2A)^s (2t)^{2\nu(A+4)}(\log(2tkX))^4$$

having the property that $\pi \nmid \varUpsilon^*(\mathscr{A})$, and such that $m_\varTheta$ splits into linear factors over $\mathbb{F}_\pi$. Let a_0 be any zero of the polynomial $m_\varTheta$ in $\mathbb{F}_\pi$. Since $\mathscr{A} \subset \mathbb{Z}[\varTheta]$, the ring homomorphism $\varPhi : \mathbb{Z}[\varTheta] \to \mathbb{F}_\pi$ defined by putting $\varPhi(\varTheta) = a_0$ restricts to a well-defined map $\varphi : \mathbb{Z}[\mathscr{A}] \to \mathbb{F}_\pi$.

We claim that the set $\mathscr{A}$ has image $\mathscr{B} = \varphi(\mathscr{A})$ in which, for pairs of elements $a_1, a_2 \in \mathscr{A}$, one has $\varphi(a_1) = \varphi(a_2)$ if and only if $a_1 = a_2$. This claim will be confirmed by verifying that whenever $a_1 \neq a_2$, then $\varphi(a_1) \neq \varphi(a_2)$. By way of seeking a contradiction, suppose that $a_1 \neq a_2$ and $\varphi(a_1) = \varphi(a_2)$. Then we have $\varPhi(a_1) = \varPhi(a_2)$, and the homomorphism property of $\varPhi$ implies that $\varPhi(a_1 - a_2) = 0$. But $\varUpsilon^*$ is a multiple of $a_1 - a_2$, say $\varUpsilon^* = \mu(a_1 - a_2)$ for a suitable element μ of $\mathbb{Z}[\varTheta]$. The homomorphism property of $\varPhi$ thus ensures that $\varPhi(\varUpsilon^*) = \varPhi(\mu)\varPhi(a_1 - a_2) = 0$. However, we have $\varUpsilon^* \in \mathbb{Z}$, and since $\pi \nmid \varUpsilon^*$ we find that $0 = \varPhi(\varUpsilon^*) = \varUpsilon^*\varPhi(1)$ and hence $\varPhi(1) = 0$. This contradicts the homomorphism property of $\varPhi$, confirming our earlier claim.

We also claim that, for $1 \leqslant i \leqslant r$ and $\mathbf{a} \in \mathscr{A}^s$, one has $P_i(\mathbf{a}) = 0$ if and only if $P_i(\varphi(\mathbf{a})) = 0$. In this instance it suffices to show that when $P_i(\mathbf{a}) \neq 0$, then $P_i(\varphi(\mathbf{a})) \neq 0$. We again proceed by seeking a contradiction, assuming that $P_i(\mathbf{a}) \neq 0$ and $P_i(\varphi(\mathbf{a})) = 0$. Then the homomorphism property of Φ ensures that $\Phi(P_i(\mathbf{a})) = 0$. But Υ^* is a multiple of $P_i(\mathbf{a})$, say $\Upsilon^* = \mu' P_i(\mathbf{a})$ for a suitable element μ' of $\mathbb{Z}[\Theta]$. Thus, in a similar manner to that described in the previous paragraph, we find that $\Phi(\Upsilon^*) = \Phi(\mu')\Phi(P_i(\mathbf{a})) = 0$, contradicting the fact that $\pi \nmid \Upsilon^*$. This contradiction again confirms our claim.

Lemma 5.5. *Suppose that π is a prime number having the property that $\pi \nmid \Upsilon^*(\mathscr{A})$, and such that m_Θ splits into linear factors over $\mathbb{F}_\pi$. Suppose also that*

$$\pi > (2kt)^{(2t)^{2^{A+1}}}. \tag{5.18}$$

Then there exists an algebraic extension L of $\mathbb{Q}$ of degree at most $(2t)^{2^A}$, and a subset $\mathscr{C} \subset L$ with $\operatorname{card}(\mathscr{C}) = A$, having the following properties:

(a) there is an injective map $\omega : \mathscr{C} \to \mathbb{F}_\pi$, with $\omega(\mathscr{C}) = \varphi(\mathscr{A})$, having the property that the canonical induced map $\widetilde{\omega} : \mathbb{Z}[\mathscr{C}] \to \mathbb{F}_\pi$ is a ring homomorphism;

(b) given $\mathbf{a} \in \mathscr{A}^s$, define $c_i = \omega^{-1}(\varphi(a_i))$ $(1 \leqslant i \leqslant s)$. Then one has $P_i(\mathbf{c}) = 0$ $(1 \leqslant i \leqslant r)$ for $\mathbf{c} \in \mathscr{C}^s$ if and only if $P_i(\varphi(\mathbf{a})) = 0$ for $\mathbf{a} \in \mathscr{A}^s$;

(c) one has $\operatorname{Env}(\mathscr{C}) \leqslant \nu(A+1)\pi$.

In order to avoid ambiguity, we stress that the map $\widetilde{\omega}$ is defined for $f(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_m]$ by taking

$$\widetilde{\omega}\,(f(c_1, \dots, c_m)) = f(\omega(c_1), \dots, \omega(c_m)).$$

Proof (of Lemma 5.5). The desired conclusion is a consequence of the argument of Grosu [7, Lemma 8.1], though care is required in interpreting the argument underlying the latter proof so as to obtain the desired outcome. Following the general strategy of Grosu, we assign distinct indeterminates x_a to each element $\varphi(a)$ of $\mathscr{B} = \varphi(\mathscr{A})$. Certain equations are then known to have solutions over $\mathbb{F}_\pi$, specifically

$$P_i(x_{a_1}, \dots, x_{a_s}) = 0 \quad (1 \leqslant i \leqslant r) \tag{5.19}$$

has a solution $(x_{a_1}, \dots, x_{a_s}) = (\varphi(a_1), \dots, \varphi(a_s))$ whenever

$$P_i(a_1, \dots, a_s) = 0 \quad (1 \leqslant i \leqslant r)$$

for $\mathbf{a} \in \mathscr{A}^s$. In addition, one has certain non-equations. First, of course, one has

$$x_{a_1} - x_{a_2} \neq 0$$

whenever $x_{a_1} = \varphi(a_1)$ and $x_{a_2} = \varphi(a_2)$ for $a_1 \neq a_2$ with $a_1, a_2 \in \mathscr{A}$. Moreover, we have

$$P_i(x_{a_1}, \ldots, x_{a_s}) \neq 0$$

whenever $x_{a_j} = \varphi(a_j)$ $(1 \leqslant j \leqslant s)$ for $(a_1, \ldots, a_s) \in \mathscr{A}^s$ satisfying $P_i(a_1, \ldots, a_s) \neq 0$. Taken together, we now have a list of equations and non-equations in the variables x_a $(a \in \mathscr{A})$, all defined over $\mathbb{F}_\pi$, and with the defining equations all (k,t)-bounded. It is worth emphasising, for the uninitiated, that the number of equations here may be very large. When $r = 1$, for example, the number of equations may be as large, roughly speaking, as A^{s-1}.

The argument of the proof of Grosu [7, Lemma 8.1] now shows via an elimination procedure using resultants that over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, the equations (5.19) possess a solution if and only if certain eliminant polynomials are constant and equal to 0. By applying the same elimination procedure over $\mathbb{F}_\pi$, however, one sees that these constant polynomials must be 0 over $\mathbb{F}_\pi$, since the equations (5.19) possess the solution $x_a = \varphi(a)$ $(a \in \mathscr{A})$ in that setting. Provided that these eliminant polynomials have small enough coefficients in terms of π, therefore, one finds that in the setting of $\overline{\mathbb{Q}}$, these eliminant polynomials are indeed 0, and hence the system (5.19) possesses a solution, say $x_a = \psi(a)$ $(a \in \mathscr{A})$, lying in $\overline{\mathbb{Q}}$.

This is not the end of the story. It is shown first by Grosu [7, Lemma 8.1] that the field $L = \mathbb{Q}(\psi(\mathscr{A}))$ has degree at most $\tilde{t} = (2t)^{2^A}$ over $\mathbb{Q}$. Second, all of the eliminant polynomials to which we alluded above have coefficients bounded by

$$\tilde{k} = (2kt)^{(2t)^{2^{A+1}}},$$

and thus the condition (5.18) suffices for the desired conclusion. Indeed, Grosu shows that the eliminant polynomials are all $(\tilde{k}, \tilde{t})$-bounded. Third, the elements $\psi(a)$ $(a \in \mathscr{A})$ may be chosen in such a manner that there is a ring homomorphism $\gamma : \mathbb{Z}[\mathscr{C}] \to \mathbb{F}_\pi$ which sends $\psi(a)$ to $\varphi(a)$ for each $a \in \mathscr{A}$. A subtle detail of this last conclusion is that it may be necessary to take $\psi(a)$ to be a rational integer b lying in the set $\{0, 1, \ldots, \pi - 1\}$ with $b \equiv \varphi(a) \pmod{\pi}$ (see the fifth and sixth paragraphs of Step 2 of the proof of [7, Lemma 8.1]).

We are now in possession of sufficient detail to complete the proof of the lemma. We have already confirmed the claims made in the statement of the lemma concerning the existence of L, the subset $\mathscr{C}$, the degree of L over $\mathbb{Q}$, and we have also explained the hypothesis (5.18). We define

$\omega : \mathscr{C} \to \mathbb{F}_\pi$ by taking $\omega(c) = \gamma(c)$ for $c \in \mathscr{C}$, and then $\widetilde{\omega}$ coincides with γ by virtue of the ring homomorphism property of γ. Moreover, if $\omega(c_1) = \omega(c_2)$ for some elements c_1 and c_2 of $\mathscr{C}$, then $\gamma(c_1) = \gamma(c_2)$. When $c_i = \psi(a_i)$ $(i = 1, 2)$ with $a_1, a_2 \in \mathscr{A}$, then we have

$$\varphi(a_1) = \gamma(\psi(a_1)) = \gamma(c_1) = \gamma(c_2) = \gamma(\psi(a_2)) = \varphi(a_2).$$

Thus, from the properties of the mapping φ, we have $a_1 = a_2$. Hence

$$c_1 = \psi(a_1) = \psi(a_2) = c_2.$$

The mapping ω is consequently injective. This confirms the claim (a).

By construction, if $c_i = \psi(a_i)$ for $1 \leqslant i \leqslant s$ and $\mathbf{a} \in \mathscr{A}^s$, then

$$P_i(\mathbf{c}) = 0 \quad (1 \leqslant i \leqslant r)$$

if and only if

$$\widetilde{\omega}(P_i(\mathbf{c})) = 0 \quad (1 \leqslant i \leqslant r).$$

But

$$\widetilde{\omega}(P_i(\mathbf{c})) = P_i(\omega(c_1), \dots, \omega(c_s)) = P_i(\varphi(a_1), \dots, \varphi(a_s)) = 0 \quad (1 \leqslant i \leqslant r).$$

Thus $P_i(\mathbf{c}) = 0$ $(1 \leqslant i \leqslant r)$ for $\mathbf{c} \in \mathscr{C}^s$ if and only if $P_i(\varphi(\mathbf{a})) = 0$ $(1 \leqslant i \leqslant r)$. This confirms the claim (b).

Finally, each element $c \in \mathscr{C}$ is either an integer lying in the set $\{0, 1, \dots, \pi - 1\}$, or else satisfies a $(\tilde{k}, \tilde{t})$-bounded polynomial of degree at most $(2t)^{2^A}$ having integral coefficients of absolute value at most

$$(2kt)^{(2t)^{2^{A+1}}} \leqslant \pi.$$

In the latter case, the minimal polynomial m_c of c over $\mathbb{Z}$ is a divisor of a polynomial $q \in \mathbb{Z}[t]$, with $\|q\|_1 \leqslant \tilde{k} \leqslant \pi$ and $\deg(q) \leqslant (2t)^{2^A}$. If $\deg(q) = d$ and we write $q(x) = q_d x^d + \ldots + q_1 x + q_0$ with $q_i \in \mathbb{Z}$ $(0 \leqslant i \leqslant d)$, then we have

$$\sum_{l=0}^{d} |q_l|^2 \leqslant \Bigl(\sum_{l=0}^{d} |q_l| \Bigr)^2 = \|q\|_1^2.$$

It is then a consequence of the corollary to the main theorem of Granville [6] that if $r \in \mathbb{Z}[x]$ is any polynomial divisor of q, then

$$\|r\|_2 \leqslant \Bigl(\frac{\sqrt{5}+1}{2} \Bigr)^d \|q\|_2 \leqslant \Bigl(\frac{\sqrt{5}+1}{2} \Bigr)^d \|q\|_1 \leqslant \Bigl(\frac{\sqrt{5}+1}{2} \Bigr)^d \pi.$$

By Cauchy's inequality, therefore, we have

$$\|r\|_1 \leqslant (\deg(r)+1)^{1/2}\|r\|_2 \leqslant 2d\Big(\frac{\sqrt{5}+1}{2}\Big)^d \pi.$$

Hence, every element $c \in \mathscr{C}$ has minimal polynomial m_c over $\mathbb{Z}$ having degree at most $(2t)^{2^A}$, with

$$\|m_c\|_1 \leqslant 2(2t)^{2^A} 2^{(2t)^{2^A}} \pi \leqslant \nu(A+1)\pi.$$

Thus $\operatorname{Env}(\mathscr{C}) \leqslant \nu(A+1)\pi$, completing the proof of claim (c).

The plan outlined in the previous section may now be applied to good effect. Suppose that $\mathscr{A}$ is a set of algebraic numbers with

$$d(\mathscr{A}) \leqslant (2t)^{2^A} \quad \text{and} \quad \operatorname{Env}(\mathscr{A}) = X.$$

Then, assuming GRH for all Dedekind zeta functions, it follows from Lemma 5.4 that we can find a rational prime number π with

$$\pi > (2kt)^{(2t)^{2^{A+1}}}$$

and

$$\pi \leqslant \max\{16(2kt)^{(2t)^{2^{A+1}}}, 16M_1 r A^{2s}(2t)^{2\nu(A+4)}(\log(2tkX))^4\} \tag{5.20}$$

such that $\pi \nmid \Upsilon^*(\mathscr{A})$, and having the property that m_Θ splits into linear factors over $\mathbb{F}_\pi$. As a consequence of Lemma 5.5, we deduce that there is a set $\mathscr{C}$ of algebraic numbers having the property that

$$d(\mathscr{C}) \leqslant (2t)^{2^A} \quad \text{and} \quad \operatorname{Env}(\mathscr{C}) \leqslant \nu(A+1)\pi,$$

and having the property, moreover, that there is a bijection $\psi : \mathscr{A} \to \mathscr{C}$ which is an algebraic Freiman **P**-isomorphism.

We may now iterate this step, starting with the set of algebraic numbers $\mathscr{C}$, and deriving a new set $\mathscr{C}'$ algebraic Freiman **P**-isomorphic to $\mathscr{C}$, and with

$$d(\mathscr{C}') \leqslant (2t)^{2^A} \quad \text{and} \quad \operatorname{Env}(\mathscr{C}') \leqslant \nu(A+1)\pi',$$

where

$$\pi' \leqslant \max\{16(2kt)^{(2t)^{2^{A+1}}}, 16M_1 r A^{2s}(2t)^{2\nu(A+4)}(\log(2tk\nu(A+1)\pi))^4\}.$$

The composition of the two algebraic Freiman **P**-isomorphisms that we have encountered here provides an algebraic Freiman **P**-isomorphism from

$\mathscr{A}$ to $\mathscr{C}'$. Plainly, it makes sense to iterate this process repeatedly so long as the associated algebraic enveloping radius is decreasing.

In order to assess the strength of the ensuing bounds, it makes sense to simplify our estimates so as to make iteration tractable. Observe first that the bound (5.20) may be simplified by noting that, when it is satisfied, one has

$$\pi \leqslant 16M_1 r A^{2s}(2kt)^{2\nu(A+4)}(\log(2tkX))^4,$$

whence

$$\begin{aligned}\nu(A+1)\pi &\leqslant 16M_1 r A^{2s}(2kt)^{2\nu(A+4)}\nu(A+1)(\log(2tkX))^4\\ &\leqslant M_1 r A^{2s}(2kt)^{\nu(A+5)}(\log(2tkX))^4.\end{aligned}$$

We therefore have

$$\mathrm{Env}(\mathscr{C}) \leqslant \nu(A+1)\pi \leqslant \tfrac{1}{2}X = \tfrac{1}{2}\mathrm{Env}(\mathscr{A})$$

provided that X is large and

$$X \geqslant M_1^2 r^2 A^{4s}(2kt)^{2\nu(A+5)+1}.$$

Indeed, provided that X is large enough, one has

$$(\log(2tkX))^4 \leqslant \tfrac{1}{2}\sqrt{tkX},$$

and hence

$$\begin{aligned}M_1 r A^{2s}(2kt)^{\nu(A+5)}(\log(2tkX))^4 &\leqslant \tfrac{1}{2}M_1 r A^{2s}(2kt)^{\nu(A+5)}(tk)^{1/2}X^{1/2}\\ &\leqslant \tfrac{1}{2}X.\end{aligned}$$

Thus, by iterating this condensation process, we may ensure that $\mathscr{A}$ is algebraic Freiman $\mathbf{P}$-isomorphic to a set $\mathscr{B}$ of algebraic numbers with

$$d(\mathscr{B}) \leqslant (2t)^{2^A} \quad \text{and} \quad \mathrm{Env}(\mathscr{B}) \leqslant M_1^2 r^2 A^{4s}(2kt)^{\nu(A+6)}.$$

We summarise these deliberations in the form of a theorem.

Theorem 5.1. *Assume GRH for all Dedekind zeta functions. Let*

$$P_i(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s] \quad (1 \leqslant i \leqslant r)$$

be polynomials each of degree at most t, and with $\|P_i\|_1 \leqslant k$ $(1 \leqslant i \leqslant r)$. Suppose that $\mathscr{A}$ is a set of algebraic numbers with $d(\mathscr{A}) \leqslant (2t)^{2^A}$. Then $\mathscr{A}$ is algebraic Freiman $\mathbf{P}$-isomorphic to a set of algebraic numbers $\mathscr{B}$ with

$$d(\mathscr{B}) \leqslant (2t)^{2^A} \quad \textit{and} \quad \mathrm{Env}(\mathscr{B}) \ll r^2 A^{4s}(2kt)^{(2t)^{(2t)^{2^{A+6}}}}.$$

Here, the implicit constant in Vinogradov's notation is absolute.

We remark that, by inflating the parameter t so that $(2t)^{2^A} \geqslant d(\mathscr{A})$, the theorem can be applied so as to accomodate sets $\mathscr{A}$ of algebraic integers of arbitrarily large finite degree $d(\mathscr{A})$. The following corollary may make the conclusion of Theorem 5.1 more transparent.

Corollary 1. *In the setting of Theorem 5.1, we have*

$$\mathrm{Env}_\delta^*(\mathscr{A};\mathbf{P}) \leqslant \exp_4(c_1 A) \quad \textit{with} \quad \delta \leqslant (2t)^{2^A},$$

where $c_1 = c_1(r,s,t,k)$ is a positive number depending at most on r, s, t and k.

In certain situations, one may be interested in working with algebraic integers rather than more general algebraic numbers. For homogeneous polynomials, this is of course easily handled by clearing denominators.

Corollary 2. *Assume GRH for all Dedekind zeta functions. Let*

$$P_i(\mathbf{x}) \in \mathbb{Z}[x_1,\dots,x_s] \quad (1 \leqslant i \leqslant r)$$

be homogeneous polynomials each of degree at most t, and with $\|P_i\|_1 \leqslant k$ $(1 \leqslant i \leqslant r)$. Suppose that $\mathscr{A}$ is a set of algebraic integers with $d(\mathscr{A}) \leqslant (2t)^{2^A}$. Then $\mathscr{A}$ is algebraic Freiman $\mathbf{P}$-isomorphic to a set of algebraic integers $\mathscr{B}$ with

$$d(\mathscr{B}) \leqslant (2t)^{2^A} \quad \textit{and} \quad \mathrm{Env}(\mathscr{B}) \ll (r^{2A}A^{4sA})^{(2t)^{2^A}}(2kt)^{(2t)^{(2t)^{2^{A+7}}}}.$$

Here, the implicit constant in Vinogradov's notation is absolute.

Proof. Under the hypotheses of the statement of the corollary, it follows from Theorem 5.1 that $\mathscr{A}$ is algebraic Freiman $\mathbf{P}$-isomorphic to a set of algebraic numbers $\mathscr{C}$ with

$$d(\mathscr{C}) \leqslant (2t)^{2^A} \quad \text{and} \quad \mathrm{Env}(\mathscr{C}) \ll r^2 A^{4s}(2kt)^{\nu(A+6)}.$$

Consider a typical element $c \in \mathscr{C}$ and its minimal polynomial m_c over $\mathbb{Z}$. For some integer $d = d_c \leqslant d(\mathscr{C})$, we can write

$$m_c(x) = g_0 x^d + \ldots + g_{d-1}x + g_d,$$

where $g_i = g_i(c) \in \mathbb{Z}$ satisfies $|g_i| \leqslant \mathrm{Env}(\mathscr{C})$ for $0 \leqslant i \leqslant d$. Let G to be the least common multiple of all of the integers $g_0(c)$ with $c \in \mathscr{C}$, so that

$$G \leqslant \prod_{c\in\mathscr{C}} g_0(c) \leqslant (\mathrm{Env}(\mathscr{C}))^A$$

and for each $c_0 \in \mathscr{C}$ one has

$$G/g_0(c_0) \leqslant \prod_{c \in \mathscr{C} \setminus \{c_0\}} g_0(c) \leqslant (\mathrm{Env}(\mathscr{C}))^{A-1}.$$

Observe that when $c \in \mathscr{C}$, the polynomial $(G^d/g_0)m_c(x)$ is equal to

$$(Gx)^d + (G/g_0)g_1(Gx)^{d-1} + \ldots + (G^{d-1}/g_0)g_{d-1}(Gx) + (G^d/g_0)g_d,$$

so that Gc is an algebraic integer whose minimal polynomial m_{Gc} satisfies

$$\|m_{Gc}\|_1 \leqslant (G^d/g_0(c))\mathrm{Env}(\mathscr{C}) \leqslant (\mathrm{Env}(\mathscr{C}))^{dA}.$$

We consider the set

$$\mathscr{B} = \{Gc : c \in \mathscr{C}\}.$$

It follows from the above discussion that $\mathscr{B}$ is a set of algebraic integers with $d(\mathscr{B}) = d(\mathscr{C}) \leqslant (2t)^{2^A}$ and

$$\mathrm{Env}(\mathscr{B}) \leqslant (\mathrm{Env}(\mathscr{C}))^{d(\mathscr{B})A} \leqslant \left(r^{2A} A^{4As} (2kt)^{A\nu(A+6)}\right)^{d(\mathscr{B})}.$$

The conclusion of the corollary follows with a modicum of computation.

Corollary 3. *In the setting of Corollary 2, the set of algebraic integers $\mathscr{A}$ is algebraic Freiman* $\mathbf{P}$*-isomorphic to a set of algebraic integers $\mathscr{B}$ with*

$$d(\mathscr{B}) \leqslant (2t)^{2^A} \quad \textit{and} \quad \mathrm{Env}(\mathscr{B}) \ll \exp_4(c_2 A),$$

where $c_2 = c_2(r, s, t, k)$ is a positive number depending at most on r, s, t and k.

We finish this section by remarking that, in certain non-linear situations, conclusions significantly stronger than are made available via Theorem 5.1 can be obtained by making use of underlying linear structure.

Theorem 5.2. *Let $P_i(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ $(1 \leqslant i \leqslant r)$ be diagonal polynomials of the shape*

$$P_i(\mathbf{x}) = \sum_{j=1}^{s} c_{ij} x_j^t \quad (1 \leqslant i \leqslant r),$$

where $\|P_i\|_1 \leqslant k$ $(1 \leqslant i \leqslant r)$. Suppose that $\mathscr{A}$ is a finite set of integers. Then, when $\mathrm{card}(\mathscr{A})$ *is large, one has*

$$\mathrm{Env}^*_\delta(\mathscr{A}; \mathbf{P}) \leqslant t2^{t+1}(k+1)^A \quad \textit{with} \quad \delta \leqslant t^A.$$

Proof. We consider the set of integers $\mathscr{A}_t = \{a^t : a \in \mathscr{A}\}$ and the set of linear polynomials

$$L_i(\mathbf{y}) = \sum_{j=1}^{s} c_{ij} y_j \quad (1 \leqslant i \leqslant r).$$

By Theorem 3.2, the set $\mathscr{A}_t$ is Freiman $\mathbf{L}$-isomorphic to a set of integers $\mathscr{B}_t$ with $\mathrm{env}(\mathscr{B}_t) \leqslant (k+1)^A$. Now consider the set

$$\mathscr{B} = \{b^{1/t} : b \in \mathscr{B}_t\}.$$

One has $d(\mathscr{B}) \leqslant t^{\mathrm{card}(\mathscr{B})} = t^A$. Moreover, given $c \in \mathscr{B}$, one has $c^t \in \mathbb{Z}$ with $|c|^t < \mathrm{env}(\mathscr{B}_t) \leqslant (k+1)^A$. By applying the corollary to the main theorem of Granville [6], much as in the conclusion of the proof of Lemma 5.5, we find that the minimal polynomial m_c of c over $\mathbb{Z}$ is a divisor of the polynomial $f_{t,l}(x) = x^t - l$, where $l = c^t \in \mathscr{B}_t$. Thus,

$$\begin{aligned} \|m_c\|_1 &\leqslant 2\mathrm{deg}(f_{t,l}) \Big(\frac{\sqrt{5}+1}{2} \Big)^{\deg(f_{t,l})} \|f_{t,l}\|_1 \\ &\leqslant t2^{t+1} \mathrm{env}(\mathscr{B}_t) \\ &\leqslant t2^{t+1}(k+1)^A. \end{aligned}$$

Thus $\mathrm{Env}(\mathscr{B}) \leqslant t2^{t+1}(k+1)^A$, and $\mathscr{B}$ is algebraic Freiman $\mathbf{P}$-isomorphic to $\mathscr{A}$ with $d(\mathscr{B}) \leqslant t^A$. This completes the proof of the theorem.

6 Densifications of sets

We turn next to a discussion of the densification idea to which we alluded in the introduction. We begin with an analogue of the Freiman $\mathbf{P}$-isomorphism defined in Definition 2.1 suitable for the discussion of cartesian products. In this context, when $P_1, \dots, P_r \in \mathbb{Z}[x_1, \dots, x_s]$ and $\mathscr{C} \subset \mathbb{Z}$, we again write

$$S(\mathscr{C}; \mathbf{P}) = \{\mathbf{x} \in \mathscr{C}^s : P_i(\mathbf{x}) = 0 \ (1 \leqslant i \leqslant r)\}.$$

Also, when $\mathbf{x}_1, \dots, \mathbf{x}_t \in \mathscr{C}^s$, we have in mind the notational convention that

$$\mathbf{x}_i = (x_{i1}, \dots, x_{is}).$$

Then, when $(\mathbf{x}_1, \dots, \mathbf{x}_t) \in \mathscr{C}^s \times \dots \times \mathscr{C}^s$, it is convenient to abbreviate the t-tuple $(x_{1j}, x_{2j}, \dots, x_{tj})$ as $\mathbf{x}^{(j)}$.

Definition 6.1. *Let $t \in \mathbb{N}$, and suppose that $\mathscr{A}$ and $\mathscr{B}$ are finite sets of integers with $|\mathscr{B}| = |\mathscr{A}|^t$. Suppose in addition that the polynomials $P_1, \dots, P_r$ lie in $\mathbb{Z}[x_1, \dots, x_s]$. We say that a bijection $\omega : \mathscr{A}^t \to \mathscr{B}$ is a t-fold Freiman $\mathbf{P}$-isomorphism (from $\mathscr{A}$ to $\mathscr{B}$) if it is the case that*

$$(\mathbf{x}_1, \dots, \mathbf{x}_t) \in S(\mathscr{A}; \mathbf{P})^t$$

if and only if

$$\Big(\omega(\mathbf{x}^{(1)}), \dots, \omega(\mathbf{x}^{(s)})\Big) \in S(\mathscr{B}; \mathbf{P}).$$

As in the discussion of §2, we emphasise that a t-fold Freiman $\mathbf{P}$-isomorphism is specific to a particular polynomial tuple $\mathbf{P}$, and maps a t-tuple of integers to an integer. This once again permits an iterative approach in which t-fold Freiman $\mathbf{P}$-isomorphisms are successively composed in the natural manner.

It may be useful to highlight the utility of such a definition. When $t > 1$, the structure of the solutions of the system of polynomials

$$P_i(\mathbf{x}) = 0 \quad (1 \leqslant i \leqslant r), \tag{6.1}$$

with $\mathbf{x} \in \mathscr{A}^s$, both determines and is determined by

$$S(\mathscr{A}; \mathbf{P})^t = S(\mathscr{A}; \mathbf{P}) \times \ldots \times S(\mathscr{A}; \mathbf{P}).$$

When $\omega : \mathscr{A}^t \to \mathscr{B}$ is a t-fold Freiman $\mathbf{P}$-isomorphism, it follows from Definition 6.1 that $S(\mathscr{A}; \mathbf{P})^t$ is in bijective correspondence with

$$S(\omega(\mathscr{A}^t); \mathbf{P}) = S(\mathscr{B}; \mathbf{P}).$$

Thus, the structure of the solutions of the system (6.1) with $\mathbf{x} \in \mathscr{A}^s$ both determines and is determined by the structure of the solutions of the system (6.1) with $\mathbf{x} \in \mathscr{B}^s$. A particularly simple consequence of this observation is that, just as $|\mathscr{B}| = |\mathscr{A}|^t$, so too one has

$$|S(\mathscr{B}; \mathbf{P})| = |S(\mathscr{A}; \mathbf{P})|^t.$$

Provided that $\mathrm{env}(\mathscr{B})$ is not too much larger than $\mathrm{env}(\mathscr{A})$, then the solution set $S(\mathscr{A}; \mathbf{P})$ of a sparse set $\mathscr{A}$ may be understood precisely in terms of a potentially denser set $\mathscr{B}$ and its solution set $S(\mathscr{B}; \mathbf{P})$. This motivates the next definition.

Definition 6.2. *We say that a map $\omega : \mathscr{A}^t \to \mathscr{D}$ is a t-fold $\mathbf{P}$-densifier of $\mathscr{A}$ if it is a t-fold Freiman $\mathbf{P}$-isomorphism having the property that $env(\mathscr{D}) \leqslant env(\mathscr{A})^t$. When the latter inequality is strict, we refer to ω as a strict t-fold $\mathbf{P}$-densifier of $\mathscr{A}$. In either case, we refer to $\mathscr{D}$ as being a t-fold $\mathbf{P}$-densification of $\mathscr{A}$.*

Of particular interest are the t-fold $\mathbf{P}$-densifications $\mathscr{D}_t$ of $\mathscr{A}$ distinguished by the property that

$$\frac{\log \operatorname{env}(\mathscr{D}_t)}{\log |\mathscr{D}_t|}$$

is particularly small.

Definition 6.3. *Let $\mathscr{A}$ be a finite set of integers, and suppose that the polynomials $P_1, \dots, P_r$ lie in $\mathbb{Z}[x_1, \dots, x_s]$. We say that the set $\mathscr{A}$ has* $\mathbf{P}$*-densification exponent κ when*

$$\kappa = \liminf_{t\to\infty} \left\{ \frac{\log env(\mathscr{D}_t)}{\log |\mathscr{D}_t|} : \mathscr{D}_t \textit{ is a } t\textit{-fold densification of } \mathscr{A} \right\}.$$

It follows that when $\mathscr{A}$ has finite $\mathbf{P}$-densification exponent κ, then for each $\varepsilon > 0$ there is a natural number t and a t-fold $\mathbf{P}$-densification $\mathscr{D}_t$ of $\mathscr{A}$ such that

$$\operatorname{env}(\mathscr{D}_t) \leqslant |\mathscr{D}_t|^{\kappa+\varepsilon}.$$

Suppose that, in addition, one has an estimate of the shape

$$|S(\mathscr{B};\mathbf{P})| \ll \operatorname{env}(\mathscr{B})^{\varepsilon} |\mathscr{B}|^{\theta},$$

valid for all finite sets of integers $\mathscr{B}$. Then we may infer that

$$|S(\mathscr{A};\mathbf{P})|^t = |S(\mathscr{D}_t;\mathbf{P})| \ll \operatorname{env}(\mathscr{D}_t)^{\varepsilon} |\mathscr{D}_t|^{\theta} < |\mathscr{D}_t|^{\theta+2\kappa\varepsilon} \ll |\mathscr{A}|^{t(\theta+2\kappa\varepsilon)},$$

whence

$$|S(\mathscr{A};\mathbf{P})| \ll |\mathscr{A}|^{\theta+2\kappa\varepsilon}.$$

In this way, it should be apparent that the existence of finite $\mathbf{P}$-densification exponents would lead from conclusions such as Theorem 1.1 to the validity of conjectures of the shape of that recorded in Conjecture 1. We shall see in the next section that, while such objectives are attainable for linear systems $\mathbf{P}$, it would seem that for systems $\mathbf{P}$ of higher degree, currently accessible conclusions are necessarily weaker.

7 Densifications for linear systems of equations

The polynomial systems most amenable to densification via the circle of ideas already presented in §3 are systems of homogeneous linear equations. Since the results concerning such systems are both simple and instructive, we expend the bulk of this section on their analysis. In order to fix ideas, suppose that $s \geqslant 2$, $r \geqslant 1$ and for $1 \leqslant i \leqslant r$ one has $c_{ij} \in \mathbb{Z}$ $(1 \leqslant j \leqslant s)$. We again ignore the trivial situation in which for some index i one has $c_{ij} = 0$ for $1 \leqslant j \leqslant s$. The system of polynomials initially of interest to us in this section is

$$P_i(\mathbf{x}) = \sum_{j=1}^{s} c_{ij} x_j \quad (1 \leqslant i \leqslant r).$$

Next, when $\mathscr{A} \subset \mathbb{Z}$ is a finite set of integers, we recall the notation of writing $S(\mathscr{A}; \mathbf{P})$ for the set of solutions of the system of equations $P_i(\mathbf{x}) = 0$ $(1 \leqslant i \leqslant r)$, with $\mathbf{x} \in \mathscr{A}^s$. In accordance with the treatment of §3, we define $\mathit{\Lambda} = \mathit{\Lambda}(\mathbf{c})$ by putting

$$\mathit{\Lambda} = \max_{1 \leqslant i \leqslant r} \sum_{j=1}^{s} |c_{ij}|.$$

Theorem 7.1. *Consider a system* $\mathbf{P}$ *of linear polynomials as described in the preamble, and consider a finite set of integers* $\mathscr{A}$*. Then provided that* $A = \mathrm{card}(\mathscr{A})$ *is sufficiently large in terms of* r *and* s*, the set* $\mathscr{A}$ *has a finite* $\mathbf{P}$*-densification exponent* κ *satisfying* $\kappa \leqslant s$*. In particular, whenever* $\varepsilon > 0$*, there exists a natural number* t *and a* t*-fold Freiman* $\mathbf{P}$*-isomorphism* $\omega : \mathscr{A}^t \to \mathscr{D}$ *having the property that* $\mathrm{env}(\mathscr{D}) \leqslant \mathrm{card}(\mathscr{D})^{s+\varepsilon}$.

Proof. Fix a small positive number ε. We seek to apply an iterative strategy that, given a set $\mathscr{D}$ that is t-fold Freiman $\mathbf{P}$-isomorphic to $\mathscr{A}$, generates a new set $\mathscr{D}'$ that is t'-fold Freiman $\mathbf{P}$-isomorphic to $\mathscr{D}$ and satisfies

$$\frac{\log \mathrm{env}(\mathscr{D}')}{\log \mathrm{card}(\mathscr{D}')} \leqslant (1-\varepsilon) \frac{\log \mathrm{env}(\mathscr{D})}{\log \mathrm{card}(\mathscr{D})}. \tag{7.1}$$

Notice that the composition of a t-fold Freiman $\mathbf{P}$-isomorphism from $\mathscr{A}$ to $\mathscr{D}$, and a t'-fold Freiman $\mathbf{P}$-isomorphism from $\mathscr{D}$ to $\mathscr{D}'$, gives a tt'-fold Freiman $\mathbf{P}$-isomorphism from $\mathscr{A}$ to $\mathscr{D}'$. Thus, the relation (7.1) suggests an improvement in the densification exponent. Provided that we are able to iterate this process sufficiently many times, we find that a $\mathbf{P}$-densification $\mathscr{D}$ of $\mathscr{A}$ exists with

$$\frac{\log \mathrm{env}(\mathscr{D})}{\log \mathrm{card}(\mathscr{D})} \leqslant (1-\varepsilon)^n \frac{\log \mathrm{env}(\mathscr{A})}{\log \mathrm{card}(\mathscr{A})},$$

with n as large as is necessary. It transpires that when

$$\mathrm{env}(\mathscr{D}) > \mathrm{card}(\mathscr{D})^{s+\varepsilon},$$

then further iteration is possible, and in this way we see that the $\mathbf{P}$-densification exponent of $\mathscr{A}$ is at most s.

We now initiate the proof proper. We may suppose without loss of generality that $\Lambda \geqslant 2$ and $s \geqslant 2$. We consider a finite set of integers $\mathscr{D}$ that is t-fold Freiman $\mathbf{P}$-isomorphic to $\mathscr{A}$, so that $|\mathscr{D}| = A^t \geqslant A$. Write $D = |\mathscr{D}|$ and $X = \mathrm{env}(\mathscr{D}) - 1$. If one were to have

$$X + 1 \leqslant D^{s(1+4\varepsilon)},$$

then the desired conclusion would follow, since $\varepsilon > 0$ may be taken arbitrarily small. We may therefore suppose that $X + 1 > D^{s(1+4\varepsilon)}$.

Next, in accordance with (3.1), we define the natural number Υ by putting

$$\Upsilon = \Bigg(\prod_{\substack{d_1,d_2 \in \mathscr{D}\\ d_1 \neq d_2}} |d_1 - d_2| \Bigg) \Bigg(\prod_{\substack{\mathbf{d} \in \mathscr{D}^s\\ \mathbf{d} \notin S(\mathscr{D};\mathbf{P})}} \sum_{i=1}^r |P_i(\mathbf{d})| \Bigg).$$

Then one finds that

$$1 \leqslant \Upsilon \leqslant (2X)^{D^2} (r\Lambda X)^{D^s} \leqslant \tfrac{1}{3} (r\Lambda X)^{2D^s}.$$

Note that

$$2\log(3\Upsilon) \leqslant 4D^s \log(r\Lambda X).$$

Then provided that $Y \geqslant 4D^s \log(r\Lambda X)$, it follows from the prime number theorem that in any interval $(Y, 2Y)$, there exist at least D prime numbers π with $\pi \nmid \Upsilon$. Let $\pi_1, \ldots, \pi_D$ be any D such distinct prime numbers.

We next construct a map $\omega : \mathscr{D}^D \to \mathbb{Z}$ as follows. When

$$\mathbf{d} = (d_1, \ldots, d_D) \in \mathscr{D}^D,$$

we define

$$\omega(\mathbf{d}) = \sum_{i=1}^D d_i \prod_{\substack{1 \leqslant j \leqslant D\\ j \neq i}} \pi_j. \tag{7.2}$$

Write $\mathscr{E} = \omega(\mathscr{D}^D)$. Then we claim that the mapping $\omega : \mathscr{D}^D \to \mathscr{E}$ is a D-fold Freiman $\mathbf{P}$-isomorphism from $\mathscr{D}$ to $\mathscr{E}$.

We first verify that $\omega : \mathscr{D}^D \to \mathscr{E}$ is a bijection, and for this it suffices to check that ω is injective. However, if $\mathbf{d}, \mathbf{d}' \in \mathscr{D}^D$ and $\omega(\mathbf{d}) = \omega(\mathbf{d}')$, then it is apparent that

$$\sum_{i=1}^D d_i \prod_{\substack{1 \leqslant j \leqslant D\\ j \neq i}} \pi_j \equiv \sum_{i=1}^D d_i' \prod_{\substack{1 \leqslant j \leqslant D\\ j \neq i}} \pi_j \pmod{\pi_k} \quad (1 \leqslant k \leqslant D),$$

whence

$$(d_k-d_k')\prod_{\substack{1\leqslant j\leqslant D\\ j\ne k}}\pi_j\equiv 0 \pmod{\pi_k}\quad (1\leqslant k\leqslant D).$$

For each index k, however, one has

$$\Biggl(\pi_k,\prod_{\substack{1\leqslant j\leqslant D\\ j\ne k}}\pi_j\Biggr)=1,$$

and thus we deduce that $d_k\equiv d_k' \pmod{\pi_k}$ $(1\leqslant k\leqslant D)$. Recalling the definition of Υ, however, one sees that $\pi_k\nmid (d_k-d_k')$ whenever $d_k\ne d_k'$, and so we must have $d_k=d_k'$ $(1\leqslant k\leqslant D)$. In this way, we conclude that $\mathbf{d}=\mathbf{d}'$, whence $\omega:\mathscr{D}^D\to\mathscr{E}$ is indeed bijective.

Next, whenever $(\mathbf{d}_1,\dots,\mathbf{d}_D)\in S(\mathscr{D};\mathbf{P})^D$, the linearity of the polynomials $\mathbf{P}$ ensures that for $1\leqslant l\leqslant r$, one has

$$P_l\left(\omega(\mathbf{d}^{(1)}),\dots,\omega(\mathbf{d}^{(s)})\right)=\sum_{i=1}^D P_l(d_{i1},\dots,d_{is})\prod_{\substack{1\leqslant j\leqslant D\\ j\ne i}}\pi_j=0.$$

Thus $\left(\omega(\mathbf{d}^{(1)}),\dots,\omega(\mathbf{d}^{(s)})\right)\in S(\mathscr{E};\mathbf{P})$. Also, when

$$(\mathbf{d}_1,\dots,\mathbf{d}_D)\notin S(\mathscr{D};\mathbf{P})^D,$$

then for some index l with $1\leqslant l\leqslant r$, and some index k with $1\leqslant k\leqslant D$, one has

$$P_l(d_{k1},\dots,d_{ks})\ne 0.$$

Meanwhile, if one were to have

$$P_l\left(\omega(\mathbf{d}^{(1)}),\dots,\omega(\mathbf{d}^{(s)})\right)=0\quad (1\leqslant l\leqslant r), \tag{7.3}$$

then in particular,

$$\sum_{i=1}^D P_l(d_{i1},\dots,d_{is})\prod_{\substack{1\leqslant j\leqslant D\\ j\ne i}}\pi_j\equiv 0 \pmod{\pi_k}\quad (1\leqslant l\leqslant r).$$

The latter congruences imply that

$$P_l(d_{k1},\dots,d_{ks})\prod_{\substack{1\leqslant j\leqslant D\\ j\ne k}}\pi_j\equiv 0 \pmod{\pi_k}\quad (1\leqslant l\leqslant r),$$

whence

$$P_l(d_{k1},\dots,d_{ks})\equiv 0 \pmod{\pi_k}\quad (1\leqslant l\leqslant r). \tag{7.4}$$

But the definition of Υ ensures that when $\mathbf{d}_k\notin S(\mathscr{D};\mathbf{P})$, as we may assume, then

$$\sum_{l=1}^{r}|P_l(\mathbf{d}_k)|\not\equiv 0 \pmod{\pi_k}.$$

Thus we have $P_l(\mathbf{d}_k)\not\equiv 0 \pmod{\pi_k}$ for some index l with $1\leqslant l\leqslant r$, and this contradicts the relation (7.4). We therefore conclude that (7.3) cannot hold. In consequence, when $(\mathbf{d}_1,\dots,\mathbf{d}_D)\notin S(\mathscr{D};\mathbf{P})^D$, one must have

$$\left(\omega(\mathbf{d}^{(1)}),\dots,\omega(\mathbf{d}^{(s)})\right)\notin S(\mathscr{E};\mathbf{P}).$$

We have thus shown that the map $\omega:\mathscr{D}^D\to\mathscr{E}$ is a D-fold Freiman $\mathbf{P}$-isomorphism.

We next investigate the $\mathbf{P}$-densification exponent associated with the mapping $\omega:\mathscr{D}^D\to\mathscr{E}$. Observe first that the definition (7.2) shows that

$$\mathrm{env}(\mathscr{E})\leqslant D(2Y)^{D-1}\max_{1\leqslant i\leqslant D}|d_i|\leqslant D(2Y)^{D-1}\mathrm{env}(\mathscr{D}).$$

We take $Y=4D^s\log(r\Lambda X)$, in which we recall that $X=\mathrm{env}(\mathscr{D})-1$. Thus

$$\begin{aligned}\frac{\log\mathrm{env}(\mathscr{E})}{\log|\mathscr{E}|}&\leqslant\frac{\log\mathrm{env}(\mathscr{D})+\log D+(D-1)\log(2Y)}{D\log D}\\&=\frac{1}{D}\left(\frac{\log\mathrm{env}(\mathscr{D})}{\log D}\right)+\left(1-\frac{1}{D}\right)\left(\frac{\log(2Y)}{\log D}\right)+\frac{1}{D}.\end{aligned}$$

It follows that whenever

$$\frac{\log(2Y)}{\log D}\leqslant(1-2\varepsilon)\frac{\log\mathrm{env}(\mathscr{D})}{\log D}, \tag{7.5}$$

then one has

$$\frac{\log\mathrm{env}(\mathscr{E})}{\log|\mathscr{E}|}\leqslant(1-\varepsilon)\frac{\log\mathrm{env}(\mathscr{D})}{\log|\mathscr{D}|}. \tag{7.6}$$

This is the improving $\mathbf{P}$-densification argument outlined in the opening discussion of the proof.

Let us return to examine the condition (7.5). This condition is satisfied provided that

$$2Y\leqslant(\mathrm{env}(\mathscr{D}))^{1-2\varepsilon}=(X+1)^{1-2\varepsilon},$$

which is to say that

$$8D^s \log(r\Lambda X) \leqslant (X+1)^{1-2\varepsilon}.$$

However, in the opening discussion of the proof, we were at liberty to suppose that $X+1 > D^{s(1+4\varepsilon)}$. Thus we have

$$\frac{(X+1)^{1-2\varepsilon}}{\log(r\Lambda X)} > D^{s(1+\varepsilon)} > 8D^s,$$

and in consequence the condition (7.5) is fulfilled. This justifies the conclusion (7.6).

As we explained in the opening discussion of the proof, the upper bound (7.6) permits an iterative approach to be employed that delivers a t-fold $\mathbf{P}$-densification $\mathscr{D}$ of $\mathscr{A}$ satisfying the property that

$$\frac{\log \mathrm{env}(\mathscr{D})}{\log \mathrm{card}(\mathscr{D})} \leqslant (1-\varepsilon)^n \frac{\log \mathrm{env}(\mathscr{A})}{\log \mathrm{card}(\mathscr{A})}, \tag{7.7}$$

with n arbitarily large, provided only that $\mathrm{env}(\mathscr{D}) > (\mathrm{card}(\mathscr{D}))^{s(1+4\varepsilon)}$. Since for sufficiently large n, the bound (7.7) contradicts the condition $\mathrm{env}(\mathscr{D}) > (\mathrm{card}(\mathscr{D}))^{s(1+4\varepsilon)}$, we are forced to conclude that such a t-fold $\mathbf{P}$-densification $\mathscr{D}$ exists in which $\mathrm{env}(\mathscr{D}) \leqslant (\mathrm{card}(\mathscr{D}))^{s(1+4\varepsilon)}$. By taking $\varepsilon > 0$ arbitrarily small, this shows that

$$\liminf_{t\to\infty} \left\{ \frac{\log \mathrm{env}(\mathscr{D}_t)}{\log |\mathscr{D}_t|} : \mathscr{D}_t \text{ is a } t\text{-fold } \mathbf{P}\text{-densification of } \mathscr{A} \right\} \leqslant s.$$

This completes the proof of the theorem.

The strategy underlying the proof of Theorem 7.1 can be generalised in some sense both to inhomogeneous systems, and also to systems of equations of degree exceeding 1. In order to illustrate ideas, consider a system of homogeneous polynomials $P_i(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]^r$, not necessarily linear. Suppose that these polynomials are of degree at most k, and that the sum of the absolute values of the coefficients in the polynomial $P_i(\mathbf{x})$ is at most Λ for $1 \leqslant i \leqslant r$. Let $\mathscr{D}$ be a finite set of integers that is t-fold Freiman $\mathbf{P}$-isomorphic to $\mathscr{A}$, and write $D = |\mathscr{D}|$ and $X = \mathrm{env}(\mathscr{D})$. Also, define the integer Υ now by putting

$$\Upsilon = \Bigg(\prod_{\substack{d_1, d_2 \in \mathscr{D} \\ d_1 \neq d_2}} |d_1 - d_2| \Bigg) \Bigg(\prod_{i=1}^{r} \prod_{\substack{\mathbf{d} \in \mathscr{D}^s \\ P_i(\mathbf{d}) \neq 0}} |P_i(\mathbf{d})| \Bigg).$$

Then provided that $Y \geqslant 4rD^{2s}\log(\Lambda X^k)$, it follows from the prime number theorem that in any interval $(Y, 2Y)$, there exist at least D prime numbers π with $\pi \nmid \Upsilon$. Let $\pi_1, \dots, \pi_D$ be any D such distinct prime numbers.

We again define a map $\omega : \mathscr{D}^D \to \mathbb{Z}/(\pi_1 \dots \pi_D \mathbb{Z})$ via (7.2), and write $\mathscr{E} = \omega(\mathscr{D}^D)$. The map ω is a bijection from $\mathscr{D}^D$ to $\mathscr{E}$, just as in the analogous argument in the proof of Theorem 7.1. We observe that for $1 \leqslant l \leqslant r$, one has

$$\begin{aligned} &P_l\left(\omega(\mathbf{d}^{(1)}), \dots, \omega(\mathbf{d}^{(s)})\right) \\ &\qquad \equiv \sum_{i=1}^{D} P_l(d_{i1}, \dots, d_{is}) \Bigg(\prod_{\substack{1 \leqslant j \leqslant D \\ j \neq i}} \pi_j \Bigg)^{\deg(P_l)} \pmod{\pi_1 \dots \pi_D}. \end{aligned}$$

If $(\mathbf{d}_1, \dots, \mathbf{d}_D) \notin S(\mathscr{D}; \mathbf{P})^D$, then for some index l with $1 \leqslant l \leqslant r$, and some index k with $1 \leqslant k \leqslant D$, one has

$$P_l(d_{k1}, \dots, d_{ks}) \neq 0.$$

Since $\pi_j \nmid \Upsilon$ for $1 \leqslant j \leqslant D$, one cannot have

$$P_l(d_{k1}, \dots, d_{ks}) \equiv 0 \pmod{\pi_k},$$

and consequently

$$P_l\left(\omega(\mathbf{d}^{(1)}), \dots, \omega(\mathbf{d}^{(s)})\right) \not\equiv 0 \pmod{\pi_1 \dots \pi_D} \quad (1 \leqslant l \leqslant r).$$

On the other hand, whenever $(\mathbf{d}_1, \dots, \mathbf{d}_D) \in S(\mathscr{D}; \mathbf{P})^D$, then for $1 \leqslant l \leqslant r$ one must have

$$P_l\left(\omega(\mathbf{d}^{(1)}), \dots, \omega(\mathbf{d}^{(s)})\right) \equiv 0 \pmod{\pi_1 \cdots \pi_D}.$$

We thus perceive that the solution structure of $S(\mathscr{D}; \mathbf{P})^D$ is preserved by the map ω in a manner analogous to that in our discussion of densifications. One can now attempt to rectify the set $\omega(\mathscr{D}^D) \subseteq \mathbb{Z}/(\pi_1 \dots \pi_D \mathbb{Z})$ to obtain a new set $\mathcal{F} \subset \overline{\mathbb{Q}}$ by means of the method of Grosu [7]. In this way one perceives the possibility of a densification process for sets of algebraic numbers. However, in common with the method of Grosu, there is only weak control of the degree and other data associated with the field extension in which the elements of $\mathcal{F}$ are embedded. This level of control would appear to be far too weak to facilitate useful densification conclusions.

We finish this section with some comments concerning the main conclusion of Theorem 7.1. We are interested in understanding the set of solutions $S(\mathscr{A};\mathbf{P})$ of a given system of polynomial equations

$$P_i(\mathbf{x})=0 \quad (1\leqslant i\leqslant r),$$

with variables restricted to a set $\mathscr{A}$. The conclusion of Theorem 7.1 shows that, in circumstances wherein the polynomials $P_i(\mathbf{x})$ are both homogeneous and linear at least, this objective can be achieved by studying instead a related set of integers $\mathscr{D}$ with $\mathrm{env}(\mathscr{D})\leqslant |\mathscr{D}|^{s+\varepsilon}$. While this polynomial dependence of $\mathrm{env}(\mathscr{D})$ on $|\mathscr{D}|$ may seem significantly superior to the exponential dependence available in the condensation results of §3, one may interpret this nonetheless as a "non-result". If it is the case that $\mathscr{D}$ is a typical set having roughly $X^{1/s-\varepsilon}$ elements in a box of size X, then conventional heuristics suggest nothing more than that the number of solutions of the system $P_i(\mathbf{x})=0$ $(1\leqslant i\leqslant r)$, with $\mathbf{x}\in\mathscr{D}^s$, could be $O(1)$ or even 0. In other words, the exponent $1/s$ is already small enough that in general little or nothing can be learned from the counting function for $|\mathscr{D}\cap[1,X]|$ alone. Perhaps it is more illuminating to point out that more or less any solution behaviour can be encoded in a set $\mathscr{D}$ for which $|\mathscr{D}\cap[1,X]|\ll X^{1/s-\varepsilon}$.

8 Remarks on sets of real points

We now explore some consequences of work of Vu, Wood and Wood [16, Theorem 1.1]. Let D be an integral domain of characteristic zero, such as the field of real numbers $\mathbb{R}$, and let $\mathscr{D}$ be a finite subset of D. Consider a system of polynomials $P_i(\mathbf{x})\in\mathbb{Z}[x_1,\dots,x_s]$ $(1\leqslant i\leqslant r)$. In this section, we are interested in the set $S(\mathscr{D};\mathbf{P})$ of solutions $\mathbf{x}\in\mathscr{D}^s$ of the simultaneous equations

$$P_i(x_1,\dots,x_s)=0 \quad (1\leqslant i\leqslant r).$$

The structure of the solution set $S(\mathscr{D};\mathbf{P})$ is determined by the hypergraph $\Gamma(\mathscr{D};\mathbf{P})$ defined just as in the analogous discussion of §2.

Given a large prime number p, one may seek a ring homomorphism $\varphi_p:\mathbb{Z}[\mathscr{D}]\to\mathbb{F}_p$ with the property that, whenever $(x_1,\dots,x_s)\in\mathscr{D}^s$, then

$$P_i(x_1,\dots,x_s)=0 \quad (1\leqslant i\leqslant r)$$

if and only if

$$P_i(\varphi_p(x_1),\dots,\varphi_p(x_s))=0 \quad (1\leqslant i\leqslant r).$$

We emphasise here that the latter system of equations over $\mathbb{F}_p$ amount to a system of congruences. The conclusion of [16, Theorem 1.1] demonstrates that there exists an infinite sequence of primes with positive relative density having the property that such a ring homomorphism exists. This conclusion may not at first sight be obvious from [16, Theorem 1.1]. Of course, any ring homomorphism $\varphi_p:\mathbb{Z}[\mathscr{D}]\to\mathbb{F}_p$ has the property that, whenever $(x_1,\dots,x_s)\in\mathscr{D}^s$ satisfies $P_i(x_1,\dots,x_s)=0$ $(1\leqslant i\leqslant r)$, then

$$P_i(\varphi_p(x_1),\dots,\varphi_p(x_s))=\varphi_p(P_i(x_1,\dots,x_s))=\varphi_p(0)=0 \quad (1\leqslant i\leqslant r). \tag{8.1}$$

Thus, the interesting feature for us is that whenever

$$(x_1,\dots,x_s)\in\mathscr{D}^s \quad \text{and} \quad P_i(x_1,\dots,x_s)\neq 0$$

for some index i with $1\leqslant i\leqslant r$, then

$$P_i(\varphi_p(x_1),\dots,\varphi_p(x_s))=\varphi_p(P_i(x_1,\dots,x_s))\neq 0.$$

The approach here is to define a set L of all elements

$$P_i(x_1,\dots,x_s)\in\mathbb{Z}[\mathscr{D}],$$

with $\mathbf{x}\in\mathscr{D}^s$, having the property that $P(x_1,\dots,x_s)\neq 0$. The conclusion of [16, Theorem 1.1] guarantees that the ring homomorphisms φ_p, whose existence is asserted, may be constructed in such a manner that $0\notin\varphi_p(L)$. This last assertion guarantees that the condition (8.1) holds, and this ensures that the sought after ring homomorphisms φ_p do indeed exist.

Equipped with these ring homomorphisms $\varphi_p:\mathbb{Z}[\mathscr{D}]\to\mathbb{F}_p$, we see that $\Gamma(\mathscr{D};\mathbf{P})$ is isomorphic as a hypergraph to $\Gamma(\varphi_p(\mathscr{D});\mathbf{P})$. Thus, the solution structure of $S(\mathscr{D};\mathbf{P})$ may be faithfully embedded into appropriate finite fields $\mathbb{F}_p$. If the prime number p has been chosen sufficiently large, then one may apply [7, Theorem 1.3] to obtain a faithful model of the finite field solution structure inside a number field K with degree at most $\exp(\exp(c_{\mathbf{P}}|\mathscr{D}|))$, for a suitable real number $c_{\mathbf{P}}$ depending at most on $\mathbf{P}$. For systems of linear equations, moreover, one can restrict to an integer model. In this way, one sees that linear problems involving sets of real points, for example, may be considered instead as linear problems involving sets of integers. For non-linear polynomial problems, we must instead work with sets of algebraic numbers of bounded algebraic enveloping radius. In both settings, the condensation and densification ideas of this paper become applicable.

9 The conclusion of Theorem 1.1

As promised in the introduction, we briefly justify the conclusion of Theorem 1.1. Suppose that $\mathscr{A} \subset \mathbb{Z}$ is finite with $A = \mathrm{card}(\mathscr{A})$, and define

$$\mathfrak{a}_n = \begin{cases} 1, & \text{when } n \in \mathscr{A}, \\ 0, & \text{when } n \notin \mathscr{A}. \end{cases}$$

Suppose first that $\varphi_j \in \mathbb{Z}[t]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials with

$$\det\left(\frac{\mathrm{d}^i \varphi_j(t)}{\mathrm{d}t^i}\right)_{1 \leqslant i,j \leqslant k} \neq 0.$$

Let s and k be natural numbers with $s \leqslant k(k+1)/2$. Then for each $\varepsilon > 0$, the conclusion of [17, Theorem 1.1] shows that

$$\int_{[0,1)^k} \biggl| \sum_{|n| \leqslant X} \mathfrak{a}_n e(\alpha_1 \varphi_1(n) + \ldots + \alpha_k \varphi_k(n)) \biggr|^{2s} \mathrm{d}\boldsymbol{\alpha} \ll X^\varepsilon \biggl(\sum_{|n| \leqslant X} |\mathfrak{a}_n|^2 \biggr)^s$$
$$\ll X^\varepsilon A^s.$$

Since for each $n \in \mathscr{A}$, one has $|n| \leqslant \mathrm{env}(\mathscr{A})$, the first conclusion of Theorem 1.1 follows on setting $X = \mathrm{env}(\mathscr{A})$.

The second conclusion of Theorem 1.1 follows on making use of the translation invariance property of the system of equations

$$x_1^j + \ldots + x_s^j = x_{s+1}^j + \ldots + x_{2s}^j \quad (1 \leqslant j \leqslant k).$$

Put $m = \min \mathscr{A}$, and observe that whenever $\mathbf{x} \in \mathscr{A}^{2s}$ satisfies this system of equations, then as a consequence of the binomial theorem, one has

$$(x_1 - m)^j + \ldots + (x_s - m)^j = (x_{s+1} - m)^j + \ldots + (x_{2s} - m)^j \quad (1 \leqslant j \leqslant k).$$

Thus, if we put $\mathscr{B} = \{a - m : a \in \mathscr{A}\}$, then we have $J_{s,k}(\mathscr{A}) = J_{s,k}(\mathscr{B})$. We therefore deduce from the special case $\varphi_j(t) = t^j$ $(1 \leqslant j \leqslant k)$ of the first part of the theorem that

$$J_{s,k}(\mathscr{A}) \leqslant (\mathrm{env}(\mathscr{B}))^\varepsilon A^s = (\max(\mathscr{A}) - \min(\mathscr{A}) + 1)^\varepsilon A^s = (\mathrm{diam}(\mathscr{A}))^\varepsilon A^s.$$

The second conclusion of Theorem 1.1 follows when $s \leqslant k(k+1)/2$. When instead $s > k(k+1)/2$, we observe that a trivial estimate combines with orthogonality to show that

$$J_{s,k}(\mathscr{A}) \leqslant A^{2s-k(k+1)} \int_{[0,1)^k} \biggl| \sum_{|n| \leqslant X} \mathfrak{a}_n e(\alpha_1 n + \ldots + \alpha_k n^k) \biggr|^{k(k+1)} \mathrm{d}\boldsymbol{\alpha}$$
$$\ll A^{2s-k(k+1)} \cdot (\mathrm{diam}(\mathscr{A}))^\varepsilon A^{k(k+1)/2}.$$

The desired conclusion is now immediate in this case, since

$$A^{2s-k(k+1)/2} > A^s.$$

References

1. R. C. Baker and G. Harman, *Small remainder of a vector to a suitable modulus*, Math. Z. **221** (1996), no. 1, 59–71.
2. Y. F. Bilu, V. F. Lev and I. Z. Ruzsa, *Rectification principles in additive number theory*, Discrete Comput. Geom. **19** (1998), no. 3, 343–353.
3. J. Bourgain, C. Demeter and L. Guth, *Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three*, Ann. of Math. (2) **184** (2016), no. 2, 633–682.
4. G. A. Freiman, *Addition of finite sets*, Dokl. Akad. Nauk SSSR **158** (1964), 1038–1041.
5. G. A. Freiman, *Foundations of a structure theory of set addition*, Translations of Math. Monographs **37** (1973), American Math. Soc., Providence, RI.
6. A. Granville, *Bounding the coefficients of a divisor of a given polynomial*, Monatsh. Math. **109** (1990), no. 4, 271–277.
7. C. Grosu, $\mathbb{F}_p$ *is locally like* $\mathbb{C}$, J. London Math. Soc. (2) **89** (2014), no. 3, 724–744.
8. S. Guo, Z. K. Li and P.-L. Yung, *Improved discrete restriction for the parabola*, Math. Res. Letters, to appear.
9. L. Guth, D. Maldague and H. Wang, *Improved decoupling for the parabola*, J. Eur. Math. Soc., to appear.
10. S. V. Konyagin and V. F. Lev, *Combinatorics and linear algebra of Freiman's isomorphism*, Mathematika **47** (2000), no. 1-2, 39–51.
11. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in: Algebraic number fields: L-functions and Galois properties (Proc. Symposia in Math., Univ. Durham, Durham, 1975), pp. 409–464, Academic Press, London, 1977.
12. A. Mudgal, *Diameter free estimates for the quadratic Vinogradov mean value theorem*, Proc. London Math. Soc. (3) **126** (2023), no. 1, 76–128.
13. R. Schippa, *Improved decoupling for the moment curve in three dimensions*, arXiv:2302.10884.
14. T. Tao and V. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, 2006.
15. H. Tôyama, *A note on the different of the composed field*, Kodai Math. Sem. Rep. **7** (1955), no. 2, 43–44.
16. V. H. Vu, M. M. Wood and P. M. Wood, *Mapping incidences*, J. London Math. Soc. (2) **84** (2011), no. 2, 433–445.
17. T. D. Wooley, *Nested efficient congruencing and relatives of Vinogradov's mean value theorem*, Proc. London Math. Soc. (3) **118** (2019), no. 4, 942–1016.