

# RANGES OF POLYNOMIALS CONTROL DEGREE RANKS OF GREEN AND TAO OVER FINITE PRIME FIELDS

THOMAS KARAM 

*Mathematical Institute, University of Oxford, Oxford, Oxfordshire, OX26GG, United Kingdom*

Email: [thomaskaram@sjtu.edu.cn](mailto:thomaskaram@sjtu.edu.cn)

(Received 2 March 2025)

*Abstract* Let  $p$  be a prime, let  $1 \leq t < d < p$  be integers, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . We establish that if a polynomial  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  with degree  $d$  is such that the image  $P(S^n)$  does not contain the full image  $A(\mathbb{F}_p)$  of any non-constant polynomial  $A : \mathbb{F}_p \rightarrow \mathbb{F}_p$  with degree at most  $t$ , then  $P$  coincides on  $S^n$  with a polynomial that in particular has bounded degree- $\lfloor d/(t+1) \rfloor$ -rank in the sense of Green and Tao. Similarly, we prove that if the assumption holds even for  $t = d$ , then  $P$  coincides on  $S^n$  with a polynomial determined by a bounded number of coordinates.

*Keywords:* finite fields; polynomials

*2010 Mathematics subject classification:* Primary 11T06

## 1. Introduction and main results

Throughout this paper, the letter  $n$  will always denote a positive integer, and all our statements will be uniform in  $n$ .

### 1.1. A theorem of Green and Tao and its applications

A landmark result of Green and Tao proved in 2007 [12] states that over a finite prime field  $\mathbb{F}_p$  for some prime  $p$ , a multivariate polynomial with degree  $1 \leq d < p$  that is not approximately equidistributed can be expressed as a function of a bounded number of polynomials each with degree at most  $d - 1$ . More formally, we have the following statement.

**Theorem 1.1** ([12], Theorem 1.7). *Let  $p$  be a prime, and let  $1 \leq d < p$  be an integer. Then there exists a function  $K_{p,d} : (0, 1] \rightarrow \mathbb{N}$  such that for every  $\epsilon > 0$ , if*

$P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  is a polynomial with degree  $d$  satisfying  $|\mathbb{E}_{x \in \mathbb{F}_p^n} \omega_p^{sP(x)}| \geq \epsilon$  for some  $s \in \mathbb{F}_p^*$ , then there exist  $k \leq K_{p,d}(\epsilon)$ , polynomials  $P_1, \dots, P_k : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  with degree at most  $d-1$  and a function  $F : \mathbb{F}_p^k \rightarrow \mathbb{F}_p$  satisfying

$$P = F(P_1, \dots, P_k).$$

It appears difficult to describe the full extent of the influence of this theorem in the space of a few paragraphs, so we will limit ourselves to three directions.

One important application of Theorem 1.1 is to the notion of list-decoding of Elias [7] and Wozencraft [21]. Theorem 1.1 was indeed used by Bhowmick and Lovett [3] (STOC 2015) to solve a conjecture of Gopalan–Klivans–Zuckerman [8] (STOC 2008) on the list decoding radius of fixed degree Reed-Muller codes over a field with fixed size. Later, Bhowmick and Lovett [4] extended Theorem 1.1 to the case where the field size is allowed to increase with  $n$ , which allowed them to then determine in the same paper the list decoding radius even if the field size increases with  $n$ . Even before the result of Green and Tao, list decoding had been known to have applications to several other topics, such as the construction of hard-core predicates from one-way functions as discussed by Akavia, Goldwasser, and Safra [2] (FOCS 2003) and the construction of extractors and pseudorandom generators as described by Shaltiel and Umans [20] (J. ACM 2005).

Another direction of research that Theorem 1.1 essentially started is the related question of the comparison between the partition rank and the analytic rank of tensors (or equivalently multilinear forms). The analytic rank, defined [11] by Gowers and Wolf, quantifies how close the distribution of a tensor (or equivalently multilinear form) over a finite field is to the uniform equidistribution, whereas the partition rank, introduced by Naslund [19], quantifies how difficult it is to express a tensor in terms of lower-order tensors. It had been known since the original paper [11] of Gowers and Wolf that the analytic rank is bounded above by a multiple of the partition rank (that was later improved by Lovett [16] to the more precise result that the analytic rank is at most the partition rank), but the story of results in the converse and much more difficult direction began largely with Theorem 1.1.

By now, the question of comparing partition and analytic rank has itself found several applications, not least to complexity theory. In particular, the paper [5] of Cohen and Moshkovitz (STOC 2021), which proved that for order-3 tensors the analytic and partition rank are equivalent, used that result to obtain strong trade-offs on the arithmetic complexity of a biased bilinear map, and on the separation between exactly computing a bilinear map and computing it on average. We refer to the introduction of the paper [18] of Moshkovitz and Zhu for a discussion of several more applications.

## 1.2. Degree ranks and ranges of polynomials

The main topic of the present paper will be to return to Theorem 1.1 itself and develop close analogues for ranges rather than distributions. Before stating our main results, we shall introduce some definitions and make a few more preliminary comments on Theorem 1.1 in order to properly compare our result with it.

It has been known since at least the works of Janzer [13] and Milićević [17] that the conclusion of Theorem 1.1 can be made qualitatively more precise. Before stating this strengthening, let us define a correspondingly adapted notion of degree- $d$  rank for polynomials.

**Definition 1.2.** *Let  $\mathbb{F}$  be a field, and let  $P : \mathbb{F}^n \rightarrow \mathbb{F}$  be a polynomial. Let  $d \geq 1$  be an integer.*

*We say that a polynomial  $P$  has degree- $d$  rank at most 1 if we can write  $P$  as a product of polynomials each with degree at most  $d$ .*

*The degree- $d$  rank of  $P$  is defined to be the smallest nonnegative integer  $k$  such that there exist polynomials  $P_1, \dots, P_k$  each with degree- $d$  rank at most 1, with degree at most the degree of  $P$ , and satisfying*

$$P = P_1 + \dots + P_k.$$

*We denote this quantity by  $\text{rk}_d P$ .*

The zero polynomial in particular has degree- $d$  rank equal to 0 for all  $d$ , and constant polynomials have degree- $d$  rank at most 1 for all  $d$ .

We define this notion of degree- $d$  rank in this way as doing so will be convenient for us, but it is worth pointing out that in the original paper [12] of Green and Tao, the notion referred to as the degree- $d$  rank was slightly different: for instance the degree- $(d-1)$  rank was the largest possible  $k$  in Theorem 1.1. Nonetheless, it follows immediately from the definitions that for every polynomial  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  and every positive integer  $d$ , the degree- $d$  rank of  $P$  in the sense of Green and Tao is at most  $d$  times the degree- $d$  rank of  $P$  in our sense. Therefore, proving that a polynomial has bounded degree- $d$  rank in our sense implies showing that it has bounded degree- $d$  rank in the sense of Green and Tao.

The main qualitative refinement shown in the papers of Janzer [13] and Milićević [17] is that there exists some function  $H_{p,d} : (0, 1] \rightarrow \mathbb{N}$  such that under the assumptions of Theorem 1.1, we can find  $k \leq H_{p,d}(\epsilon)$  and polynomials  $Q_1, R_1, \dots, Q_k, R_k$  satisfying

$$\deg Q_i, \deg R_i \leq d - 1 \text{ and } \deg Q_i + \deg R_i \leq d$$

for each  $i \in [k]$  and such that

$$P = Q_1 R_1 + \dots + Q_k R_k.$$

In other words, it was shown that

$$\text{rk}_{d-1} P \leq H_{p,d}(\epsilon).$$

This is a bound on the degree- $(d-1)$  rank of  $P$ , and the numerous developments which attempted to strengthen the statement of Theorem 1.1 itself have to our knowledge entirely or almost entirely focused on the degree- $(d-1)$  rank of  $P$ : some extended the range of validity of the results (Kaufman and Lovett [15], Bhowmick and Lovett [3]), and others improved the quantitative bounds on the degree- $(d-1)$  rank, through the question of comparing the partition rank to the analytic rank of tensors that we discussed earlier

(Janzer [13], Milićević [17], Adiprasito, Kazhdan and Ziegler [1], Cohen and Moshkovitz [5], [6], Moshkovitz and Zhu [18]).

For the purposes of studying approximate equidistribution of polynomials this is unsurprising, since the notion of degree- $(d-1)$  rank is indeed by far the most relevant: for instance a random polynomial of the type

$$x_1 Q(x_2, \dots, x_n)$$

with  $\deg Q = d-1$  has high degree- $(d-2)$  rank but is nonetheless not approximately equidistributed, since the probability that it takes the value 0 is approximately  $2/p - 1/p^2 > 1/p$ .

Rather than focus on the fact that for a degree- $d$  polynomial, lack of equidistribution implies bounded degree- $(d-1)$  rank, we may ask for analogues of this statement involving much stronger properties in the assumption and in the conclusion. Correspondingly, the main motivations of this paper are twofold. In one direction, we ask what can be deduced about polynomials for which we know much more than the lack of equidistribution. What can we say if we know that a polynomial does not take every value of  $\mathbb{F}_p$ , or has a smaller range still, in a sense to be made precise? In the other direction, we can ask, for a fixed integer  $1 \leq e \leq d-1$ , whether there are any properties of the distribution of the values of a polynomial which would guarantee that its degree- $e$  rank is bounded above. We will contribute to both directions simultaneously, by showing that if a polynomial  $P$  does not have full range, then it must have bounded degree- $e$  rank, for some integer  $e$  that is determined by the degree of  $P$  and by the smallest degree of a non-constant *one-variable* polynomial that has a range contained in the range of  $P$ .

**Theorem 1.3.** *Let  $p$  be a prime, and let  $1 \leq t \leq d < p$  be integers. There exists a positive integer  $\gamma(p, d, t)$  such that the following holds. Let  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be a polynomial with degree at most  $d$ . Assume that the image  $P(\mathbb{F}_p^n)$  does not contain the image of  $\mathbb{F}_p$  by any non-constant polynomial  $\mathbb{F}_p \rightarrow \mathbb{F}_p$  with degree at most  $t$ .*

- (1) *If  $t \leq d-1$ , then  $P$  has degree- $\lfloor d/(t+1) \rfloor$ -rank at most  $\gamma(p, d, t)$ .*
- (2) *If  $t = d$  then  $P$  is a constant polynomial.*

The quantitative bounds on  $\gamma(p, d, t)$  resulting from our proof seem not reasonable enough to be useful, a situation which mirrors that of the original Theorem 1.1 of Green and Tao. Nonetheless, the value  $\lfloor d/(t+1) \rfloor$  in the degree of the rank in Theorem 1.9 is optimal in general, as the following example shows.

**Example 1.4.** *Let  $p$  be a prime, let  $1 \leq d < p$  be an integer, let  $t, u \geq 1$  be integers such that  $tu \leq d$ . If  $Q$  is a random polynomial  $Q : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  with degree  $u$ , then  $Q^t$  has degree at most  $d$ , the image  $Q(\mathbb{F}_p^n)$  is contained in the set  $\{y^t : y \in \mathbb{F}_p\}$  of  $t$ -th power residues mod- $p$ , but the degree- $(u-1)$ -rank of  $P$  is usually arbitrarily large as  $n$  tends to infinity, even if it is taken in the sense of Green and Tao.*

The last part follows from a counting argument: as  $n$  tends to infinity there are  $p^{O(n^{u-1})}$  polynomials  $\mathbb{F}_p^n \rightarrow \mathbb{F}_p$  with degree at most  $u-1$ , so for every  $k \geq 1$ , the number of polynomials of the type  $F(P_1, \dots, P_k)$  with  $P_1, \dots, P_k$  with degree at most  $u-1$  and

$F : \mathbb{F}_p^k \rightarrow \mathbb{F}_p$  a function is at most  $p^k p^{O(kn^{u-1})} = p^{O(kn^{u-1})}$ , whereas there are  $p^{\Omega(kn^u)}$  polynomials  $\mathbb{F}_p^n \rightarrow \mathbb{F}_p$  with degree  $u$  and hence at least  $1/t$  times as many polynomials of the type  $Q^t$  above.

Powers of polynomials are not the only simple examples of polynomials that do not have a full range in general. They can instead be viewed as a special case of a broader class of examples that arises from composition with a one-variable polynomial.

**Example 1.5.** *Let  $p$  be a prime, let  $1 \leq d < p$  be an integer, let  $t, u \geq 1$  be integers such that  $tu \leq d$ . If  $Q : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  is a polynomial with degree  $u$ , and  $A : \mathbb{F}_p \rightarrow \mathbb{F}_p$  is a polynomial with degree  $t$ , then the polynomial  $A \circ Q$  has degree at most  $d$ , and the image  $A \circ Q(S^n)$  is contained in the image  $A(\mathbb{F}_p)$ .*

We stress that the main result from the approximate equidistribution regime will itself be an important black box that we will use in our proof of Theorem 1.3.

### 1.3. Variables with restricted range

We shall in fact prove results in a more general setting than that of Theorem 1.3, where we allow the assumption to be on the image  $P(S^n)$  for some non-empty subset  $S$  of  $\mathbb{F}_p$  rather than on the whole image  $P(\mathbb{F}_p^n)$ . On a first reading, the set  $S$  may be taken to be  $\{0, 1\}$ . In the setting of restrictions to  $S^n$ , the approximate equidistribution statement was proved by Gowers and the author in [10]. Before stating it, let us recall from that paper two points to be aware of regarding restrictions of polynomials to  $S^n$ .

The first is that whereas an affine polynomial is either constant or perfectly equidistributed on  $\mathbb{F}_p^n$ , there is already something to say about the distribution of an affine polynomial  $P$  on  $S^n$  for general non-empty  $S$ : if  $S \neq \mathbb{F}_p$  and  $P$  depends only on one coordinate, then  $P(S^n)$  is not even the whole of  $\mathbb{F}_p$ . As a simple Fourier argument, however, shows ([10], Proposition 2.2), an affine polynomial depending on many coordinates is approximately equidistributed on  $S^n$ , provided that  $S$  contains at least two elements. The second is that we may no longer hope to conclude in general that a polynomial with degree  $d$  which is not approximately equidistributed on  $S^n$  must itself have bounded degree- $(d-1)$  rank: for instance, the polynomial

$$\sum_{i=1}^n x_i^2 - x_i$$

has degree-1 rank equal to  $n$ , but only takes the value 0 on  $\{0, 1\}^n$  and is in particular not approximately equidistributed on  $\{0, 1\}^n$ . Nonetheless, the zero polynomial, with which this polynomial coincides on  $\{0, 1\}^n$ , itself has degree-1 rank equal to 0.

These two remarks motivate an extension of Definition 1.2.

**Definition 1.6.** *Let  $\mathbb{F}$  be a field, and let  $P : \mathbb{F}^n \rightarrow \mathbb{F}$  be a polynomial.*

*The degree-0 rank of  $P$  is defined to be the smallest nonnegative integer  $k$  such that we can write  $P$  as a linear combination of at most  $k$  monomials. We denote this quantity by  $\text{rk}_0 P$ .*

If  $d$  is a nonnegative integer and  $S$  is a non-empty subset of  $\mathbb{F}$  then we define the degree- $d$  rank of  $P$  with respect to  $S$  as the smallest value of  $\text{rk}_d(P - P_0)$ , where the minimum is taken over all polynomials  $P_0$  with degree at most the degree of  $P$  and satisfying  $P_0(S^n) = \{0\}$ . We denote this quantity by  $\text{rk}_{d,S} P$ .

How the notions of degree-0 rank and degree-1 rank differ may be illustrated for instance by the polynomial  $(x_1 + \cdots + x_v)(x_{v+1} + \cdots + x_{2v})$ , which has degree-1 rank equal to 1 as the previous factorization shows but also degree-0 rank equal to  $v^2$  as it cannot be written as a sum of any fewer number of monomials with degree at most 2.

We now recall a slight weakening of the main result of [10], Theorem 1.4 from that paper. (Although the full statement of that theorem is slightly more precise, the formulation below is slightly simpler to use and suffices for the purposes of the present paper.)

**Theorem 1.7** *Let  $p$  be a prime, let  $1 \leq d < p$  be an integer, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . There exists a function  $H_{p,d,S} : (0, 1] \rightarrow \mathbb{N}$  such that for every  $\epsilon > 0$ , if  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  is a polynomial with degree  $d$  satisfying  $|\mathbb{E}_{x \in S^n} \omega_p^{sP(x)}| \geq \epsilon$  for some  $s \in \mathbb{F}_p^*$ , then  $\text{rk}_{d-1,S} P \leq H_{p,d,S}(\epsilon)$ .*

We note that if  $S$  has size 1, then Theorem 1.7 as well as many of the new results of the present paper hold for immediate reasons: the set  $S^n$  then also has size 1, so every polynomial coincides on  $S^n$  with a constant polynomial, so has degree- $d$  rank at most 1 for every  $d$ .

Theorem 1.7 as well as the main results in this paper with an assumption on the distribution of values of a polynomial on  $S^n$  have a conclusion which holds up to some polynomial that vanishes on  $S^n$  (and that has degree at most the degree of the original polynomial). Although we have by now explained why having a conclusion that merely holds up to these polynomials cannot be avoided, we point out that that it is not difficult to describe polynomials which vanish on  $S^n$ : for instance, if  $S = \{0, 1\}$ , then all powers  $x_i, x_i^2, x_i^3, \dots$  are the same, and a polynomial which collapses to 0 after we identify  $x_i^{a_i}$  with  $x_i$  inside all monomials whenever  $i \in [n]$  and  $a_i \geq 1$  necessarily vanishes on  $\{0, 1\}^n$ . Conversely, the combinatorial Nullstellensatz shows that if the polynomial resulting from this identification is not the zero polynomial, then it does not vanish on  $\{0, 1\}^n$ . This characterization extends, with the exact same proof, to arbitrary non-empty subsets  $S$  of  $\mathbb{F}_p$ : a polynomial vanishes on  $S^n$  if and only if substituting  $x_i^{a_i}$  by its remainder modulo

$$\prod_{w \in S} (x_i - w)$$

at every instance of  $x_i^{a_i}$ , for all  $i \in [n]$  and  $a_i \geq 1$  leads to the zero polynomial after expanding and simplifying.

When  $S$  is not the whole of  $\mathbb{F}_p$ , one important difference between the sets  $\mathbb{F}_p^n$  and  $S^n$  is that the former is invariant under linear transformations, whereas the latter is not. We have already discussed one effect on this: the fact that  $x_1$  does not take every value of  $\mathbb{F}_p$  whereas  $x_1 + \cdots + x_n$  is approximately equidistributed for  $n$  large. The role of coordinates as opposed to general degree-1 polynomials will manifest itself further in the

proofs and in the main results of this paper. For this purpose, let us make one last round of definitions.

**Definition 1.8.** *Let  $p$  be a prime, and let  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be a polynomial with degree at most  $p - 1$ .*

*For each  $i \in [n]$ , we say that  $P$  depends on  $x_i$  if the coordinate  $x_i$  appears in one of the monomials of  $P$ .*

*We write  $I(P)$  for the set of  $i \in [n]$  such that  $P$  depends on  $x_i$ . We will refer to this set as the set of coordinates on which  $P$  depends.*

*If  $P$  is an affine polynomial, that is, a polynomial with degree at most 1, then we will also write  $I(P)$  as  $Z(P)$ , and refer to it as the support of  $P$ .*

*For  $k$  nonnegative integer, we will say that  $P$  is  $k$ -determined if the set  $I(P)$  has size at most  $k$ .*

We note that the definition above is unambiguous, as the combinatorial Nullstellensatz shows that any polynomial  $\mathbb{F}_p^n \rightarrow \mathbb{F}_p$  with degree at most  $p - 1$  has only one expansion into monomials, where we do not allow repeated terms (such as  $x_1 - x_1$ ).

#### 1.4. Statements of main results

Using Theorem 1.7 as a black box we will prove the following analogue of Theorem 1.3, where the assumption on the image is now on  $P(S^n)$  rather than on  $P(\mathbb{F}_p^n)$ . The following theorem is the main result that we shall prove in the present paper.

**Theorem 1.9.** *Let  $p$  be a prime, let  $1 \leq t \leq d < p$  be integers, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . Then there exists a positive integer  $C(p, d, t)$  such that the following holds. Let  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be a polynomial with degree at most  $d$ . Assume that  $P(S^n)$  does not contain the image of  $\mathbb{F}_p$  by any non-constant polynomial  $\mathbb{F}_p \rightarrow \mathbb{F}_p$  with degree at most  $t$ .*

- (1) *If  $t \leq d - 1$ , then  $P$  coincides on  $S^n$  with a polynomial that has degree- $\lfloor d/(t+1) \rfloor$ -rank at most  $C(p, d, t)$  and has degree at most  $d$ .*
- (2) *If  $t = d$  then  $P$  coincides on  $S^n$  with a linear combination of at most  $C(p, d, t)$  monomials with degrees at most  $d$ .*

*Equivalently, in both cases, we have*

$$\text{rk}_{\lfloor \frac{d}{t+1} \rfloor, S} P \leq C(p, d, t).$$

The optimal bounds in Theorem 1.9 and in several of our other statements involving the set  $S$  may depend on the choice of  $S$ . However, to avoid heavy notation, we will at many places avoid making this dependence explicit. (We may safely do so, since for each prime  $p$  there are only finitely many subsets of  $\mathbb{F}_p$ ).

Let us look at the extreme cases of item 1 from Theorem 1.9, and at a situation where they are both simultaneously realized.

**Corollary 1.10.** *Let  $p$  be a prime, let  $1 \leq t \leq d < p$  be integers, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . Let  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be a polynomial with degree at most  $d$ . Let  $C_{(1)}(p, d) = C(p, d, 1)$  and let  $C_{(2)}(p, d) = C(p, d, \lfloor d/2 \rfloor)$ .*

- (1) *If  $P(S^n) \neq \mathbb{F}_p$  then  $\text{rk}_{\lfloor d/2 \rfloor, S} P \leq C_{(1)}(p, d)$ .*
- (2) *If  $P(S^n)$  does not contain the image of any non-constant polynomial  $\mathbb{F}_p \rightarrow \mathbb{F}_p$  with degree at most  $\lfloor d/2 \rfloor$  then  $\text{rk}_{1, S} P \leq C_{(2)}(p, d)$ .*
- (3) *If  $d = 3$  and  $P(S^n) \neq \mathbb{F}_p$ , then  $\text{rk}_{1, S} P \leq C_{(1)}(p, 3) = C_{(2)}(p, 3)$ .*

**Proof.** Items (1) and (2) follow from taking  $t = 1$  and  $t = \lfloor d/2 \rfloor$  in Theorem 1.9 respectively. Item (3) follows from either of the items (1) and (2).  $\square$

We make the assumption  $d < p$  in Theorem 1.9 in order to be able to prove it using Theorem 1.7, which assumes  $d < p$ . However, this assumption in the original result of Green and Tao, Theorem 1.1, was later removed by Kaufman and Lovett [15], and it seems likely to us that Theorem 1.7 is true without this assumption as well. Aside from the use of Theorem 1.7, the remainder of our proof of Theorem 1.9 does not use this assumption at any point. In other words, our proof shows that removing this assumption in Theorem 1.7 would suffice to remove it in Theorem 1.9 (and to remove it in Theorem 1.3 and in Corollary 1.10).

If Theorem 1.9 still holds for  $d \geq p$ , then we would also be able to take  $t \geq p$  in Theorem 1.9, but if the latter inequality is satisfied (or even if  $t \geq p - 1$  is) then the content of Theorem 1.9 becomes immediate. Indeed Fermat's little theorem allows us to construct a degree- $(p - 1)$  polynomial  $\mathbb{F}_p \rightarrow \mathbb{F}_p$  with image equal to any prescribed pair of values, and the assumption of Theorem 1.9 is then only satisfied by polynomials which coincide with a constant on  $S^n$ .

We now turn our attention to the case of degree-2 polynomials. Throughout the paper, we will write  $Q_p$  for the set  $\{y^2 : y \in \mathbb{F}_p\}$  of mod- $p$  quadratic residues. Provided that  $p \geq 3$ , this set has size  $\frac{p+1}{2}$  and is in particular not the whole of  $\mathbb{F}_p$ . We say that a subset of  $\mathbb{F}_p$  is an *affine translate* of  $Q_p$  if it can be written as  $aQ_p + b$  for some  $a \in \mathbb{F}_p^*$  and some  $b \in \mathbb{F}_p$ . In light of the preceding discussion, we can formulate three basic constructions of a degree-2 polynomial  $P$  such that  $P(S^n) \neq \mathbb{F}_p$ .

- (1) A polynomial of the type  $A \circ L$  for some affine polynomial  $L : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  and some degree-2 polynomial  $A : \mathbb{F}_p \rightarrow \mathbb{F}_p$ . (Equivalently, the sum of a multiple of  $L^2$  and of a constant.)
- (2) A polynomial that depends only on a small number  $r < \log p / \log |S|$  of coordinates, since  $P(S^n)$  then necessarily has size at most  $|S|^r$ .
- (3) A polynomial that vanishes on  $S^n$  and has degree at most 2.

The first item of the following result can be interpreted as a converse, which says that every example arises as a sum of these three examples, letting aside the value of the bound on the number of coordinates in the second example.

**Proposition 1.11.** *There exists an absolute constant  $\kappa > 0$  such that the following holds. Let  $p$  be a prime, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . Let  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be a polynomial with degree 2.*

- (1) If  $P(S^n) \neq \mathbb{F}_p$ , then there exists an affine polynomial  $L : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ , a degree-2 polynomial  $A : \mathbb{F}_p \rightarrow \mathbb{F}_p$ , and a  $\kappa p^{15}$ -determined polynomial  $J$  with degree at most 2 such that  $P$  coincides on  $S^n$  with  $A \circ L + J$ . (Equivalently, with  $AL^2 + J$  for some  $A \in \mathbb{F}_p$ , with  $J$  changed by a constant.)
- (2) If furthermore  $P(S^n)$  does not contain any affine translate of  $Q_p$ , then  $P$  coincides on  $S^n$  with a  $\kappa p^{15}$ -determined polynomial that has degree at most 2.

Item 1 from Proposition 1.11 is significantly stronger than the conclusion that item 1 from Theorem 1.9 gives in the corresponding case  $d = 2$  and  $t = 1$ : the latter is merely that  $P$  has bounded degree-1 rank with respect to  $S$ , which we already know by Theorem 1.7. The proof of Proposition 1.11 will instead use different techniques that do not appear to generalize well to higher-degree polynomials.

In the more general case where  $P$  has general degree  $2 \leq d \leq p-1$ , one may ask whether just as with item 1 from Proposition 1.11, it is the case that provided that  $P(S^n) \neq \mathbb{F}_p$  we can always obtain a decomposition  $P = A \circ Q + J$  with  $Q : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ ,  $A : \mathbb{F}_p \rightarrow \mathbb{F}_p$  polynomials satisfying  $\deg Q \deg A \leq d$ ,  $\deg A \geq 2$  and with  $J$  a polynomial determined by a bounded number of coordinates and with degree at most  $d$ . This is however not the case in general, as a wider class of examples comes in: for instance, if  $d = p-1$ , then the polynomial  $A : x \rightarrow x^{p-1}$  satisfies  $A(\mathbb{F}_p) = \{0, 1\}$ , so if  $L_1, \dots, L_{p-2}$  are arbitrary affine polynomials then the image of  $\mathbb{F}_p^n$  by the polynomial

$$P = A \circ L_1 + \dots + A \circ L_{p-2}$$

does not contain  $p-1$ . For  $d = 2$ , such a situation cannot occur, because the Cauchy-Davenport theorem, which will play some role in the proof of Proposition 1.11, shows that the sumset of any two affine translates of  $Q_p$  is the whole of  $\mathbb{F}_p$ . (However, this is by no means the only or even the main specificity of the case  $d = 2$  that allows us to say more there than for general  $d < p$ .)

### 1.5. Connection to Ramsey theory

Ranges of polynomials on restricted subsets become relevant in Ramsey theory in many situations where the desired structure involves products of coordinate sets that are dependent. For illustration, let us explain how it relates to obstructions in the following special case of the polynomial density Hales-Jewett conjecture, discussed for instance in [9], which would be to the polynomial Szemerédi theorem what the density Hales-Jewett theorem is to Szemerédi's theorem.

**Conjecture 1.12.** *Let  $d$  be a positive integer, and let  $\delta > 0$ . Then, for  $N$  large enough depending on  $d$  and  $\delta$ , every subset of  $\{0, 1\}^{[N]^d}$  that has density at least  $\delta$  contains a pair  $(A, B)$  of subsets of  $[N]^d$  such that  $A \subset B$  and  $B \setminus A = X^d$  for some  $X \subset [N]$ .*

If  $\phi_1, \dots, \phi_d : \mathbb{F}_p^N \rightarrow \mathbb{F}_p$  are linear forms written as

$$\phi_j(x) = \sum_{i=1}^N a_{j,i} x_i$$

for every  $j \in [d]$ , and  $(A, B)$  satisfies the conclusion of Conjecture 1.12 then the linear form  $\Phi = \phi_1 \otimes \cdots \otimes \phi_d : \mathbb{F}_p^{[N]^d} \rightarrow \mathbb{F}_p$  defined by

$$\Phi(x) = \sum_{i_1, \dots, i_d \in [N]} a_{1, i_1} \cdots a_{d, i_d} x_{i_1, \dots, i_d} \quad (1.1)$$

then necessarily satisfies

$$\Phi(B) - \Phi(A) = \Phi(X^d) = \phi_1(X) \cdots \phi_d(X). \quad (1.2)$$

for every  $X \subset [N]$ .

For instance, in the case where  $\phi_1, \dots, \phi_d$  are all equal to the same linear form  $\phi$ , the right-hand side simplifies to  $(\phi(X))^d$ , so it is a  $d$ th power residue modulo  $p$ . Therefore, if  $\mathcal{A}, \mathcal{B}$  are subsets of  $\{0, 1\}^{[N]^d}$  such that  $\phi^{\otimes d}(\mathcal{B}) - \phi^{\otimes d}(\mathcal{A})$  contains no  $d$ th power residue modulo  $p$ , then there is no pair  $(A, B) \in \mathcal{A} \times \mathcal{B}$  that satisfies the conclusion of Conjecture 1.12. When the set of  $d$ th power residue modulo  $p$  is not equal to  $\mathbb{F}_p$ , this constrains  $\phi^{\otimes d}(\mathcal{A})$  and  $\phi^{\otimes d}(\mathcal{B})$ , and hence  $\mathcal{A}$  and  $\mathcal{B}$ .

This construction can then be taken further, from monomials to polynomials. Given  $n$  linear forms  $\phi_1, \dots, \phi_n : \mathbb{F}_p^N \rightarrow \mathbb{F}_p$ , and given a homogeneous degree- $d$  polynomial  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ , we can use (1.1) to produce for each monomial  $x_{i_1} \cdots x_{i_d}$  of  $P$  a linear form  $\Phi_{i_1, \dots, i_d} : \mathbb{F}_p^{[N]^d} \rightarrow \mathbb{F}_p$  satisfying

$$\Phi_{i_1, \dots, i_d}(X^d) = \phi_{i_1}(X) \cdots \phi_{i_d}(X)$$

for every  $X \subset [N]$ . This then allows us to produce a linear form  $\Phi : \mathbb{F}_p^{[N]^d} \rightarrow \mathbb{F}_p$  satisfying

$$\Phi(X^d) = P(\phi_1(X), \dots, \phi_n(X))$$

for every  $X \subset [N]$ . As earlier, if  $A, B$  are elements of  $\{0, 1\}^{[N]^d}$  such that  $A \subset B$  and  $B \setminus A = X^d$  for some  $X \subset [N]$ , then  $\Phi(B) - \Phi(A) = \Phi(X^d)$  belongs to the image

$$(P \circ (\phi_1, \dots, \phi_n))(\{0, 1\}^N). \quad (1.3)$$

The contrapositive of this is that if  $\mathcal{A}, \mathcal{B}$  are subsets of  $\{0, 1\}^{[N]^d}$  and the images  $\Phi(\mathcal{A}), \Phi(\mathcal{B})$  are such that the set  $\Phi(\mathcal{B}) - \Phi(\mathcal{A})$  has empty intersection with the image (1.3) then no pair  $(A, B) \in \mathcal{A} \times \mathcal{B}$  that satisfies the conclusion of Conjecture 1.12.

If we try to construct pairs  $(\mathcal{A}, \mathcal{B})$  of subsets of  $\{0, 1\}^{[N]^d}$  without any pair  $(A, B)$  satisfying the conclusion of Conjecture 1.12, then for the assumption of this contrapositive to be usable (that is, not immediately cause  $\mathcal{A}$  or  $\mathcal{B}$  to be empty) it is necessary that the image (1.3) is not equal to  $\mathbb{F}_p$ . In the case where the forms  $\phi_1, \dots, \phi_n$  are non-zero and of the type

$$\phi_j(x) = \sum_{i \in I_j} x_i$$

for pairwise disjoint subsets  $I_1, \dots, I_n \subset [N]$ , this image is between  $P(\{0, 1\}^n)$  and  $P(\mathbb{F}_p^n)$ , and Theorem 1.9 and Theorem 1.3 respectively give us necessary conditions for these two images to be strict subsets of  $\mathbb{F}_p$ , so allow us to better understand which polynomials  $P$  can be used to construct pairs  $(\mathcal{A}, \mathcal{B})$  without any  $d$ th power difference.

## 1.6. Final preliminary discussion

The special case  $t = d$  of Theorem 1.9 has a weaker variant where we merely forbid images of  $S$  (rather than of  $\mathbb{F}_p$ ) by one-variable polynomials; its proof is then much simpler, and already contains one of the main ideas of the proof of Theorem 1.9.

**Proposition 1.13.** *Let  $p$  be a prime, let  $d \geq 1$  be an integer, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . If  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  is a polynomial with degree at most  $d$  and  $P(S^n)$  does not contain the image of  $S$  by any non-constant polynomial  $A : \mathbb{F}_p \rightarrow \mathbb{F}_p$  with degree at most  $d$  then  $P$  coincides on  $S^n$  with a constant polynomial.*

**Proof.** We can write

$$P(x) = \sum_{k=0}^d P_k(x_1, \dots, x_{n-1})x_n^k$$

for some polynomials  $P_0, \dots, P_d : \mathbb{F}_p^{n-1} \rightarrow \mathbb{F}_p$  and for all  $x \in \mathbb{F}_p^n$ . The assumption shows that every polynomial  $P_k$  with  $1 \leq k \leq d$  vanishes on  $S^n$ , so  $P$  coincides on  $S^n$  with a polynomial with degree at most  $d$  and which only involves the coordinates  $x_1, \dots, x_{n-1}$ . We then conclude by induction on  $n$ .  $\square$

When  $S$  has size 2, checking Proposition 1.13 is immediate: for every subset  $U$  of  $\mathbb{F}_p$  with size 2 there is an affine polynomial  $A$  such that  $A(S) = U$ , so the assumption states that  $P(S^n)$  has size 1, which is the same as the conclusion.

We note that by taking  $S = \mathbb{F}_p$  in Proposition 1.13 we obtain item 2 of Theorem 1.3. Since item 1 from Theorem 1.9 specializes to item 1 from Theorem 1.3, establishing Theorem 1.9 suffices to prove Theorem 1.3.

The basic strategy which we will use to prove Theorem 1.9 will be essentially as follows: because  $P$  has degree  $d$  and is not approximately equidistributed, Theorem 1.7 shows that  $P$  coincides on  $S^n$  with some polynomial with degree at most  $d$  and of the type

$$M \circ (P_1, \dots, P_k)$$

where  $k$  is bounded and  $M$  is some polynomial. We then aim to imitate to some extent the proof of Proposition 1.13, with the polynomials  $P_1, \dots, P_k$  playing the role of the coordinates  $x_1, \dots, x_n$ . Unlike the latter, the former are however not jointly equidistributed in general (with the set of values taken to be  $\mathbb{F}_p^k$  rather than  $S^n$ ), so we cannot conclude straight away as we did in the proof of Proposition 1.13, but one of the following is

always true: either the polynomials are approximately jointly equidistributed, in which case the image  $(P_1, \dots, P_k)(S^n)$  is the same as if the polynomials  $P_1, \dots, P_k$  were jointly equidistributed, or they are not, in which case at least one non-trivial linear combination of the polynomials  $P_1, \dots, P_k$  has bounded degree- $(d' - 1)$  rank with respect to  $S$ , where

$$d' = \max(\deg P_1, \dots, \deg P_k),$$

and we may hence without loss of generality assume that  $P$  coincides on  $S^n$  with some polynomial with degree at most  $d$  and of the type

$$M' \circ (P_1, \dots, P_{k-1}, Q_1, \dots, Q_{k'})$$

where  $k'$  is bounded,  $Q_1, \dots, Q_{k'}$  are polynomials with degree strictly smaller than the degree of  $P_k$ , and  $M'$  is some polynomial. This second step, in turn, can only be performed a bounded number of times, which will conclude the argument.

The remainder of the paper is organized as follows. In [Section 2](#), we will state and prove the dichotomy on polynomials on which the previous argument relies, and which will be used in [Sections 3](#) and [4](#). Then, in [Section 3](#), we will prove [Proposition 1.11](#), and in [Section 4](#), we will write the details of the process described in the previous paragraph and hence prove [Theorem 1.9](#).

## 2. A dichotomy on the conditional range and rank of polynomials

Let us begin by formally stating the dichotomy which we just mentioned. The purpose of the remainder of the present section will be to prove it, and the two auxiliary lemmas which we will use to do so, [Lemma 2.2](#) and [Lemma 2.3](#), will not themselves be directly used at any point in any later section of the paper.

**Proposition 2.1.** *Let  $p$  be a prime, let  $1 \leq d < p$  be an integer, let  $S$  be a non-empty subset of  $\mathbb{F}_p$ , and let  $k$  be a nonnegative integer. Let  $P_1, \dots, P_k, P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be polynomials with degree at most  $d$ . If*

$$\text{rk}_{d-1,S} P > H_{p,d,S}(1/2p)$$

then  $P(S^n) = \mathbb{F}_p$ . If  $k \geq 1$  and

$$\text{rk}_{d-1,S} \left( P + \sum_{i=1}^k a_i P_i \right) > H_{p,d,S}(|S|^{-(p-1)dk}/2p)$$

for every  $a \in \mathbb{F}_p^k$ , then for every  $(v_1, \dots, v_k) \in \mathbb{F}_p^k$  the following holds: if  $(v_1, \dots, v_k) \in (P_1, \dots, P_k)(S^n)$  then

$$\mathbb{F}_p \times \{(v_1, \dots, v_k)\} \subset (P, (P_1, \dots, P_k))(S^n).$$

We begin by showing a statement which informally says that if  $P$  is sufficiently far from any linear combination of a family of polynomials  $P_1, \dots, P_k$ , then in absolute terms the

values of  $P(x)$  and of  $(P_1(x), \dots, P_k(x))$  are approximately independent, when  $x$  is chosen uniformly at random in  $S^n$ .

**Lemma 2.2.** *Let  $p$  be a prime, let  $1 \leq d < p$  be an integer, let  $S$  be a non-empty subset of  $\mathbb{F}_p$  and let  $k \geq 1$  be an integer. Let  $P_1, \dots, P_k, P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be polynomials with degree at most  $d$ . Let  $\epsilon > 0$ . If*

$$\text{rk}_{d-1, S} \left( P + \sum_{i=1}^k a_i P_i \right) > H_{p,d,S}(\epsilon)$$

for every  $(a_1, \dots, a_k) \in \mathbb{F}_p^k$ , then for every  $u \in \mathbb{F}_p$  and  $(v_1, \dots, v_k) \in \mathbb{F}_p^k$  we have that

$$|\mathbb{P}_{x \in S^n}(P(x) = u, P_1(x) = v_1, \dots, P_k(x) = v_k) - p^{-1} \mathbb{P}_{x \in S^n}(P_1(x) = v_1, \dots, P_k(x) = v_k)|$$

is at most  $\epsilon$ .

**Proof.** The proof is a standard Fourier-analytic calculation. The difference in the left-hand side can be rewritten as

$$\begin{aligned} & \mathbb{E}_{a_1, \dots, a_k \in \mathbb{F}_p} \mathbb{E}_{x \in S^n} \omega_p^{aP(x) + a_1 P_1(x) + \dots + a_k P_k(x)} - p^{-1} \mathbb{E}_{a_1, \dots, a_k \in \mathbb{F}_p} \mathbb{E}_{x \in S^n} \omega_p^{a_1 P_1(x) + \dots + a_k P_k(x)} \\ &= p^{-(k+1)} \sum_{a \in \mathbb{F}_p^*, a_1, \dots, a_k \in \mathbb{F}_p} \mathbb{E}_{x \in S^n} \omega_p^{aP(x) + a_1 P_1(x) + \dots + a_k P_k(x)}. \end{aligned}$$

By Theorem 1.7 each Fourier coefficient (i.e. each inner expectation) has modulus at most  $\epsilon$ . We conclude by the triangle inequality.  $\square$

We note that Lemma 2.2 in particular implies a “multidimensional” version of Theorem 1.7: if a family of polynomials  $P_1, \dots, P_k$  each with degree at most  $d$  is such that every non-zero linear combination of  $P_1, \dots, P_k$  has high degree- $(d-1)$  rank with respect to  $S$ , then the  $k$ -tuple  $(P_1(x), \dots, P_k(x))$  is approximately equidistributed on the set of values  $\mathbb{F}_p^k$  when  $x$  is chosen uniformly at random in  $S^n$ . Although that multidimensional version guided us in discovering the proof of Theorem 1.9, we will however not formally use it at any point in this paper, so we leave it to the interested reader to write the deduction in full.

Lemma 2.2 stated an approximation in terms of absolute probabilities: however it does not by itself immediately entail that  $P(x)$  is approximately equidistributed (or even that it takes every value of  $\mathbb{F}_p$ , which is what ultimately interests us) conditionally on any  $k$ -tuple of values of  $(P_1(x), \dots, P_k(x))$  taken with positive probability on  $S^n$ : if the probability

$$\mathbb{P}_{x \in S^n}(P_1(x) = v_1, \dots, P_k(x) = v_k)$$

is positive but very small, then the probability

$$\mathbb{P}_{x \in S^n}(P(x) = u, P_1(x) = v_1, \dots, P_k(x) = v_k)$$

could still potentially be zero.

In our next lemma, we show that this cannot happen. We thank Lisa Sauermann for explaining to us its proof in the case where all polynomials have degree 1 and  $S = \{0, 1\}$ .

**Lemma 2.3.** *Let  $p$  be a prime, let  $d \geq 1$  be an integer, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . Let  $k \geq 1$  be an integer and let  $P_1, \dots, P_k$  be polynomials  $\mathbb{F}_p^n \rightarrow \mathbb{F}_p$  each with total degree at most  $d$ . Then for each  $v \in \mathbb{F}_p^k$  the probability*

$$\mathbb{P}_{x \in S^n}(P_1(x) = v_1, \dots, P_k(x) = v_k)$$

is either 0 or at least  $|S|^{-(p-1)dk}$ .

**Proof.** Let  $v = (v_1, \dots, v_k) \in \mathbb{F}_p^k$  be fixed throughout. We define the polynomial

$$E := \prod_{i=1}^k ((P_i - v_i)^{p-1} - 1).$$

Then for each  $x \in S^n$  we have  $E(x) \neq 0$  if and only if

$$(P_1(x), \dots, P_k(x)) = (v_1, \dots, v_k). \quad (2.1)$$

The polynomial  $E$  has total degree at most  $(p-1)dk$  and can hence be expanded as a linear combination of monomials  $x_1^{t_1} \dots x_n^{t_n}$  with  $t_1 + \dots + t_n$  at most  $(p-1)dk$ . All elements of  $S$  are roots of the polynomial  $\Delta_S : \mathbb{F}_p \rightarrow \mathbb{F}_p$  defined by

$$\Delta_S(y) = \prod_{w \in S} (y - w),$$

so any polynomial  $A : \mathbb{F}_p \rightarrow \mathbb{F}_p$  in one variable coincides on  $S$  with its remainder  $A \bmod \Delta_S$  through the Euclidean division by  $\Delta_S$ , and hence each monomial  $x_1^{t_1} \dots x_n^{t_n}$  coincides on  $S^n$  with the product of remainders

$$(x_1^{t_1} \bmod \Delta_S(x_1)) \dots (x_n^{t_n} \bmod \Delta_S(x_n)),$$

which we expand into a linear combination of monomials of the type  $x_1^{t_1} \dots x_n^{t_n}$  with  $0 \leq t_i \leq |S| - 1$  for each  $i \in [n]$ . We have hence obtained a polynomial  $R$  in  $x_1, \dots, x_n$  which coincides with  $E$  on  $S^n$  and has each of its monomials of the type  $x_1^{t_1} \dots x_n^{t_n}$  with  $0 \leq t_i \leq |S| - 1$  for each  $i \in [n]$  and has total degree at most the total degree of  $E$ . Because the degree of each monomial of  $E$  is at most  $(p-1)dk$ , the total degree of  $R$  is at most  $(p-1)dk$ .

For every  $x \in S^n$ , the three statements

$$(P_1(x), \dots, P_k(x)) \neq (v_1, \dots, v_k), E(x) = 0, R(x) = 0$$

are all equivalent. In particular, if there exists  $x \in S^n$  satisfying (2.1) then  $R$  is not the zero polynomial, so one of its monomials with degree equal to the total degree of  $R$  (which may be the constant term, if  $R$  has degree 0) has a non-zero coefficient. Without loss of generality, we can assume that this monomial is  $x_1^{t_1} \dots x_s^{t_s}$  with  $0 \leq s \leq (p-1)dk$  and  $1 \leq t_i \leq |S| - 1$  for each  $i \in [s]$ . For every  $u := (u_{s+1}, \dots, u_n) \in \mathbb{F}_p^{[s+1, n]}$  the polynomial  $R_u : \mathbb{F}_p^s \rightarrow \mathbb{F}_p$  defined by

$$R_u(x_1, \dots, x_s) = R(x_1, \dots, x_s, u_{s+1}, \dots, u_n)$$

still has total degree  $s$ . By the combinatorial Nullstellensatz, there exists  $(x_1, \dots, x_s) \in S^s$  such that  $R_u(x_1, \dots, x_s) \neq 0$  and hence such that

$$(P_1, \dots, P_k)(x_1, \dots, x_s, u_{s+1}, \dots, u_n) = (v_1, \dots, v_k).$$

By the law of total probability we conclude that

$$\mathbb{P}_{x \in S^n}(P_1(x) = v_1, \dots, P_k(x) = v_k) \geq |S|^{-s} \geq |S|^{-(p-1)dk}.$$

□

Although we will not use this we note that these bounds are sharp for  $S = \{0, 1\}$ , as can be seen by taking

$$P_a = \sum_{b=1}^{p-1} \prod_{c=1}^d x_{(a-1)(p-1)d+(b-1)d+c}$$

for each  $a = 1, \dots, k$  and  $(v_1, \dots, v_k) = (p-1, \dots, p-1)$ .

The proof of Proposition 2.1 is now almost finished. The first part of Proposition 2.1 follows immediately from Theorem 1.7. In the case  $k \geq 1$ , for every fixed  $(v_1, \dots, v_k) \in (P_1, \dots, P_k)(S^n)$ , applying Lemma 2.2 with  $\epsilon = p^{-1}|S|^{-(p-1)dk}/2$  and then Lemma 2.3 we obtain

$$\mathbb{P}_{x \in S^n}(P(x) = u, P_1(x) = v_1, \dots, P_k(x) = v_k) \geq p^{-1}|S|^{-(p-1)dk}/2 > 0.$$

### 3. Deduction of the more precise result for degree-2 polynomials

In this section, we prove Proposition 1.11. The proof will use an inductive argument revolving around the following type of decomposition.

**Definition 3.1.** Let  $p$  be a prime, and let  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be a degree-2 polynomial. For any nonnegative integers  $k, l$ , we say that a  $k$ -square- $l$ -determined decomposition of  $P$  is a decomposition of the type

$$P = A_1 L_1^2 + \cdots + A_k L_k^2 + J \quad (3.1)$$

for some  $A_1, \dots, A_k \in \mathbb{F}_p$ , some affine polynomials  $L_1, \dots, L_k$ , and some  $l$ -determined polynomial  $J$  with degree at most 2.

Throughout this section, we will use the following notations. If  $k$  is a nonnegative integer, then we will write  $H_1(k)$  as shorthand for  $H_{p,1,S}(|S|^{-(p-1)k}/2p)$ . For  $L : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  an affine polynomial,  $I$  a subset of  $[n]$  and  $y$  an element of  $S^I$ , we will write

$$L(y \rightarrow I) : \mathbb{F}_p^{[n] \setminus I} \rightarrow \mathbb{F}_p$$

for the affine polynomial obtained by evaluating  $x_i$  as  $y_i$  for each  $i \in I$ . We will write  $\{y\} \times S^{I^c}$  for the subset

$$\{x \in S^n : x_i = y_i \text{ for all } i \in I\}.$$

The first component of the proof of Proposition 1.11 is the following lemma. It will play the role of an inductive step in the proof of Proposition 1.11, even though the proof of this lemma also contains an induction within.

**Lemma 3.2.** Let  $p \geq 3$  be a prime, let  $S$  be a non-empty subset of  $\mathbb{F}_p$  containing at least two elements, and let  $P$  be a degree-2 polynomial such that  $P(S^n) \neq \mathbb{F}_p$ . If  $P$  has a  $k$ -square- $l$ -determined decomposition for some nonnegative integers  $k, l$  with  $k \geq 2$ , then there exists some  $0 \leq k' < k$  such that  $P$  has a  $k'$ -square- $(l + (k - k')H_1(k))$ -determined decomposition.

**Proof.** The assumption provides a square-determined decomposition (3.1). Let  $I = I(J)$  be the set of coordinates on which the polynomial  $J$  depends. Assume for contradiction that there exist two distinct indices in  $[k]$ , which without loss of generality we can take to be  $k-1$  and  $k$ , which satisfy both inequalities

$$\begin{aligned} |Z(L_{k-1} - \sum_{i=1}^{k-2} a_i L_i) \cap I^c| &> H_1(k) \\ |Z(L_k - \sum_{i=1}^{k-1} a_i L_i) \cap I^c| &> H_1(k) \end{aligned}$$

respectively for all  $a \in \mathbb{F}_p^{k-2}$  and for all  $a \in \mathbb{F}_p^{k-1}$ . Let us fix  $y \in S^I$  arbitrarily. Then the affine polynomials  $L_i(y \rightarrow I)$  with  $i = 1, \dots, k$  satisfy both inequalities

$$\begin{aligned} |Z(L_{k-1}(y \rightarrow I) - \sum_{i=1}^{k-2} a_i L_i(y \rightarrow I))| &> H_1(k) \\ |Z(L_k(y \rightarrow I) - \sum_{i=1}^{k-1} a_i L_i(y \rightarrow I))| &> H_1(k) \end{aligned} \quad (3.2)$$

respectively for all  $a \in \mathbb{F}_p^{k-2}$  and for all  $a \in \mathbb{F}_p^{k-1}$ , so by Proposition 2.1 and (3.1) the image  $P(\{y\} \times S^{I^c})$  contains some translate of  $A_{k-1}Q_p + A_kQ_p$ ; since  $|Q_p| \geq (p+1)/2$ , the Cauchy-Davenport theorem shows that  $P(\{y\} \times S^{I^c}) = \mathbb{F}_p$  and hence  $P(S^n) = \mathbb{F}_p$ , which contradicts our assumption.

Therefore, we may without loss of generality assume that (3.2) is false and hence that

$$L_k = \sum_{i=1}^{k-1} a_i L_i + L_k^{\text{rem}}$$

for some  $a \in \mathbb{F}_p^{k-1}$  and some affine polynomial  $L_k^{\text{rem}}$  with support contained in a union  $I'$  of  $I$  and of at most  $H_1(k)$  elements. The set  $I'$  hence has size at most  $H_1(k) + |I|$ . Substituting in (3.1) and expanding, we obtain a decomposition of the type

$$P = Y \circ (L_1, \dots, L_{k-1}) + U \circ (x_j, L_i : j \in I', i \in [k-1]) + W \circ (L_1, \dots, L_{k-1}) + J',$$

where  $Y : \mathbb{F}_p^{k-1} \rightarrow \mathbb{F}_p$  is a quadratic form,  $U : \mathbb{F}_p^{I'} \otimes \mathbb{F}_p^{k-1} \rightarrow \mathbb{F}_p$  is a bilinear form,  $W : \mathbb{F}_p^k \rightarrow \mathbb{F}_p$  is a linear form, and  $J'$  is a polynomial with degree at most 2 satisfying  $I(J) \subset I'$ . We can diagonalize the quadratic form  $Y$  as

$$Y = A'_1 \Omega_1^2 + \dots + A'_{k-1} \Omega_{k-1}^2$$

for some linearly independent linear forms  $\Omega_1, \dots, \Omega_{k-1} : \mathbb{F}_p^{k-1} \rightarrow \mathbb{F}_p$  and some coefficients  $A'_1, \dots, A'_{k-1} \in \mathbb{F}_p$ . We obtain

$$Y \circ (L_1, \dots, L_{k-1}) = A'_1 L_1'^2 + \dots + A'_{k-1} L_{k-1}'^2 \quad (3.3)$$

for some affine polynomials

$$L'_1 = \Omega_1 \circ (L_1, \dots, L_{k-1}), \dots, L'_{k-1} = \Omega_{k-1} \circ (L_1, \dots, L_{k-1})$$

satisfying

$$\langle L'_1, \dots, L'_{k-1} \rangle = \langle L_1, \dots, L_{k-1} \rangle,$$

which allows us to furthermore rewrite

$$U \circ (x_j, L_i : j \in I', i \in [k-1])$$

as a linear combination of terms of the type  $x_j L'_i$  with  $j \in I'$  and  $i \in [k-1]$ , and

$$W \circ (L_1, \dots, L_{k-1})$$

as a linear combination of  $L'_1, \dots, L'_{k-1}$ . The resulting decomposition is hence of the type

$$P = \sum_{i=1}^{k-1} \left( A'_i L_i'^2 + \sum_{j \in I'} U_{i,j} x_j L'_i + B'_i L'_i \right) + J' \quad (3.4)$$

for some coefficients  $U_{i,j}, B'_i \in \mathbb{F}_p$ . If for some  $i \in [k]$  we have  $A'_i = 0$ ,  $B'_i = 0$ , and  $U_{i,j} = 0$  for all  $j \in I'$  then the expression (3.4) may be rewritten with a smaller value of  $k$ , so we may assume without loss of generality that this does not happen for any  $i \in [k]$ . Let us now distinguish two cases.

**Case 1:** Assume that all coefficients  $A'_1, \dots, A'_{k-1}$  are non-zero. Then, letting

$$L''_i = L'_i + \sum_{j \in I'} (U_{i,j}/2A'_i) x_j + B'_i/2A'_i$$

for each  $i \in [k-1]$  we may rewrite

$$P = \sum_{i=1}^{k-1} A'_i L_i''^2 + J''$$

for some polynomial  $J''$  with degree at most 2 satisfying  $I(J'') \subset I'$ . Compared to (3.1), the number of terms in the summation has decreased by 1, at the cost of  $J''$  depending on at most  $H_1(k)$  more coordinates than  $J$  does. This finishes the proof in this case.

**Case 2:** Assume that one of the coefficients  $A'_1, \dots, A'_{k-1}$  is zero. Without loss of generality, we may assume it to be  $A'_{k-1}$ . Then by the assumption that we have made in the previous paragraph, the terms  $B'_i$  and  $U_{i,j}$  with  $j \in I'$  cannot all be zero, so because  $S$  has size 2 or more, there necessarily exists  $y \in S^{I'}$  such that

$$\sum_{j \in I'} U_{i,j} y_j + B'_i \neq 0. \quad (3.5)$$

If we have

$$|Z(L'_{k-1} - \sum_{i=1}^{k-2} a_i L'_i) \cap I^c| > H_1(k)$$

for every  $a \in \mathbb{F}_p^{k-2}$  then the affine polynomials  $L'_i(y \rightarrow I')$  with  $i = 1, \dots, k-1$  obtained by evaluating the coordinate  $x_j$  to  $y_j$  for each  $j \in I'$  satisfy

$$|Z(L'_{k-1}(y \rightarrow I') - \sum_{i=1}^{k-2} a_i L'_i(y \rightarrow I'))| > H_1(k)$$

for all  $a \in \mathbb{F}_p^{k-2}$ . Using Proposition 2.1 together with (3.4) and (3.5) shows  $P(\{y\} \times S^{I^c}) = \mathbb{F}_p$  and in particular  $P(S^n) = \mathbb{F}_p$ , contradicting our assumption. Therefore, we may write

$$L'_{k-1} = \sum_{i=1}^{k-2} a_i L'_i + L'_{k-1}{}^{\text{rem}}$$

for some affine polynomial  $L'_{k-1}{}^{\text{rem}}$  with support contained in a union  $I''$  of  $I'$  and of at most  $H_1(k)$  elements. We may then rewrite (3.4) as

$$P = \sum_{i=1}^{k-2} \left( A'_i L_i'^2 + \sum_{j \in I'} U_{i,j} x_j L'_i + B'_i L'_i \right) + J''$$

for some polynomial  $J''$  with degree at most 2 satisfying  $I(J'') \subset I''$ . Compared to (3.4), the number of terms in the summation has decreased by 1, at the cost of  $J''$  depending on at most  $H_1(k)$  more coordinates than  $J$  does. We again split into cases, and iterate until we are no longer in Case 2.  $\square$

The other main component of the proof of Proposition 1.11 is the special case  $d = 2$  of the equidistribution statement, Theorem 1.7, which will give us that  $P$  coincides on  $S^n$  with a  $k$ -square- $l$ -determined decomposition for some bounded integers  $k, l$ , at which we may start the inductive process of which Lemma 3.2 encapsulates an iteration. We note for the reader interested in an utterly self-contained proof of Proposition 1.11 that the proof of this special case of Theorem 1.7 involves far fewer difficulties than the proof of the theorem in full generality: the proof of that special case is carried out in Section 2 of [10].

**Proof of Proposition 1.11** The result is immediate if  $S$  has size 1, so we may assume  $|S| \geq 2$ . The result is also immediate if  $p = 2$ , since if  $P(S^n) \neq \mathbb{F}_2$  then  $P$  coincides with a constant on  $S^n$ , so we may also assume  $p \geq 3$ . Because  $P(S^n)$  is not the whole of  $\mathbb{F}_p$ , applying Theorem 1.7 shows that  $P$  coincides on  $S^n$  with some polynomial (which we will continue referring to as  $P$  throughout the remainder of the proof) that we may decompose as

$$P = \Lambda_{1,1} \Lambda_{1,2} + \cdots + \Lambda_{r,1} \Lambda_{r,2}$$

for some  $r \leq H_{p,2,S}(1/2p)$  and some affine polynomials  $\Lambda_{1,1}, \Lambda_{1,2}, \dots, \Lambda_{r,1}, \Lambda_{r,2}$  (which may be constant polynomials). Writing  $L_{i,1}$  (resp.  $L_{i,2}$ ) for the linear part of each  $\Lambda_{i,1}$  (resp.  $\Lambda_{i,2}$ ) we obtain a decomposition

$$P = Q + L_0 \tag{3.6}$$

where

$$Q = L_{1,1} L_{1,2} + \cdots + L_{r,1} L_{r,2}$$

is the quadratic part of  $P$  and  $L_0$  is an affine polynomial. We may rewrite

$$Q = A_1 L_1^2 + \cdots + A_k L_k^2$$

for some  $k \leq 2r$ , some non-zero coefficients  $A_1, \dots, A_k \in \mathbb{F}_p$ , and some linear polynomials  $L_1, \dots, L_k$ . If

$$|Z(L_0 - \sum_{i=1}^k b_i L_i)| > H_1(k)$$

for all  $b \in \mathbb{F}_p^k$ , then by choosing  $(v_1, \dots, v_k)$  such that

$$\mathbb{P}_{x \in S^n}(L_1(x) = v_1, \dots, L_k(x) = v_k) > 0$$

and applying Proposition 2.1 we obtain that  $(L_0, L_1, \dots, L_k)(S^n)$  contains  $\mathbb{F}_p \times \{(v_1, \dots, v_k)\}$ , and the decomposition (3.6) then shows that the image  $P(S^n)$  contains the whole of  $\mathbb{F}_p$ , which contradicts our assumption. Therefore, we may write

$$L_0 = \sum_{i=1}^k B_i L_i + L_0^{\text{rem}}$$

for some  $B \in \mathbb{F}_p^k$  and some affine polynomial  $L_0^{\text{rem}}$  with support size at most  $H_1(k)$ . In turn, this leads to the decomposition

$$P = \sum_{i=1}^k (A_i L_i^2 + B_i L_i) + L_0^{\text{rem}}.$$

Because  $A_1, \dots, A_k$  are all non-zero, we may assume without loss of generality that  $B_1, \dots, B_k$  are all zero, since it suffices to replace  $L_i$  by  $L_i + B_i/2A_i$  for each  $i \in [k]$ : doing so only adds a constant to  $L_0^{\text{rem}}$ .

We have now obtained a  $k$ -square- $H_1(k)$ -determined decomposition (3.1) of  $P$ . Iterating Lemma 3.2, we eventually get a 1-square- $kH_1(k)$ -determined decomposition or a 0-square- $(k+1)H_1(k)$ -determined decomposition. This establishes item 1, aside from the value of the bound. To finish the proof of item 2, we furthermore add one last step. In the second situation we are done, and in the first situation we can write

$$P = AL_{\text{one}}^2 + J_{\text{one}}$$

for some  $A \in \mathbb{F}_p$ , some affine polynomial  $L_{\text{one}}$  and some degree-2 polynomial  $J_{\text{one}}$  such that the set  $I_{\text{one}} = I(J_{\text{one}})$  of coordinates on which  $J_{\text{one}}$  depends has size at most  $kH_1(k)$ . If  $A = 0$  then we are done, so let us assume that this is not the case. If the support of  $L$  contains at least  $H_1(k) + 1$  elements outside  $I_{\text{one}}$ , then for any (arbitrary)  $y \in S^{I_{\text{one}}}$  we have

$$|Z(L(y \rightarrow I_{\text{one}}))| > H_1(k),$$

so by Proposition 2.1 the image  $P(S^n)$  contains a translate of  $AQ_p$ , which contradicts the assumption of item 2. We conclude that  $P$  is  $(k+1)H_1(k)$ -determined.

All that remains to do is to compute the bounds. By [10], Proposition 2.11 and then [10], Proposition 2.2 respectively there exist some absolute constants  $\kappa'', \kappa'$  such that  $k \leq \kappa'' p^5$  and  $H_1(k) \leq \kappa' p^{10}$ , so  $(k+1)H_1(k) \leq \kappa p^{15}$  for some absolute constant  $\kappa$ , as desired.  $\square$

#### 4. Deduction of the main theorem in the general case

In this section, we prove Theorem 1.9. There too, we can conclude immediately if  $|S| = 1$ , so throughout the remainder of the proof we will assume  $|S| \geq 2$ . We begin by defining the kinds of decompositions that the proof will focus on, and the hierarchy that we will use between them.

**Definition 4.1.** *Let  $p$  be a prime, let  $1 \leq d < p$  be an integer, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . We say that an acceptable decomposition (with respect to  $S$ ) of a polynomial  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  with degree  $d$  is a pair  $(\mathcal{F}, F)$  with  $\mathcal{F}$  a finite set of non-zero polynomials each with degree at most  $d$ , and*

$$F : \{(i, j) : i \in [r], j \in J_i\} \rightarrow \mathcal{F}$$

*a function for some nonnegative integer  $r$  and some finite sets  $J_i$  for each  $i \in [r]$ , which satisfies the following two properties.*

- (1) *We have the decomposition*

$$P = P_0 + \sum_{i=1}^r \alpha_i \prod_{j \in J_i} F(i, j) \tag{4.1}$$

*for some polynomial  $P_0$  with degree at most  $d$  such that  $P_0(S^n) = \{0\}$  and for some coefficients  $\alpha_i \in \mathbb{F}_p$ .*

- (2) *Every  $i \in [r]$  satisfies*

$$\deg \prod_{j \in J_i} F(i, j) \leq d.$$

**Definition 4.2.** *Let  $p$  be a prime, let  $1 \leq d < p$  be an integer, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . Let  $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be a polynomial with degree  $d$ . We say that the degree description of a given acceptable decomposition  $(\mathcal{F}, F)$  of  $P$  is the  $(d+1)$ -tuple  $(D_0, \dots, D_d) \in \mathbb{N}^d$  such that*

- (1)  *$D_0$  is the number of polynomials of  $\mathcal{F}$  which are either of the type  $ax_i$  for some  $i \in [n]$  and  $a \in \mathbb{F}_p^*$ , or of the type  $c$  for some  $c \in \mathbb{F}_p$*

- (2)  $D_1$  is the number of all other affine polynomials of  $\mathcal{F}$
- (3)  $D_u$  is the number of degree- $u$  polynomials of  $\mathcal{F}$  for every  $u \in \{2, \dots, d\}$ .

We say that the size of the acceptable decomposition is the size of the set  $\mathcal{F}$ . For every polynomial  $Q \in \mathcal{F}$ , we furthermore say that the modified degree of the polynomial  $Q$  is the unique  $u$  of  $\{0, 1, \dots, d\}$  such that  $Q$  is of the type described above in the definition of  $D_u$ .

Let  $P$  be as in the assumption of Theorem 1.9, and let  $e = \lfloor d/(t+1) \rfloor$ . The main idea of the proof will be to successively obtain a sequence of acceptable decompositions of  $P$  which have degree descriptions that are strictly decreasing in the colexicographic order, until we obtain an acceptable decomposition in which all polynomials of  $\mathcal{F}$  have modified degree at most  $e$ . For each step  $l$  of the process, we write  $\mathcal{F}_l$  for the family  $\mathcal{F}$  at the start of the  $l$ th acceptable decomposition of the process. The following three properties will be satisfied.

- (1) The difference  $\mathcal{F}_l \setminus \mathcal{F}_{l+1}$  is a singleton containing a polynomial of  $\mathcal{F}_l$  with maximal modified degree among those of the polynomials of  $\mathcal{F}_l$ .
- (2) The difference  $\mathcal{F}_{l+1} \setminus \mathcal{F}_l$  has size bounded by a function of the degree description of  $\mathcal{F}_l$  (and of  $p, d, t, S$ ).
- (3) All polynomials of  $\mathcal{F}_{l+1} \setminus \mathcal{F}_l$  have modified degrees strictly smaller than that of the polynomial of  $\mathcal{F}_l \setminus \mathcal{F}_{l+1}$ .

The acceptable decomposition obtained at the end of the process will still have bounded size, with bounds depending on  $p, d, t, S$  only. For the convenience of the reader, we will formalize the main principle behind this as a separate lemma. Although we have found it more convenient to state it in its somewhat abstract form, the case where we will use it is that where  $K(D)$  is the size of a given acceptable decomposition obtained at the end of an induction starting with an acceptable decomposition with degree description  $D$ , the quantity  $V(D)$  is the size  $D_0 + \dots + D_e$  whenever  $D_{e+1} = \dots = D_d = 0$  (since if the original acceptable decomposition has all its polynomials with degrees at most  $e$ , then there is nothing to do), and  $W(D)$  is a bound on the number of extra polynomials coming from item (2), when the family  $\mathcal{F}_l$  has degree description  $D$ .

**Lemma 4.3.** *Let  $0 \leq e \leq d$  be nonnegative integers. Let  $V, W : \mathbb{N}^{d+1} \rightarrow \mathbb{N}$  be functions. Then there exists a function  $B : \mathbb{N}^{d+1} \rightarrow \mathbb{N}$  depending on  $e, d, V, W$  only such that whenever  $K : \mathbb{N}^{d+1} \rightarrow \mathbb{N}$  is a function satisfying*

$$K(D_0, D_1, \dots, D_e, 0, \dots, 0) \leq V(D_0, D_1, \dots, D_e, 0, \dots, 0)$$

for all  $D_0, D_1, \dots, D_e \in \mathbb{N}$  and such that for each integer  $m$  with  $e < m \leq d$  and all  $D_0, D_1, \dots, D_m \in \mathbb{N}$  with  $D_m \neq 0$  there exist

$$0 \leq u_0, \dots, u_{m-1} \leq W(D_0, D_1, \dots, D_m, 0, \dots, 0)$$

satisfying

$$K(D_0, D_1, \dots, D_m, 0, \dots, 0) \leq K(D_0 + u_0, D_1 + u_1, \dots, D_{m-1} + u_{m-1}, D_m - 1, 0, \dots, 0)$$

then  $K(D) \leq B(D)$  for all  $D \in \mathbb{N}^{d+1}$ .

**Proof.** The first assumption shows that we may take  $B(D) = V(D)$  for all  $D \in \mathbb{N}^{d+1}$  such that  $D_m = 0$  for all  $e < m \leq d$ , which finishes the base case. Then, assuming for contradiction that there exists some other  $D = (D_1, \dots, D_m, 0, \dots, 0)$  with  $D_m \neq 0$  for which the conclusion is not satisfied, we consider the smallest such  $D$  for the colexicographic order on  $\mathbb{N}^{d+1}$ ; but then, the second assumption shows that taking

$$B(D) = \max_{0 \leq u_0, \dots, u_{m-1} \leq W(D_0, D_1, \dots, D_m, 0, \dots, 0)} B(D_0 + u_0, D_1 + u_1, \dots, D_{m-1} + u_{m-1}, D_m - 1, 0, \dots, 0) \quad (4.2)$$

does ensure  $K(D) \leq B(D)$ , a contradiction.  $\square$

There remains the matter of how the successive acceptable decompositions will be obtained.

**Proof of Theorem 1.9.** Let  $P$  be as in the assumption of Theorem 1.9, that is, let us assume that  $P(S^n)$  does not contain  $A(\mathbb{F}_p)$  for any non-constant polynomial  $A: \mathbb{F}_p \rightarrow \mathbb{F}_p$  with degree at most  $t$ . Our starting acceptable decomposition consists in writing  $P$  merely as itself: this provides a decomposition of size 1 and with degree description  $(0, \dots, 0, 1)$ .

The image  $P(S^n)$  is in particular not the whole of  $\mathbb{F}_p$ , so by Theorem 1.7, the polynomial  $P$  coincides on  $S^n$  with some polynomial of the type

$$P = Q_1 R_1 + \dots + Q_s R_s$$

for some  $s \leq H_{p,d,S}(1/2p)$  and some polynomials  $Q_1, \dots, Q_s, R_1, \dots, R_s$  satisfying

$$\deg Q_i \leq d - 1, \deg R_i \leq d - 1 \text{ and } \deg Q_i + \deg R_i \leq d$$

for each  $i \in [s]$ . This is in particular an acceptable decomposition  $(\mathcal{F}_1, F_1)$  with size at most  $2H_{p,d,S}(1/2p)$  and with degree description  $(D_0, \dots, D_{d-1}, 0)$  for some

$$D_0, \dots, D_{d-1} \leq 2H_{p,d,S}(1/2p).$$

After this, diminishing the degree description becomes more complicated, and lends itself to the inductive step that we will now describe. Assume that for some  $l \geq 1$  we have obtained an acceptable decomposition  $(\mathcal{F}_l, F_l)$  of  $P$ , and let us construct  $(\mathcal{F}_{l+1}, F_{l+1})$ . Let  $s$  be the size of the decomposition  $(\mathcal{F}_l, F_l)$ . Recall that  $e = \lfloor d/(t+1) \rfloor$ . We now distinguish three cases. Letting  $k$  be the size of  $\mathcal{F}_l$ , we may write  $\mathcal{F}_l = \{P_1, \dots, P_k\}$  for some polynomials  $P_1, \dots, P_k$ .

**Case 1:** All polynomials  $P_1, \dots, P_k$  have modified degrees at most  $e$ . Then we stop the induction.

We now assume that we are not in Case 1. Without loss of generality, we may assume that  $P_k$  has modified degree strictly greater than  $e$ , and has maximal modified degree  $m$  among the modified degrees of  $P_1, \dots, P_k$ . By gathering terms inside (4.1) depending

on the power of  $P_k$  appearing inside the term, we may hence rewrite the decomposition (4.1) as

$$P = \sum_{r=0}^t (T_r \circ (P_1, \dots, P_{k-1})) P_k^r \quad (4.3)$$

for some polynomials  $T_0, \dots, T_t : \mathbb{F}_p^{k-1} \rightarrow \mathbb{F}_p$ , such that the degree of each summand is still at most  $d$ : in particular this is why we may stop the summation at  $t$ .

**Case 2:** The image

$$(T_1 \circ (P_1, \dots, P_{k-1}), \dots, T_t \circ (P_1, \dots, P_{k-1}))(S^n)$$

is equal to  $\{0\}^t$ . Then  $P$  coincides on  $S^n$  with the polynomial  $T_0 \circ (P_1, \dots, P_{k-1})$ . This provides a new acceptable decomposition  $(\mathcal{F}_{l+1}, F_{l+1})$  of  $P$ , with  $\mathcal{F}_{l+1} = \mathcal{F}_l \setminus \{P_k\}$ . We can check that the families  $\mathcal{F}_l$  and  $\mathcal{F}_{l+1}$  satisfy items (1)–(3). We now assume that we are not in Case 2 either.

**Case 3:** Assume for contradiction that the polynomial  $P_s$  satisfies

$$\text{rk}_{m-1, S} \left( P_k - \sum_{i=1}^{k-1} a_i P_i \right) > H_{p, m, S}(|S|^{-(p-1)mk}/2p) \quad (4.4)$$

for all  $a \in \mathbb{F}_p^{k-1}$ , where we recall that  $m$  is defined as the modified degree of  $P_k$ . Because we are not in Case 2, the image

$$(T_0 \circ (P_1, \dots, P_{k-1}), T_1 \circ (P_1, \dots, P_{k-1}), \dots, T_t \circ (P_1, \dots, P_{k-1}))(S^n)$$

contains some element  $h$  of  $\mathbb{F}_p^{t+1}$  which has its  $t$  last coordinates not all equal to 0, so there exists some  $y \in \mathbb{F}_p^{k-1}$  in the image  $(P_1, \dots, P_{k-1})(S^n)$  such that  $(T_1, \dots, T_t)(y) \neq 0$ . By (4.4) and Proposition 2.1, the image  $(P_k, P_1, \dots, P_{k-1})(S^n)$  contains  $\mathbb{F}_p \times \{y\}$ , so the decomposition (4.3) shows that the image  $P(S^n)$  contains the image  $A(\mathbb{F}_p)$ , where  $A : \mathbb{F}_p \rightarrow \mathbb{F}_p$  is the polynomial defined by

$$A(u) = h_0 + h_1 u + \dots + h_t u^t.$$

By construction the polynomial  $A$  is non-constant and has degree at most  $t$ , which contradicts the assumption of Theorem 1.9. We can hence obtain some  $a \in \mathbb{F}_p^{k-1}$ , some

$$k' \leq H_{p, m, S}(|S|^{-(p-1)mk}/2p),$$

some polynomials  $P'_1, \dots, P'_k$ , each with modified degree strictly less than the modified degree  $m$  of  $P_k$  and some polynomial  $P'_0$  with degree at most  $m$  satisfying  $P'_0(S^n) = \{0\}$ ,

such that we can write

$$P_k = P'_0 + \sum_{i=1}^{k-1} a_i P_i + \sum_{i=1}^{k'} P'_i. \quad (4.5)$$

Replacing each instance of  $P_k$  by the linear combination (4.5) in the expression (4.1) (and gathering the contribution of  $P'_0$  together with  $P_0$  there) leads to a new acceptable decomposition  $(\mathcal{F}_{l+1}, F_{l+1})$  of  $P$ , where

$$\mathcal{F}_{l+1} = (\mathcal{F}_l \setminus \{P_k\}) \cup \{P'_1, \dots, P'_{k'}\}.$$

Again, the families  $\mathcal{F}_l$  and  $\mathcal{F}_{l+1}$  satisfy items (1)–(3). This concludes the inductive step.

Items (1)–(3) and Lemma 4.3 then show that there exists some integer  $\Psi(p, d, t)$  such that we can obtain an acceptable decomposition  $(\mathcal{F}, F)$  of  $P$  with size at most  $\Psi(p, d, t)$  and such that all its polynomials in  $\mathcal{F}$  have modified degree at most  $e$ . We define the quantities

$$C_{\text{pre}}(p, d, t) = \sum_{0 \leq v \leq d} \Psi(p, d, t)^v \text{ and } C(p, d, t) = p^{C_{\text{pre}}(p, d, t)}.$$

The number of products of elements of  $\mathcal{F}$  which are polynomials with degree at most  $d$  is at most  $C_{\text{pre}}(p, d, t)$ , so the number of linear combinations of them is at most  $C(p, d, t)$  and we conclude as desired that

$$\text{rk}_{e,S} P \leq C(p, d, t).$$

□

## 5. Further questions

Our results still leave open several questions regarding what we may infer about the structure of a polynomial from its range.

Let us begin by looking at degree-2 polynomials. As we discussed at the very end of the proof of Proposition 1.11, the special case of Theorem 1.7 for degree-2 polynomials, Proposition 2.11 of [10], implies in particular that there exists an absolute constant  $\kappa'' > 0$  such that if  $P$  is a degree-2 polynomial satisfying  $P(S^n) \neq \mathbb{F}_p$ , then  $\text{rk}_{1,S} P \leq \kappa'' p^5$ . We may ask whether this power bound in  $p$  may be improved to a linear bound, and even what the optimal bound is.

In the case where  $P$  has degree 1 and  $|S| \geq 2$ , the Cauchy-Davenport theorem provides an analogous bound  $\text{rk}_0 P \leq \frac{p-2}{|S|-1}$  on the size of any such polynomial (if  $|S| = 1$ , then  $\text{rk}_0 P \leq 1$  automatically). The value  $\frac{p-2}{|S|-1}$  is attained for instance for  $S = \{0, 1\}$  and

$$P = x_1 + \dots + x_{p-2}.$$

A degree-2 analogue of this example is the polynomial

$$P = x_1 x_2 + \dots + x_{2p-5} x_{2p-4},$$

which has degree-1 rank equal to  $p - 2$ . Indeed,  $P$  has rank  $2p - 4$  as a quadratic form, and it is straightforward to check that the rank of a quadratic form is at most twice its degree-1 rank. We have not found an example that would settle the following question negatively, and although this question would vaguely appear to be a kind that could potentially be approached using the combinatorial Nullstellensatz, we have not managed to use this technique to settle it positively either.

**Question 5.1.** *Let  $p$  be a prime, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . Let  $P: \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  be a degree-2 polynomial. Is it true that if  $P(S^n) \neq \mathbb{F}_p$  then  $\text{rk}_{1,S} P \leq p - 2$  ?*

More generally, we can ask for better bounds in Theorem 1.9. Even if we assume that the bounds on  $H_{p,d,S}(\epsilon)$  from Theorem 1.7 can be taken, for a fixed  $p$ , to be linear in  $\log \epsilon^{-1}$  (something which, at the time of writing, is not yet known to be true even for  $S = \mathbb{F}_p$ ), the degree-1 case ([10], Proposition 2.2) already has an inverse square dependence on  $p$ . So for any fixed degree  $3 \leq d < p$ , the number of iterations on the degree description in the proof of Theorem 1.9 would still have a worse than exponential growth rate in  $p$ , and the final bounds in Theorem 1.9 would hence be correspondingly weak.

**Question 5.2.** *Can we obtain polynomial bounds in  $p$  in Theorem 1.9 ?*

In a somewhat similar direction, we may ask whether there is some other proof of Theorem 1.9. That the proof of Theorem 1.9 in the present paper is rather short is due to the fact that it uses Theorem 1.7 as a black box: as discussed in [10], the proof of Theorem 1.7 itself uses as black boxes the facts that high partition implies high analytic rank and that high essential partition rank implies high essential disjoint partition rank, with the latter implication in the sense of [10], Definition 1.9 and [10], Theorem 1.10, which in turn was proved in [14] as a special case of [14], Theorem 1.8.

**Question 5.3.** *Does Theorem 1.9 have a purely combinatorial proof?*

As we explained in the introduction, we cannot hope, in the statement of Theorem 1.9, to obtain that if a polynomial  $P: \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  satisfies  $P(S^n) \neq \mathbb{F}_p$ , then the polynomial  $P$  coincides on  $S^n$  with the sum of a *single* polynomial of the type  $A \circ Q$  and of a polynomial determined by a bounded number of coordinates. Nonetheless, this does not mean that obtaining a variant of that description is necessarily impossible. For fixed  $1 \leq d < p$ , let  $m(p, d)$  be the smallest positive integer such that whenever  $A_1, \dots, A_m: \mathbb{F}_p \rightarrow \mathbb{F}_p$  are non-constant polynomials each with degree at most  $d$  we have

$$A_1(\mathbb{F}_p) + \dots + A_m(\mathbb{F}_p) = \mathbb{F}_p.$$

We can correspondingly formulate the most optimistic refinement of Theorem 1.9 that we may still hope for.

**Question 5.4.** *Let  $p$  be a prime, let  $1 \leq d < p$  be an integer, and let  $S$  be a non-empty subset of  $\mathbb{F}_p$ . Is it true that if  $P: \mathbb{F}_p^n \rightarrow \mathbb{F}_p$  is a polynomial with degree  $d$  satisfying*

$P(S^n) \neq \mathbb{F}_p$ , then  $P$  coincides on  $S^n$  with some polynomial of the type

$$A_1 \circ Q_1 + \cdots + A_l \circ Q_l + J$$

for some integer  $l < m$ , some polynomials  $Q_1, \dots, Q_l$  with degrees at most  $\lfloor d/2 \rfloor$ , some polynomials  $A_1, \dots, A_l : \mathbb{F}_p \rightarrow \mathbb{F}_p$  such that the polynomials  $A_1 \circ Q_1, \dots, A_l \circ Q_l$  all have degrees at most  $d$ , and some  $k$ -determined polynomial  $J$  with degree at most  $d$ , for some  $k$  that is bounded depending on  $p, d, t$  (and  $S$ ) only ?

One possibility would be to try to imitate the proof of Proposition 1.11, but it breaks down in a key way in that the obvious would-be analogue of equation (3.3) for higher degrees does not hold: unlike for  $d = 2$  it is not true for  $d \geq 3$  that if  $k$  is a positive integer, then a homogeneous polynomial of degree  $d$  in  $k$  variables can be written as a sum of at most  $k$   $d$ -powers.

We note that using the polarization identity on multilinear polynomials shows that a polynomial with degree at most  $1 \leq d < p$  and of degree- $\lfloor d/(t+1) \rfloor$  rank at most some positive integer  $r$  can always be rewritten as a linear combination of at most  $2^{dr}$  powers of polynomials with degrees at most  $d \lfloor d/(t+1) \rfloor$ . This may be viewed as going some way in establishing a result of this type, although, as is shown by the example

$$4(x_1^3 x_2 + x_3^2 x_4^2) = (x_1^3 + x_2)^2 - (x_1^3 - x_2)^2 + (x_3^2 + x_4^2)^2 - (x_3^2 - x_4^2)^2,$$

the powers may have degrees larger than the degree of the original polynomial, and this is why we have refrained from defining our notions of rank in terms of powers rather than products in Definition 1.2 and in Definition 1.6.

**Acknowledgements.** We thank Lisa Sauermann for explaining to us the proof of Lemma 2.3 in a special case already involving the main arguments of the proof of this lemma. This proof is more elegant than the proof that we would otherwise have used and furthermore provides better bounds.

## References

1. K. Adiprasito, D. Kazhdan and T. Ziegler, *On the Schmidt and analytic ranks for trilinear forms*, arXiv:2102.03659 (2021).
2. A. Akavia, S. Goldwasser and S. Safra. *Proving hard-core predicates using list decoding*, *Proceedings of the 44th IEEE Symposium on Foundations of Computer Science* (2003), 146–157.
3. A. Bhowmick and S. Lovett, *Bias vs structure of polynomials in large fields, and applications in effective algebraic geometry and coding theory*, *Electronic Colloquium on Computational Complexity, Report No. 96*. (2015).
4. A. Bhowmick and S. Lovett, *Bias vs structure of polynomials in large fields, and applications in information theory*, *IEEE Transactions on Information Theory* **69** (2022), 963–977.
5. A. Cohen and G. Moshkovitz, *Structure vs. randomness for bilinear maps*, *Discrete Analysis* **12** (2022).
6. A. Cohen and G. Moshkovitz, *Partition and analytic rank are equivalent over large fields* *Duke Mathematical Journal* **172** (2023).

7. P. Elias, *List decoding for noisy channels*, Technical report 335, Research Laboratory of Electronics, MIT (1957).
8. P. Gopalan, A. Klivans and D. Zuckerman. List decoding Reed-Muller codes over small fields, in *Proceedings 40th ACM Symposium on the Theory of Computing* pp. 265–274, (2008).
9. W. T. Gowers, *The first unknown case of polynomial DHJ*, <https://gowers.wordpress.com/2009/11/14/the-first-unknown-case-of-polynomial-dhj> (2009), Blog post.
10. W. T. Gowers and T. Karam, *Equidistribution of high-rank polynomials with variables restricted to subsets of  $\mathbb{F}_p$* , arXiv:2209.04932 (2022).
11. W. T. Gowers and J. Wolf, *Linear forms and higher-degree uniformity for functions on  $\mathbb{F}_p^n$* , *Geometric and Functional Analysis* **21** (2011), 36–69.
12. B. Green and T. Tao, *The distribution of polynomials over finite fields, with applications to the Gowers norms*, *Contributions to Discrete Mathematics* **4**(2) (2009), 1–36.
13. O. Janzer, *Polynomial bound for the partition rank vs the analytic rank of tensors*, *Discrete Analysis* **7** (2020), 1–18.
14. T. Karam, *High-rank subtensors of high-rank tensors*, arXiv:2207.08030 (2022).
15. T. Kaufman and S. Lovett. *Worst case to average case reductions for polynomials*, *49th Annual IEEE Symposium on Foundations of Computer Science* (2008), pp. 166–175.
16. S. Lovett, *The analytic rank of tensors and its applications*, *Discrete Analysis* **7** (2019), 1–10.
17. L. Milićević, *Polynomial bound for partition rank in terms of analytic rank*, *Geometric and Functional Analysis* **29** (2019), 1503–1530.
18. G. Moshkovitz and D. G. Zhu, *Quasi-linear relation between partition and analytic rank*, arXiv:2211.05780 (2022).
19. E. Nashund, *The partition rank of a tensor and  $k$ -right corners in  $\mathbb{F}_q^n$* , *Journal of Combinatorial Theory, Series A* **174** (2020), 105190.
20. R. Shaltiel and C. Umans, *Simple extractors for all min-entropies and a new pseudorandom generator*, *Journal of the ACM* **52**(2) (2005), 172–216.
21. J. Wozencraft, *List decoding. Technical Report 48:90–95*, Quarterly progress report, Research Laboratory of Electronics, MIT (1958).