Polynomial Identity Testing for Low Degree Polynomials with Optimal Randomness

Markus Bläser
Department of Computer Science, Saarland University, Saarland Informatics Campus, Saarbrücken, Germany
mblaeser@cs.uni-saarland.de

Anurag Pandey
Max Planck Institut für Informatik, Saarland Informatics Campus, Saarbrücken, Germany
apandey@mpi-inf.mpg.de

Abstract

We give a randomized polynomial time algorithm for polynomial identity testing for the class of n-variate poynomials of degree bounded by d over a field $\mathbb{F}$, in the blackbox setting.

Our algorithm works for every field $\mathbb{F}$ with $|\mathbb{F}| \geq d+1$, and uses only $d \log n + \log(1/\epsilon) + O(d \log \log n)$ random bits to achieve a success probability $1-\epsilon$ for some $\epsilon > 0$. In the low degree regime that is $d \ll n$, it hits the information theoretic lower bound and differs from it only in the lower order terms. Previous best known algorithms achieve the number of random bits (Guruswami-Xing, CCC'14 and Bshouty, ITCS'14) that are constant factor away from our bound. Like Bshouty, we use Sidon sets for our algorithm. However, we use a new construction of Sidon sets to achieve the improved bound.

We also collect two simple constructions of hitting sets with information theoretically optimal size against the class of n-variate, degree d polynomials. Our contribution is that we give new, very simple proofs for both the constructions.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory

Keywords and phrases Algebraic Complexity theory, Polynomial Identity Testing, Hitting Set, Pseudorandomness

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2020.8

Category RANDOM

Funding *Anurag Pandey*: Supported by the Chair of Raimund Seidel, Department of Computer Science, Saarland University, Saarbrücken, Germany.

Acknowledgements We thank Rohit Gurjar, Mrinal Kumar and Raimund Seidel for insightful discussions. We thank the Simons Institute for the Theory of Computing (Berkeley) and Schloss Dagstuhl – Leibniz-Zentrum für Informatik (Dagstuhl), for hosting us during certain phases of this research.

1 Introduction

We investigate algorithms for the problem of Polynomial Identity testing (PIT). Given a polynomial in some implicit representation, it asks whether the polynomial is identically zero or not. It is a fundamental problem in algorithms and complexity theory. It has found applications in algorithm design, for example in algorithms for perfect matching in graphs [17, 36, 39], for primality testing [2, 3, 4], for equivalence testing of read once branching programs [13], and for multi-set equality testing [14], and also in complexity theory, for example, in establishing some major results related to interactive proofs and probabilistically-checkable proofs [38, 9, 8, 7, 45]. In fact, it has also been discovered that an algorithm for polynomial identity testing is intimately connected with complexity theoretic lower bounds [31, 1].

In order to formalize the algorithmic problem of polynomial identity testing, it is important to specify the representation in which the polynomial is given. One possibility is that the polynomial is given as a blackbox, which means that the algorithm is restricted to using the given representation of the given polynomial only as an oracle. That is, the algorithm is only allowed to query the values of the polynomial at points of its choice. Apart from that, the algorithm only knows that the given polynomial comes from some particular class of polynomials. The other possibility is that the algorithm is also allowed to look into the representation. In this case, if the polynomial is given as a list of coefficients, the problem becomes trivial. The problem remains interesting in the case when the polynomial is given in some succinct representation, for example, either as a determinant of a given symbolic matrix, as an algebraic branching program, or more generally, as some arithmetic circuit.

It is known that randomness is necessary for a polynomial time blackbox PIT algorithm (see for example [35]). The challenge thus in this case is to find polynomial time algorithms that use optimal amount of randomness. Randomness is not known to be essential in the setting when the polynomial is given as an arithmetic circuit. In fact, it is popularly believed that there do exist polynomial time algorithms for this version of PIT which do not use randomness. More generally, it is believed that in the regime of efficient computation, randomization is not essential, that is, the complexity classes P and BPP are equal (see [30]). In this case, the challenge is to come up with a deterministic algorithm. A lot of progress has happened over the years towards both the challenges [18, 35, 32, 12, 10, 28, 27, 24, 23, 22, 6, 11, 2, 33, 15, 37, 29], however the problems are still far from the complete solution. For a history on the progress on polynomial identity testing, we refer the readers to [47, 42, 43].

In this work, we are interested in blackbox polynomial identity testing. We will focus our attention to the case when the underlying field is a finite field. More precisely, we are interested in the following computational problem.

▶ **Problem 1.** *Let $(\mathbb{F}_q, n, d)$ denote the class of multivariate polynomials over $\mathbb{F}_q$ in n variables with degree bounded by d* [1] *with $q \geq d+1$. Given a polynomial $p \in (\mathbb{F}_q, n, d)$ as a blackbox and a parameter $\epsilon > 0$, decide whether p is an identically zero polynomial in randomized $poly(n, d)$ time with success probability $1 - \epsilon$.*

We are interested in algorithms for Problem 1 which minimize the number of random bits needed to solve it. In the next subsection we discuss some previous works on the problem that are relevant to this article. While mentioning these works, we will assume the error bound ϵ to be some inverse polynomial in (nd), and we will focus only on algorithms that run in $poly(n, d)$ time under this assumption.

1.1 Previous works on Problem 1

A lot of randomized algorithms are known for PIT in the blackbox setting. The first one is the algorithm due to Schwartz-Zippel-DeMillo-Lipton [2] [44, 49, 21]. It uses $\sum_{i=1}^{n} \log(d_i + 1) + n \log n + 1$ random bits. Then came the algorithm by Lewin and Vadhan [35] which used $\sum_{i=1}^{n} \lceil \log d_i \rceil$ random bits, where d_i refers to the degree of the given polynomial with respect to the variable x_i. Using the Kronecker substitution, Agrawal and Biswas [2] gave a test with $\lceil \sum_{i=1}^{n} \log(d_i + 1) \rceil$ random bits, while Bläser-Hardt-Steurer [12] extended their Kronecker substitution based test to work for asymptotically smaller fields by using $\sum_{i=1}^{n} \log(d_i + 1) + \tilde{O}(\sqrt{\sum_{i=1}^{n} \log(d_i + 1)})$ random bits.

[1] in this paper, unless stated otherwise, degree always refers to the total degree

[2] In their paper [21], DeMillo-Lipton work with the total degree. However, implicitly, the analysis of their algorithm only assumes the individual degrees to be bounded by d.

These works achieve optimal number of random bits in the regime where individual degrees of $x_1, \ldots, x_n$ are bounded by $d_1, \ldots, d_n$ respectively. In that regime, a simple dimension argument shows a lower bound of $\log(\prod_{i=1}^{n}(d_i+1)) - \log T(n, d_1, \ldots, d_n)$, where $T(n, d_1, \ldots, d_n)$ denotes the number of queries made to the blackbox [35, Theorem 7.1]. Thus, when $T(n, d_1, \ldots, d_n)$ is $poly(n)$ bounded, we get a $(1 - o(1)) \sum_{i=1}^{n} \log(d_i + 1)$ lower bound on the number of random bits needed. However, when we are in the setting as given in Problem 1, that is, when only a bound on the total degree is given, the number of random bits used by these methods are asymptotically similar to that of Schwartz-Zippel-DeMillo-Lipton i.e. $\Omega(n \log d)$, which is far from optimal in the regime where $d \ll n$. In this regime, again using a simple dimension argument (see [35, Theorem 7.1] and Lemma 9), we have the following lower bound:

▶ **Fact 1.** *Any blackbox identity testing algorithm against $(\mathbb{F}_q, n, d)$, $q \geq d+1$ which makes $T(n,d)$ queries to the blackbox and succeeds with probability $1-\epsilon$ uses at least $\log(\binom{n+d}{d}) + \log(1/\epsilon) - \log T(n,d)$ random bits.*

Applying Stirling's approximation on $\binom{n+d}{d}$ in the above when $d = o(n)$ gives $\log(\binom{n+d}{d}) = (1+o(1))d\log(\frac{n+d}{d}) = d\log n + o(d\log n)$ [20]. Plugging this in above, with $T(n,d) = (nd)^{O(1)}$, we get the lower bound of $d\log n + \log(1/\epsilon) + o(d\log n)$.[3]

Moving on to the previous works when $d \ll n$, several algorithms are known that actually do achieve the $O(d \log n)$ random bits. For instance, Klivans-Spielman [32], Bogdanov [15], Shpilka-Volkovich generator [46], Lu [37], Guruswami-Xing [29] and finally Bshouty [16] (also see Cohen-Ta-Shma [19]). However, except for [29] and [16], all of them require the field size to be superlinear in d/ϵ as a pre-condition for the algorithm. Moreover, in all of these algorithms including the ones in Bshouty [16] and Guruswami-Xing [29], the number of random bits used is $\geq 2d \log n$.

1.2 Our contributions and methods

From the above, we can see that in the low-degree regime, the number of random bits needed by all the previously discovered algorithms, is away from the information theoretically optimal bound at least by a constant multiplicative factor. We take up the challenge and solve it. We give an algorithm that matches the information theoretic lower bound differing from it only in the lower order terms.

More precisely, we show the following:

▶ **Theorem 1.** *Given a polynomial $f \in (\mathbb{F}_q, n, d)$ with $q \geq d+1$ as a blackbox, and a parameter $\epsilon > 0$, there exists a randomized $poly(n,d)$ time algorithm which uses $d\log n + \log(1/\epsilon) + O(d \log\log n)$ random bits and outputs whether f is an identically zero polynomial with success probability $1-\epsilon$.*

Starting point of our algorithm is an algorithm given in Bshouty [16]. He used the so-called Sidon sets (discussed in Section 2.1) for polynomial identity testing by using them to reduce the problem to the univariate setting while preserving the nonzeroness. He then used the obvious randomized algorithm for the obtained univariate polynomial. This, however, requires the field-size to be large. He gets around this problem by inventing the concepts of testers (discussed in Section 2.2). Informally, testers take a point α from a field $\mathbb{F}$ and map it to a bunch of points in a smaller subfield of $\mathbb{F}$, while maintaining the property that if $f(\alpha) \neq 0$, then f will evaluate to a nonzero value on at least one of the points given by the tester.

[3] this is what we refer to as the information theoretic lower bound in this article

He used two constructions for Sidon sets for this purpose. One of them is not known to be poly time constructible, while the other, which is poly time constructible is factor 2 away from the information theoretic lower bound. To overcome this, we use a new, elementary construction of Sidon sets that is mentioned in Timothy Gowers' weblog [26] (presented in Section 2.1).

Our second contribution is aesthetic in nature. We first remind the readers that a hitting set against a class $\mathcal{P} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ is a set of point $\mathcal{H} \subseteq \mathbb{F}^n$ such that no nonzero polynomial in $\mathcal{P}$ evaluates to zero on all the points in $\mathcal{H}$. We present two simple constructions of information theoretically optimal hitting sets (i.e. of size $\binom{n+d}{d}$) against $(\mathbb{F}, n, d)$ with $|\mathbb{F}| \geq d+1$ that are, at least implicitly, present in the literature. We extract them out and give very simple and neat proofs for both. The first construction (presented in Section 3.1) is essentially the set of exponent vectors of all the monomials spanning $(\mathbb{F}, n, d)$. This works when $\{0, 1, \ldots, d\} \subseteq \mathbb{F}$. The second construction (presented in Section 3.2) says that taking all the intersection points of n-sized subsets of a set of $n+d$ hyperplanes in general position also forms a hitting set against $(\mathbb{F}, n, d)$ of optimal size.

In the rest of the paper, $(\mathbb{F}, n, d)$ (resp. $(\mathbb{F}_q, n, d)$) denotes the class of n-variate polynomials with degree bounded by d over $\mathbb{F}$ (resp. $\mathbb{F}_q$). For a natural number $d \in \mathbb{N}$, $[d]$ denotes the set $\{1, \ldots, d\}$.

2 Polynomial Identity Testing with optimal randomness

In this section, we present our main result. We first describe the main component of the proof, that is, the construction of Sidon sets in Section 2.1, and then describe the way to reduce the field size in Section 2.2. We finally give our algorithm and the proof for our main theorem in Section 2.3.

2.1 Sidon Sets

A set $\mathcal{S} := \{s_1, s_2, \ldots, s_n\} \subset \mathbb{Z}_{\geq 0}$ is said to be a Sidon B_d set if every element in the set $d\mathcal{S} := \{s_{i_1} + s_{i_2} + \ldots + s_{i_d} \mid \forall k \in [d], s_{i_k} \in \mathcal{S}\}$ are distinct up to rearrangements of the summands. We also have a stronger notion: we call $\mathcal{S}$ to be Sidon $B_{\leq d}$ set if the sums $\{s_{i_1} + s_{i_2} + \ldots + s_{i_r},\ r \leq d \mid \forall k \in [r], s_{i_k} \in \mathcal{S}\}$ are distinct up to rearrangements of the summands. For our purposes, the stronger notion of Sidon $B_{\leq d}$ set when $d \ll n$ will be useful. We are interested in constructions that minimize the size of the maximum element of $\mathcal{S}$ and are $poly(n, d)$ time constructible.

Sidon sets and its variants have a long history in mathematics and several explicit constructions are known. We refer the readers to a survey by Kevin O'Bryant [40].

In complexity theory, explicit Sidon set constructions have also been used, for example, by Bshouty for constructions of hitting sets for black box polynomial identity testing [16], and by Kumar and Volk for matrix factorization lower bounds [34].

Bshouty uses two constructions for polynomial identity testing. The first construction uses discrete log and is not known to be poly time constructible [16, Lemma 59]. The second construction is poly time constructible, but the value of the maximum element is $(2nd)^{2d}$ [16, Lemma 60]. This $2d$ in the exponent makes this construction suboptimal for our purposes because the resulting randomized PIT algorithm will have $\geq 2d \log n$ random bits, which is factor 2 away from the information theoretic bound in low degree regime which is the regime of interest in this paper.

This motivated us to look for constructions that are both polynomial time constructible and also give rises to PIT algorithm with optimal randomness. That is when we stumbled across the weblog of Timothy Gowers about the so-called dense Sidon sets [26] where he describes the idea of a construction by Imre Z. Ruzsa [41] that scales up for our purposes too.

In its core, the construction is based on the fundamental theorem of arithmetic. Informally, when we take a set of primes and consider two different multi-subsets of them. Then the product of elements will be different for the two multi-subsets. Now taking logarithm of products convert them to sums. These simple facts along with the mean value theorem constitute the ingredients of the proof of the construction. We give the construction now.

▶ **Theorem 2.** *For every n, d, there exists a poly(n, d) time constructible Sidon $B_{\leq d}$ set $S_{n,d} := \{b_1, \ldots, b_n\} \subset \mathbb{N}$ with $b_1 < b_2 < \cdots < b_n$, with $b_n \leq \lceil (d+1) \cdot (2n \log n)^d \cdot \log(2n \log n) \rceil$.*

Proof. We take the first n primes $p_1, \ldots, p_n$. By prime number theorem, we know that $p_n < n(\log n + \log \log n) < 2n \log n$. Let $I, J \subseteq \{1, \ldots, n\}$ be multisets, where $|I|, |J| \leq d$, $I \neq J$. By the fundamental theorem of arithmetic, we have $\prod_{i \in I} p_i \neq \prod_{j \in J} p_j$. Without loss of generality, we can assume that $\prod_{i \in I} p_i < \prod_{j \in J} p_j$, that is, $\prod_{i \in I} p_i \leq \prod_{j \in J} p_j + 1$. Now applying the mean value theorem on the function $f(x) = \log x$ in the interval $[a, b]$ with $a := \prod_{i \in I} p_i$ and $b := \prod_{j \in J} p_j$, we get that

$$\sum_{j \in J} \ell_j - \sum_{i \in I} \ell_i = \frac{1}{c} \left(\prod_{j \in J} p_j - \prod_{i \in I} p_i \right), \text{ for some } c \in (a, b), \text{ where } \ell_k := \log p_k.$$

The numerator in the RHS of the equation is at least 1, while the denominator is upper bounded by $b = \prod_{j \in J} p_j$. Thus, we have

$$\sum_{j \in J} \ell_j - \sum_{i \in I} \ell_i \geq \frac{1}{\prod_{j \in J} p_j}. \tag{1}$$

Thus, if we choose the set to be set of logarithm of the first n primes, we do get, that for distinct multi-subsets of size at most d, the sum of elements are also distinct. However, clearly, the elements and their differences will not be all integers. But the above calculation is suggestive of what the set should be. Note that in Equation (1), the denominator of the RHS, that is, $\prod_{j \in J} p_j$ is upper bounded by $(2n \log n)^d$, Thus,

$$\sum_{j \in J} (d+1) \cdot \ell_j \cdot (2n \log n)^d - \sum_{i \in I} (d+1) \cdot \ell_i \cdot (2n \log n)^d \geq d + 1$$

Now, if we consider the set $\mathcal{S}_{n,d}$ of size n with elements being positive integers $b_k := \lceil (d+1) \cdot \ell_k \cdot (2n \log n)^d \rceil$ of size n, we have that $\sum_{j \in J} b_j - \sum_{i \in I} b_i > 0$. Thus, $\mathcal{S}_{n,d}$ is a Sidon $B_{\leq d}$ set.

It only remains to argue that the construction can be done in $poly(n, d)$ time. We need to show that all the $b_k = \lceil (d+1) \cdot \log p_k \cdot (2n \log n)^d \rceil$ are $poly(n, d)$ time constructible, It is known that the first n primes are easily constructible, for example, by using Sieve of Eratosthenes which takes $O(n \log \log n)$ time. The other functions like log and powering function are also known to be efficiently computable to the desired precision. ◀

We now present the concept useful for transferring a polynomial identity testing algorithm over a large field to an algorithm for a small subfield of it.

2.2 Testers

The notion of testers is also crucial for our algorithm. They were introduced by Bshouty in [16]. He also used it for several applications including in the setting of blackbox PIT. We will be using it in the same fashion as he did i.e. to reduce the field size of the blackbox PIT set that we would be using for the algorithm. We present the definition of testers restricted to the setting that we need. He defined it for a more general setting.

▶ **Definition 3.** *Let $\mathbb{F}_q$ be a finite field with q elements and let $\mathbb{F}_{q^{t_1}}$ and $\mathbb{F}_{q^{t_2}}$ be two field extensions of $\mathbb{F}_q$ viewed as $\mathbb{F}_q$-algebras with $t_1 \geq t_2$, and let $\mathcal{P} \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ be a class of multivariate polynomials. Let $L = \{\ell_1, \ldots, \ell_\nu\}$ be a set of maps $\mathbb{F}_{q^{t_1}}^n \to \mathbb{F}_{q^{t_2}}^n$. For $f \in \mathcal{P}$, we denote by fL the map $\mathbb{F}_{q^{t_1}}^n \to \mathbb{F}_{q^{t_2}}^\nu$ defined as: for $\boldsymbol{a} \in \mathbb{F}_{q^{t_1}}^n$, $(fL)(\boldsymbol{a}) = (f(\ell_1(\boldsymbol{a})), \ldots, f(\ell_\nu(\boldsymbol{a})))$. We say that L is an $(\mathcal{P}, \mathbb{F}_{q^{t_1}}, \mathbb{F}_{q^{t_2}})$-tester if for every $\boldsymbol{a} \in \mathbb{F}_{q^{t_1}}^n$ and $f \in \mathcal{P}$ we have*

$$(fL)(\boldsymbol{a}) = \boldsymbol{0} \implies f(\boldsymbol{a}) = 0.$$

The size of the tester L is defined as $|L| = \nu$, the number of maps constituting L.

So, essentially, a tester L for the class of polynomials $\mathcal{P}$ is a set of maps from a field to its subfield such that for every point on which a polynomial $f \in \mathcal{P}$ evaluates to a nonzero value, the tester gives a set of points in the subfield such that the polynomial evaluates to a nonzero value on at least one of the points given by the tester.

Hence a tester is very useful for reducing a blacbox PIT set over a bigger field to a blackbox PIT set over a smaller field while incurring a blowup by the size of the tester. Bshouty [16] also gave many constructions of testers against several classes of multivariate polynomials which helped him achieve constructions of hitting sets which are optimal with respect to the field size and the size of hitting sets.

The tester that is relevant to our purposes which we will be using as a blackbox has the following property. For a proof we refer the readers to [16].

▶ **Lemma 4** ([16], Theorem 40)**.** *Let $\mathcal{P} := (\mathbb{F}_q, n, d) \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ denote the class of n-variate, degree d polynomials over $\mathbb{F}_q$, with $q \geq d + 1$. Then, for every n, d, t, there exists a $(\mathcal{P}, \mathbb{F}_{q^t}, \mathbb{F}_q)$-tester L of size $O(d^5 t)$ that can be constructed in $poly(n, d, t)$ time.*

The above lemma clearly suggests a strategy for construction of blackbox PIT sets: first design a blackbox PIT set over a large extension field and then reduce the field size to $d + 1$ using the tester promised by the above lemma.

2.3 The algorithm: Proof of Theorem 1

In this section, we present our randomized algorithm for polynomial identity testing and prove Theorem 1.

Before we prove the theorem, we state a simple lemma about univariate polynomials that we will need in the proof.

▶ **Lemma 5.** *Let $f \in \mathbb{F}_q[x]$ be a nonzero univariate polynomial whose degree is bounded by d. Let $\mathbb{F}_{q^t}$ be an extension field of $\mathbb{F}_q$ such that $|\mathbb{F}_{q^t}| \geq d/\epsilon$ and $\boldsymbol{a}$ is sampled uniformly at random from $\mathbb{F}_{q^t}$, then $f(\boldsymbol{a}) \neq 0$ with probability $1 - \epsilon$.*

Lemma 5 follows from the folklore theorem that a univariate polynomial of degree d over a field $\mathbb{F}_q$ has at most d roots in any field extension $\mathbb{F}_{q^t}$ of $\mathbb{F}_q$.

We are now ready to prove Theorem 1.

▶ **Theorem 6** (Theorem 1 restated)**.** *Given a polynomial $f \in (\mathbb{F}_q, n, d)$ with $q \geq d + 1$ as a blackbox or as a $poly(n, d)$-sized arithmetic circuit, and $\epsilon > 0$, there exists a randomized $poly(n, d)$ time algorithm which uses $d \log n + \log(1/\epsilon) + O(d \log \log n)$ random bits and succeeds with probability $1 - \epsilon$.*

Proof. Suppose we are given a polynomial $f \in (\mathbb{F}_q, n, d)$ as a blackbox. To test whether the given polynomial is an identically zero polynomial or not, our algorithm works as follows:

Step 1. Construct Sidon set: Given n, d, we construct a Sidon $B_{\leq d}$ set $\mathcal{S}_{n,d} = \{b_1, \ldots, b_n\}$ using the construction in Theorem 2.

Step 2. Pick a random point from large field: We pick a random point α from the field $\mathbb{F}_{q^t}$ with $t = \lceil \log_q((b_n d)/\epsilon) \rceil$.

Step 3. Construct the tester: Next we construct a $(\mathcal{P}, \mathbb{F}_{q^t}, \mathbb{F}_q)$-tester, $L = \{\ell_1, \ldots, \ell_\nu\}$, for $\mathcal{P} = (\mathbb{F}_q, n, d)$ and $t = \lceil \log_q((b_n d)/\epsilon) \rceil$ using the construction promised by Lemma 4.

Step 4. Reduce the field size by testers: We then apply the tester L on $(\alpha^{b_1}, \ldots, \alpha^{b_n}) \in \mathbb{F}_{q^t}^n$ to get the set of points $\ell_1(\alpha^{b_1}, \ldots, \alpha^{b_n}), \ldots, \ell_\nu(\alpha^{b_1}, \ldots, \alpha^{b_n}) \in \mathbb{F}_q^n$.

Step 5. Evaluate: We evaluate f on $\ell_1(\alpha^{b_1}, \ldots, \alpha^{b_n}), \ldots, \ell_\nu(\alpha^{b_1}, \ldots, \alpha^{b_n}) \in \mathbb{F}_q^n$. If f evaluates to zero on $\ell_k(\alpha^{b_1}, \ldots, \alpha^{b_n})$, for every $k \in 1, \ldots, \nu$, we output that f is an identically zero polynomial. Otherwise we output that f is not a zero polynomial.

We now show the correctness of the above algorithm. The Sidon $B_{\leq d}$ set $\mathcal{S}_{n,d} = \{b_1, \ldots, b_n\}$, $b_1 < b_2 < \cdots < b_n$ and $b_n = \lceil (d+1) \cdot (2n \log n)^d \cdot \log(2n \log n) \rceil$ from Theorem 2 is used to reduce the problem to the univariate case. It is also $poly(n, d)$ time constructible. By the definition of Sidon $B_{\leq d}$ set in Section 2.1, it follows that for distinct multi-subsets of $\mathcal{S}_{n,d}$, the sum of elements will also be distinct. Thus, the map $(x_1, x_2, \ldots, x_n) \mapsto (x^{b_1}, x^{b_2}, \ldots, x^{b_n})$ maps the monomials of the degree at most d in the variables $x_1, \ldots, x_n$ to distinct univariate monomials in x. In particular, every nonzero polynomial $f \in (\mathbb{F}_q, n, d)$ maps to a nonzero polynomial $g \in (\mathbb{F}_q, 1, b_n d)$. Thus, g is a polynomial of degree bounded by $b_n d$.

Now, by Lemma 5, on a randomly chosen point α from the extension field $\mathbb{F}_{q^t}$ with $|\mathbb{F}_{q^t}| \geq (b_n d)/\epsilon$, g will evaluate to a nonzero value with probability $\geq 1 - \epsilon$. Hence, f will evaluate to a non-zero value on $(\alpha^{b_1}, \ldots, \alpha^{b_n})$ with probability $\geq 1 - \epsilon$. The number of random bits needed is $\log((b_n d)/\epsilon) = \log b_n + \log d + \log(1/\epsilon) = d \log n + O(d \log \log n) + \log(1/\epsilon)$ as claimed.

Finally we use an $((\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-tester from Lemma 4 on $(\alpha^{b_1}, \ldots, \alpha^{b_n}) \in \mathbb{F}_{q^t}^n$ to get the set of points $\ell_1(\alpha^{b_1}, \ldots, \alpha^{b_n}), \ldots, \ell_\nu(\alpha^{b_1}, \ldots, \alpha^{b_n}) \in \mathbb{F}_q^n$. By Lemma 4, the number of points $\nu = O(d^5 t) = O(d^5(\log(b_n d) + \log(1/\epsilon))) = O(d^6(\log n + \log 1/\epsilon))$ and time to construct the tester is $poly(n, d, t) = poly(n, d, \log 1/\epsilon)$. By the definition of testers from Definition 3, for a nonzero polynomial $f \in (\mathbb{F}_q, n, d)$, if $f(\alpha^{b_1}, \ldots, \alpha^{b_n}) \neq 0$, then at least one of $f(\ell_1(\alpha^{b_1}, \ldots, \alpha^{b_n})), \ldots, f(\ell_\nu(\alpha^{b_1}, \ldots, \alpha^{b_n}))$ also evaluates to a nonzero value. Thus, we get the desired result. ◀

▶ Remark 7. When $d = o(\log n)$, we can get an improvement on the number of random bits from $d \log n + d \log \log n +$ lower order terms (as in Theorem 1) to $d \log n + d \log d +$ lower order terms. This can be achieved by adapting an idea due to Goldwasser-Grossman [25, Lemma 8] that they used to construct weight assignments to get unique min-weight perfect matching. Their idea suggests a map $(x_1, x_2, \ldots, x_n) \mapsto (x^{b_1}, x^{b_2}, \ldots, x^{b_n})$, where $b_i = [i]_p + (pd)[i^2]_p + (pd)^2[i^3]_p + \cdots + (pd)^d[i^{d+1}]_p$, where $[x]_p$ denotes the number between 0 and $p-1$ which is equal to x modulo p, and p is a prime number greater than n. This map can replace the map due to Sidon Sets in the Step 1 from the above proof, while the rest of the algorithm and the proof remains the same. As in the above proof of Theorem 1, the number of random bits needed equals $\log b_n + \log d + \log(\frac{1}{\epsilon})$ which becomes $d \log n + d \log d +$ lower order terms. For the correctness of this map, we refer the reader to the proof of Lemma 8 in [25].

▶ Remark 8. Our algorithm works for fields of zero characteristic as well. In fact, whenever the field size is already larger than $(b_n d)/\epsilon$, we do not need Step 3 and Step 4, and we can directly evaluate f on $(\alpha^{b_1}, \ldots, \alpha^{b_n})$ in Step 5. Thus, we have an algorithm for blackbox polynomial identity testing which uses information theoretically optimal number of random bits for all fields $\mathbb{F}$ with $|\mathbb{F}| \geq d + 1$.

3 Optimal Hitting sets

In this section, we describe a few optimal hitting sets, i.e. the ones that exactly matches with the lower bound against the class of n-variate polynomials with total degree bounded by d. The authors are excited about these proofs because of their simplicity and elegance.

We first begin by stating the straight-forward folklore lower bound.

▶ **Lemma 9.** *For any hitting set $\mathcal{H}$ against the class n-variate polynomials with total degree bounded by d over a field $\mathbb{F}$, we have $|\mathcal{H}| \geq \binom{n+d}{d}$.*

This follows by the fact that the set of all n-variate polynomials with total degree bounded by d over a field $\mathbb{F}$ forms a vector space of dimension $\binom{n+d}{d}$. This is true because the number of monomials supported on n-variables with total degree bounded by d is $\binom{n+d}{d}$, and they form the basis for the vector space as they are all $\mathbb{F}$-linearly independent, and all polynomials in the set can be represented as an $\mathbb{F}$-linear combination of them. Thus, in the worst case, one needs to query f on at least $\binom{n+d}{d}$ points.

We now consider a very popular construction which is suboptimal for our purposes.

Construction 0 – Schwartz-Zippel-DeMillo-Lipton lemma: As a consequence of the Lemma [44, 49, 21], for $(\mathbb{F}, n, d)$, one gets the hitting set $\mathcal{H}_0 := S^n$ where $S \subseteq \mathbb{F}$, with $|S| = d + 1$, which is the grid of size $(d+1)^n$. We point out that this is optimal when we are considering the set of n-variate polynomials with *individual degrees* of each variable bounded by d, by a similar argument as in Lemma 9. However, this is not optimal for $(\mathbb{F}, n, d)$ where we bound the *total degree*. Especially when $d \ll n$, the gap is huge.

Thus, it makes sense to investigate optimal hitting sets for $(\mathbb{F}, n, d)$. In what follows, we present two such constructions for the hitting set. They were both, at least implicitly, already present in the literature. We also believe that other constructions can be found without much effort. However our predilection towards these constructions and our new proofs is purely aesthetic.

3.1 Construction 1: The set of exponent vectors

The lower bound tells that any hitting set $\mathcal{H}$ should have size at least $\binom{n+d}{d}$. Now this $\binom{n+d}{d}$ comes from the number of monomials in n variables of degree at most d. Very interestingly, when $\{0, 1, \ldots, d\} \subseteq \mathbb{F}$, these monomials also suggest a set of points of size $\binom{n+d}{d}$ that can be seen as a potential hitting set: simply collect all the exponent vectors of all the monomials in a set, viewing them as points in $\mathbb{F}^n$, that is, the suggested set is $\mathcal{H}_1 := \{(x_1, \ldots, x_n) \in \{0, 1, \ldots, d\}^n \mid x_1 + x_2 + \cdots + x_n \leq d\}$. The above construction obviously requires that $\mathbb{F}^n$ indeed contains $\mathcal{H}_1$ as a subset. Surprisingly to some, and beautifully to the authors, this indeed works. This was shown by Bshouty [16, Lemma 77] using Combinatorial Nullstellensatz [5].

In this work, we give a direct inductive proof which we found with Mrinal Kumar. It bypasses the combinatorial nullstellensatz and flows along the lines of the proof of Schwartz-Zippel-DeMillo-Lipton lemma. We are suprised that we did not find this proof somewhere in the literature.

▶ **Theorem 10.** *If $\{0, 1, \ldots, d\} \subseteq \mathbb{F}$, then the set $\mathcal{H}_1 := \{(x_1, \ldots, x_n) \in \{0, 1, \ldots, d\}^n \mid x_1 + x_2 + \cdots + x_n \leq d\}$, is a hitting set for $(\mathbb{F}, n, d)$.*

Proof. Consider the integral grid $\mathcal{G} := \{0, 1, \dots d\}^n$ with $|\mathcal{G}| = (d+1)^n$. Now the statement of the theorem can be rephrased as: for every nonzero polynomial $f \in (\mathbb{F}, n, d)$, there exists a point $g \in \mathcal{G}$ with its ℓ_1-norm $\|g\|_1 \leq d$, such that $f(g) \neq 0$. We use this as our induction hypothesis and prove it by induction on the number of variables n.

For $n = 1$, that is the univariate case, this holds true because every degree d polynomial has at most d zeros. Suppose the hypothesis holds for $n-1$. For the inductive step, write a nonzero $f \in (\mathbb{F}, n, d)$ as a univariate in x_n as $f = \sum_{i=1}^{d'} P_i(x_1, \dots, x_{n-1}) x_n^i$, where d' is the maximum degree of f in x_n and $P_i(x_1, \dots, x_{n-1})$ are the coefficients coming from $\mathbb{F}[x_1, \dots, x_{n-1}]$. Now consider $P_{d'}(x_1, \dots, x_{n-1})$ which is the coefficient of the highest degree term in x_n. If f is a nonzero polynomial, then so is $P_{d'}(x_1, \dots, x_{n-1})$. Also, $\deg(P_{d'})$ is bounded by $d - d'$. By the induction hypothesis, there is a point s' in the grid $\mathcal{G}' := \{0, 1, \dots, d - d'\}^{n-1}$ with $\|s'\|_1 \leq d - d'$ such that $P_{d'}(s') \neq 0$. Now we fix $x_1, \dots, x_{n-1}$ to the values as given by s'. Now $P_{d'}$ restricted to the assignment s' is a univariate polynomial in x_n of degree d'. Thus, setting x_n to a value in $\{0, 1, \dots d'\}$ gives a point on which f evaluates to nonzero. The ℓ_1 norm of the point is at most $(d - d') + d' = d$. ◀

We now give another construction which we find beautiful.

3.2 Construction 2: Intersection of hyperplanes in general position

The construction is as follows: In the projective space $\mathbb{P}^n(\mathbb{F})$ over a field $\mathbb{F}$, with $|\mathbb{F}| \geq d + 1$, take a collection $\mathcal{C}$ of $n + d$ hyperplanes in general position i.e. every size n subsets of $\mathcal{C}$ intersect in a point, whereas no size $n + 1$ subset of $\mathcal{C}$ intersect. Now all intersection points of n-sized subset of $\mathcal{C}$ gives the desired hitting set.

We now mention a standard explicit family of hyperplanes in general position.

▶ **Example 11.** Take hyperplanes $H_1, \dots, H_{n+d}$ in the projective space $\mathbb{P}^n$ where H_i is given by the equation $t_i^1 x_1 + t_i^2 x_2 + \cdots + t_i^n x_n + x_{n+1} = 0$, where $t_i \in \mathbb{F}$. Then, $H_1, \dots, H_{n+d}$ are hyperplanes in general position.

Itaï Ben Yaacov [48] considers hyperplanes in general position and gives an algebraic proof of a generalized Vandermonde Identity in higher dimension. What his identity implies is that taking all intersection points of n-sized subsets of $n+d$ hyperplanes in general position gives a hitting set for $(\mathbb{F}, n, d)$.

In order to state his result, we need some notations. Let $M_{p\times q}(\mathbb{F})$ denote the set of all $p \times q$ matrices over $\mathbb{F}$. He defines the following three maps. It useful to think that the $(n+1) \times m$ matrix Q is denoting the family of m hyperplanes, say $\mathcal{H}_m$ in $\mathbb{P}^n$, i.e. the entries of each column correspond to the coefficients of a hyperplane.

- **i)** $\mu : M_{(n+1)\times m}(\mathbb{F}) \to M_{(n+1)\times \binom{m}{n}}(\mathbb{F})$ sends an $(n+1) \times m$ matrix Q to a matrix P whose entries are all the minors of Q of order n. Note that a lexicographic ordering on the chosen sequence of rows and columns of Q induces an ordering on the minors as well. By Cramer's rule from linear algebra, P is precisely the matrix of intersection points of all n-sized subsets of $\mathcal{H}_m$, where each column of Q has the coordinates of an intersection point as its entries.
- **ii)** $\delta : M_{(n+1)\times m}(\mathbb{F}) \to \mathbb{F}$ sends an $(n+1) \times m$ matrix Q to the product of all its minors of order $n + 1$.
- **iii)** $\nu_r : M_{(n+1)\times m}(\mathbb{F}) \to M_{\binom{n+r}{n}\times m}(\mathbb{F})$ applies the Veronese map on each column i.e. for each column, it applies all the n-variate degree r monomials on the entries of the column. Assume an ordering (say, inverse lexicographical ordering) on the monomials.

We are now ready to quote the generalized Vandermonde identity in higher dimension.

▶ **Theorem 12** ([48], Theorem 1.4)**.** *Let R be a commutative ring. $n \leq m \in \mathbb{N}$, and let Q be a $(n+1) \times m$ matrix over R. Then $\nu_{m-n}\mu Q$ is a square matrix of order $\binom{m}{n}$, and the following Vandermonde identity of order m in dimension n holds:*

$$\det(\nu_{m-n}\mu Q) = (\delta Q)^n$$

Then the above theorem with $m = n + d$, implies that if $(\delta Q) \neq 0$, which is the algebraic condition for the $n + d$ hyperplanes to be in general position, then $\det(\nu_{n+d-n}\mu Q) \neq 0$. Now $\nu_{m-n}\mu Q$ is the matrix with Veronese map applied on the intersection points of n-sized subsets of m hyperplanes. Normalizing the coordinates by the last coordinate gives us the points in the affine setting with the Veronese maps essentially applying all the monomials of degree at most d on the points. Thus, $\det(\nu_d \mu Q) \neq 0$ means that the set of intersection points form a hitting set against $(\mathbb{F}, n, d)$.

We now present a direct, simple, geometric proof of the construction which we found with Raimund Seidel.

▶ **Theorem 13.** *Let $H_1, \ldots, H_{n+d}$ be hyperplanes in general position. If $f \in (\mathbb{F}, n, d)$ vanishes on all the points obtained by intersecting all n-sized subsets of $\{H_1, \ldots, H_{n+d}\}$, then f is an identically zero polynomial.*

Proof. We prove the above statement by induction on the number of variables n. The base case $n = 1$ is the univariate case and the hyperplanes become $d+1$ points, and the statement of the lemma reduces to f vanishing on $d+1$ points. Thus, the statement holds in this case because a degree d univariate polynomial that vanishes on $d+1$ points is an identically zero polynomial.

Suppose that the statement holds for the number of variables up to $n-1$, and we assume an $f \in (\mathbb{F}, n, d)$ that vanishes on all the intersection points of n-sized subsets of $\{H_1, \ldots, H_{n+d}\}$. The assumption, in particular, implies that f restricted to the hyperplane H_1 vanishes on all the intersection points of $(n-1)$-sized subsets of $\{H_2, \ldots, H_{n+d}\}$. However, note that f restricted to H_1 reduces to an $(n-1)$-variate case and hence we can apply the induction hypothesis and conclude that f restricted to H_1 is identically zero. Doing the same for all the hyperplanes, we get that f restricted to all the hyperplanes $H_1, \ldots, H_{n+d}$ is identically zero. It remains to conclude that f is indeed identically zero. For this, restrict f to a generic line ℓ. Note that $H_1, \ldots, H_{n+d}$ all intersect ℓ at distinct points. Thus, f restricted to ℓ is a univariate which vanishes on $n + d$ points, hence f restricted to a generic ℓ is identically zero. Hence f is identically zero. ◀

Note that an explicit construction corresponding to Theorem 13 can be obtained using the family given in Example 11.

References

1 Manindra Agrawal. Proving lower bounds via pseudo-random generators. In *FSTTCS 2005: Foundations of software technology and theoretical computer science*, volume 3821 of *Lecture Notes in Comput. Sci.*, pages 92–105. Springer, Berlin, 2005. doi:10.1007/11590156_6.

2 Manindra Agrawal and Somenath Biswas. Primality and identity testing via Chinese remaindering. *J. ACM*, 50(4):429–443, 2003. doi:10.1145/792538.792540.

3 Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. of Math. (2)*, 160(2):781–793, 2004. doi:10.4007/annals.2004.160.781.

4 Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Errata: PRIMES is in P. *Ann. of Math. (2)*, 189(1):317–318, 2019. doi:10.4007/annals.2019.189.1.6.

5 NOGA ALON. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999. doi:10.1017/S0963548398003411.

6 Matthew Anderson, Michael A. Forbes, Ramprasad Saptharishi, Amir Shpilka, and Ben Lee Volk. Identity testing and lower bounds for read-k oblivious algebraic branching programs. In *31st Conference on Computational Complexity*, volume 50 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 30, 25. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2016.

7 Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998. doi:10.1145/278298.278306.

8 Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: a new characterization of NP. *J. ACM*, 45(1):70–122, 1998. doi:10.1145/273865.273901.

9 László Babai, Lance Fortnow, and Carsten Lund. Nondeterministic exponential time has two-prover interactive protocols. In *31st Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990)*, pages 16–25. IEEE Comput. Soc. Press, Los Alamitos, CA, 1990. doi:10.1109/FSCS.1990.89520.

10 Markus Bläser and Christian Engels. Randomness efficient testing of sparse black box identities of unbounded degree over the reals. In *28th International Symposium on Theoretical Aspects of Computer Science*, volume 9 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 555–566. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2011.

11 Markus Bläser, Moritz Hardt, Richard J. Lipton, and Nisheeth K. Vishnoi. Deterministically testing sparse polynomial identities of unbounded degree. *Inform. Process. Lett.*, 109(3):187–192, 2009. doi:10.1016/j.ipl.2008.09.029.

12 Markus Bläser, Moritz Hardt, and David Steurer. Asymptotically optimal hitting sets against polynomials. In *Automata, languages and programming. Part I*, volume 5125 of *Lecture Notes in Comput. Sci.*, pages 345–356. Springer, Berlin, 2008. doi:10.1007/978-3-540-70575-8_29.

13 Manuel Blum, Ashok K. Chandra, and Mark N. Wegman. Equivalence of free Boolean graphs can be decided probabilistically in polynomial time. *Inform. Process. Lett.*, 10(2):80–82, 1980. doi:10.1016/S0020-0190(80)90078-2.

14 Manuel Blum and Sampath Kannan. Designing programs that check their work. *J. ACM*, 42(1):269–291, January 1995. doi:10.1145/200836.200880.

15 Andrej Bogdanov. Pseudorandom generators for low degree polynomials. In *STOC'05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 21–30. ACM, New York, 2005. doi:10.1145/1060590.1060594.

16 Nader H. Bshouty. Testers and their applications. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:11, 2012. URL: http://eccc.hpi-web.de/report/2012/011.

17 Suresh Chari, Pankaj Rohatgi, and Aravind Srinivasan. Randomness-optimal unique element isolation with applications to perfect matching and related problems. *SIAM J. Comput.*, 24(5):1036–1050, 1995. doi:10.1137/S0097539793250330.

18 Zhi-Zhong Chen and Ming-Yang Kao. Reducing randomness via irrational numbers. In *STOC '97 (El Paso, TX)*, pages 200–209. ACM, New York, 1999.

19 Gil Cohen and Amnon Ta-Shma. Pseudorandom generators for low degree polynomials from algebraic geometry codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:155, 2013. URL: http://eccc.hpi-web.de/report/2013/155.

20 Shagnik Das. A brief note on estimates of binomial coefficients. http://page.mi.fu-berlin.de/shagnik/notes/binomials.pdf. Accessed on 2020-02-18.

21 Richard A. DeMillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Inf. Process. Lett.*, 7(4):193–195, 1978. doi:10.1016/0020-0190(78)90067-4.

22 Michael A. Forbes, Sumanta Ghosh, and Nitin Saxena. Towards blackbox identity testing of log-variate circuits. In *45th International Colloquium on Automata, Languages, and Programming*, volume 107 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 54, 16. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2018.

23 Michael A. Forbes and Amir Shpilka. Explicit Noether normalization for simultaneous conjugation via polynomial identity testing. In *Approximation, randomization, and combinatorial optimization*, volume 8096 of *Lecture Notes in Comput. Sci.*, pages 527–542. Springer, Heidelberg, 2013. doi:10.1007/978-3-642-40328-6_37.

24 Michael A. Forbes and Amir Shpilka. Quasipolynomial-time identity testing of noncommutative and read-once oblivious algebraic branching programs. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science—FOCS 2013*, pages 243–252. IEEE Computer Soc., Los Alamitos, CA, 2013. doi:10.1109/FOCS.2013.34.

25 Shafi Goldwasser and Ofer Grossman. Bipartite perfect matching in pseudo-deterministic NC. In *44th International Colloquium on Automata, Languages, and Programming*, volume 80 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 87, 13. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2017.

26 Timothy Gowers. Gowers weblog: What are dense sidon subsets of {1,2,...,n} like? https://gowers.wordpress.com/2012/07/13/what-are-dense-sidon-subsets-of-12-n-like/. Published on 2012-07-13.

27 Rohit Gurjar, Arpita Korwar, and Nitin Saxena. Identity testing for constant-width, and any-order, read-once oblivious arithmetic branching programs. *Theory Comput.*, 13:Paper No. 2, 21, 2017. doi:10.4086/toc.2017.v013a002.

28 Rohit Gurjar, Arpita Korwar, Nitin Saxena, and Thomas Thierauf. Deterministic identity testing for sum of read-once oblivious arithmetic branching programs. *Comput. Complexity*, 26(4):835–880, 2017. doi:10.1007/s00037-016-0141-z.

29 Venkatesan Guruswami and Chaoping Xing. Hitting sets for low-degree polynomials with optimal density. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 161–168. IEEE Computer Society, 2014. doi:10.1109/CCC.2014.24.

30 Russell Impagliazzo and Avi Wigderson. P = BPP if E requires exponential circuits: derandomizing the XOR lemma. In *STOC '97 (El Paso, TX)*, pages 220–229. ACM, New York, 1999.

31 Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, pages 355–364. ACM, New York, 2003. doi:10.1145/780542.780595.

32 Adam R. Klivans and Daniel Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, pages 216–223. ACM, New York, 2001. doi:10.1145/380752.380801.

33 Mrinal Kumar, Ramprasad Saptharishi, and Anamay Tengse. Near-optimal bootstrapping of hitting sets for algebraic circuits. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 639–646. SIAM, Philadelphia, PA, 2019. doi:10.1137/1.9781611975482.40.

34 Mrinal Kumar and Ben Lee Volk. Lower bounds for matrix factorization. *CoRR*, abs/1904.01182, 2019. arXiv:1904.01182.

35 Daniel Lewin and Salil Vadhan. Checking polynomial identities over any field: towards a derandomization? In *STOC '98 (Dallas, TX)*, pages 438–447. ACM, New York, 1999.

36 L. Lovász. On determinants, matchings, and random algorithms. In *Fundamentals of computation theory (Proc. Conf. Algebraic, Arith. and Categorical Methods in Comput. Theory, Berlin/Wendisch-Rietz, 1979)*, volume 2 of *Math. Res.*, pages 565–574. Akademie-Verlag, Berlin, 1979.

37 C. Lu. Hitting set generators for sparse polynomials over any finite fields. In *2012 IEEE 27th Conference on Computational Complexity*, pages 280–286, June 2012. doi:10.1109/CCC.2012.20.

38 Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. In *31st Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990)*, pages 2–10. IEEE Comput. Soc. Press, Los Alamitos, CA, 1990. doi:10.1109/FSCS.1990.89518.

39 Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987. doi:10.1007/BF02579206.

40 Kevin O'Bryant. A complete annotated bibliography of work related to sidon sequences. *The Electronic Journal of Combinatorics [electronic only]*, DS11:39 p., electronic only–39 p., electronic only, 2004. URL: http://eudml.org/doc/129129.

41 Imre Z. Ruzsa. An infinite Sidon sequence. *J. Number Theory*, 68(1):63–71, 1998. doi:10.1006/jnth.1997.2192.

42 Nitin Saxena. Progress on polynomial identity testing. *Bulletin of the EATCS*, 99:49–79, 2009.

43 Nitin Saxena. Progress on polynomial identity testing-II. In *Perspectives in computational complexity*, volume 26 of *Progr. Comput. Sci. Appl. Logic*, pages 131–146. Birkhäuser/Springer, Cham, 2014.

44 J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Comput. Mach.*, 27(4):701–717, 1980. doi:10.1145/322217.322225.

45 Adi Shamir. IP = PSPACE. In *31st Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990)*, pages 11–15. IEEE Comput. Soc. Press, Los Alamitos, CA, 1990. doi:10.1109/FSCS.1990.89519.

46 Amir Shpilka and Ilya Volkovich. Improved polynomial identity testing for read-once formulas. In *Approximation, randomization, and combinatorial optimization*, volume 5687 of *Lecture Notes in Comput. Sci.*, pages 700–713. Springer, Berlin, 2009. doi:10.1007/978-3-642-03685-9_52.

47 Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: a survey of recent results and open questions. *Found. Trends Theor. Comput. Sci.*, 5(3-4):207–388 (2010), 2009. doi:10.1561/0400000039.

48 Itaï Ben Yaacov. The vandermonde determinant identity in higher dimension, 2014. arXiv:1405.0993.

49 Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979)*, volume 72 of *Lecture Notes in Comput. Sci.*, pages 216–226. Springer, Berlin-New York, 1979.

Revision Notice

This is a revised version of the eponymous paper appeared in the proceedings of APPROX/RANDOM 2020 (LIPIcs, volume 176, https://www.dagstuhl.de/dagpub/978-3-95977-164-1, published in August, 2020), in which the proof of Theorem 6 is corrected. The proof in the previous version did not work, because the tester map constructed in Step 3, was incorrectly applied to $\alpha \in \mathbb{F}_{q^t}$, to get the points $\ell_1(\alpha), \ldots, \ell_\nu(\alpha) \in \mathbb{F}_q$, on which $f(x^{b_1}, x^{b_2}, \ldots, x^{b_n})$ was finally evaluated. In this revised version, the tester map is applied on $(\alpha^{b_1}, \ldots, \alpha^{b_n}) \in \mathbb{F}_{q^t}^n$ instead, to get the points $\ell_1(\alpha^{b_1}, \ldots, \alpha^{b_n}), \ldots, \ell_\nu(\alpha^{b_1}, \ldots, \alpha^{b_n}) \in \mathbb{F}_q^n$, on which $f(x_1, \ldots, x_n)$ is finally evaluated.

Dagstuhl Publishing – August 19, 2020.