Pseudorandom Generators for Low Degree Polynomials

Andrej Bogdanov
Computer Science Division
University of California, Berkeley
adib@cs.berkeley.edu

ABSTRACT

We investigate constructions of pseudorandom generators that fool polynomial tests of degree d in m variables over finite fields $\mathbb{F}$. Our main construction gives a generator with seed length $O(d^4 \log m(1+\log(d/\epsilon)/\log\log m)+\log|\mathbb{F}|)$ bits that achieves arbitrarily small bias ϵ and works whenever $|\mathbb{F}|$ is at least polynomial in d, $\log m$, and $1/\epsilon$. We also present an alternate construction that uses a seed that can be described by $O(c^2d^8m^{6/(c-2)}\log(d/\epsilon)+\log|\mathbb{F}|)$ bits (more precisely, $O(c^2d^8m^{6/(c-2)})$ field elements, each chosen from a set of size $\mathrm{poly}(cd/\epsilon)$, plus two field elements ranging over all of $\mathbb{F}$), works whenever $|\mathbb{F}|$ is at least polynomial in c, d, and $1/\epsilon$, and has the property that every element of the output is a function of at most c field elements in the input. Both generators are computable by small arithmetic circuits. The main tool used in the construction is a reduction that allows us to transform any "dense" hitting set generator for polynomials into a pseudorandom generator.

Categories and Subject Descriptors: F.2.0 [Analysis of algorithms and problem complexity]: General

General Terms: Theory, Algorithms

Keywords: Pseudorandomness, Derandomization

1. INTRODUCTION

A degree d test over a field $\mathbb{F}$ computes a multivariate polynomial of degree[1] d and attempts to distinguish between the cases when the inputs of the polynomial are chosen independently at random from $\mathbb{F}$ and the case when they are chosen from a smaller pseudorandom set. We are interested in unconditional constructions of pseudorandom generators for degree d tests.

A well studied subclass of degree d tests are the linear tests of Naor and Naor [16]. The epsilon biased generators of Naor and Naor, designed to fool all linear tests over the binary field, have found wide applicability, from algorithmic derandomization [16] to recent uses in derandomizing low-degree tests and constructions of short PCPs [4]. Several efficient constructions of generators for linear tests over the binary field with almost optimal seed length are known; Alon, Goldreich, Håstad and Peralta [1] describe three such constructions.

From a computational point of view, the class of linear functions over the binary field is very restricted. In particular, any such function in m variables can be computed by an oblivious branching program of width two and length m. It is therefore somewhat surprising that a generator providing security only against such weak adversaries has turned out to be so useful. Motivated by the utility of generators against linear functions, we consider a natural generalization of such generators, namely generators that fool polynomials of degree higher than one.

In the case of the binary field, pseudorandom generators against low-degree polynomials were considered by Luby, Veličković, and Wigderson [13].[2] They construct a generator that maps n bits of input into $dn^{O(\log n)}/\epsilon$ bits of output. Viola [21] recently simplified this construction, achieving a generator with the same stretch.[3] Both constructions are based on the existence of explicit functions that are average-case hard against AC^0-like classes of circuits, and it seems that better circuit lower bouds are necessary in order to improve the parameters in these constructions. (For the special case of low-degree polynomials that compute "predictor tests" over large fields, Kalyanaraman and Umans [10] recently constructed an essentially optimal generator.)

We show how to construct a pseudorandom generator that fools all tests of degree d over fields of size at least logarithmic in the number of variables. For constant bias and constant d, our generator has seed length that is within a constant factor of optimal; namely, it maps n bits of seed $2^{O_d(n)}$ field elements of output. The bias of the generator is roughly inverse polynomial in the field size. Moreover, the generator is computed by an arithmetic circuit of size polynomial in the input parameters.

Another problem that has commanded recent interest is the study of pseudorandom generators where every element of the output depends on only a constant number (say c) elements of the input. In the setting of boolean circuits, the question was initiated by Cryan and Miltersen [6]. Mossel, Shpilka, and Trevisan [15] showed that, for large c, there exist (nonuniform) generators that map n bits of in-

[1]Throughout the paper, "degree" means total degree.

[2]It is observed in [13] that these generators also work over fields of size polynomial in the length of the output.

[3]In fact, both [13] and [21] fool more general classes of tests, which in particular include low-degree polynomials.

STOC'05, May 22-24, 2005, Baltimore, Maryland, USA.

put into $n^{\Omega(\sqrt{c})}$ bits of output and fool linear tests with bias $\exp(-n^{1/2\sqrt{c}})$. More recently, Applebaum, Ishai, and Kushilevitz [3] showed how to obtain cryptographically secure pseudorandom generators in this model under standard assumptions.

We show an explicit construction of a generator that fools all degree d tests over fields and where each output element depends on at most c seed elements. The generator has constant bias even over fields whose size is polynomial in c and d and independent of the length of the input. For constant c and d, our generator maps a seed of n field elements into $O(n^{(c-1)/4})$ elements of output, and its bias can be made an arbitrarily small inverse polynomial in n, if the field is large enough. (This is optimal, up to the constant in the exponent, for fields whose size is at most polynomial in n.) Again, our generator can be computed by a small arithmetic circuit.

Connection to arithmetic identity testing Closely related to the construction of pseudorandom generators against algebraic adversaries is the problem of black-box derandomization of polynomial identity tests. In this model, one is allowed to evaluate a "black box" polynomial p in m variables on a set of inputs, typically over a finite field $\mathbb{F}$, and is asked to decide whether p is identically zero. By the Lemma of Schwartz and Zippel [20, 23], we know that if the size of $\mathbb{F}$ is slightly bigger than the total degree of p, and p is not identically zero, then a random point is likely to be a witness that p is nonzero. The derandomization challenge is to produce a smaller sample space $S \subseteq \mathbb{F}^m$, such that all nonzero polynomials p from a certain class have a witness in S. In this scenario, it is sufficient for the set S to be a "hitting set generator" rather than a full pseudorandom generator.

We show that the construction of pseudorandom generators for low degree polynomials reduces to the construction of "dense" hitting set generators for polynomials of slightly larger degree. This can be compared to the setting of Boolean circuits, where the existence of an efficient hitting set generator for circuits would imply a derandomization of BPP [2].

We note that for the class of polynomials computable by small arithmetic circuits, Kabanets and Impagliazzo [8] show a hitting set generator with polylogarithmic (in the output) seed length for identity testing under the assumption that there exists an exponential-time computable family of polynomials that requires exponential size arithmetic circuits. However, it is not clear whether this hitting set generator is pseudorandom.

Our results Let $\mathbb{F}$ be a field, X a finite set, G a function from X to $\mathbb{F}^m$, and $\mathcal{F}$ a family of polynomials from $\mathbb{F}^m$ to $\mathbb{F}$. We say G is a *hitting set generator* of *density* α for $\mathcal{F}$ if for every $p \in \mathcal{F}$, either p is the zero polynomial or $\Pr_{x \sim X}[p(G(x)) \neq 0] > \alpha$. We say G is a *pseudorandom generator* of *bias* ϵ for $\mathcal{F}$ if for every p in $\mathcal{F}$, the statistical distance between the distributions $p(G(x))$ and $p(y_1, \ldots, y_m)$, when the inputs are chosen uniformly and independently from $\mathbb{F}$, is at most ϵ. The field $\mathbb{F}$ is finite and of arbitrary characteristic. We show the following:

THEOREM 1.1. *For every integer $m > 0, d > 0$, fraction $\epsilon > 0$, and set $S \subseteq \mathbb{F}$ of size at least $d^{10} \log^2 m \cdot 1/\epsilon^2$, there exists a pseudorandom generator $G : S^n \times \mathbb{F}^2 \to \mathbb{F}^m$ of bias $O(\epsilon + d^2|\mathbb{F}|^{-1/2} + d^6|\mathbb{F}|^{-1})$ for the family of degree d polynomials over $\mathbb{F}$ in m variables, with $n = O(d^4 \log m / \log\log m)$. Moreover, G can be represented by an arithmetic circuit over $\mathbb{F}$ of size $\tilde{O}(md^4)$ that is constructible in time $\tilde{O}(md^4)$.*

THEOREM 1.2. *For every integer $m > 0, d > 0, c > 4$, fraction $\epsilon > 0$, and set $S \subseteq \mathbb{F}$ of size at least cd^6/ϵ^2, there exists a pseudorandom generator $G : S^n \times \mathbb{F}^2 \to \mathbb{F}^m$ of bias $O(\epsilon + d^2|\mathbb{F}|^{-1/2} + d^6|\mathbb{F}|^{-1})$ for the family of degree d polynomials over $\mathbb{F}$ in m variables, where $n = O(c^2 d^8 m^{6/(c-2)})$, and every output element of G depends on at most c inputs. Moreover, G can be represented by an arithmetic circuit over $\mathbb{F}$ of size $O(mc)$ that is constructible in time $m^{(6+o(1))d^4}$.*

Both of these theorems will be proved by first constructing hitting set generators of good density (Theorems 5.1 and 5.2), and then transforming the hitting set generator into a pseudorandom generator. A general reduction that enables us to carry out this transformation is shown in Theorem 3.1. The proofs of Theorems 1.1 and 1.2 are in Section 6.

In Section 7 we show two unrelated applications of the Theorems from Section 5. The first is an improvement in the length of the random seed of the Klivans-Spielman hitting set generator when the number of variables is larger than the degree of the polynomial and the number of monomials. The second is a construction of an arithmetic hitting set generator over the binary field.

Our construction The main tool in our construction of pseudorandom generators is a reduction that allows us to turn a hitting set generator of high density for polynomials of degree d in m variables into a pseudorandom generator for polynomials of degree $O(d^4)$ and $3m-2$ variables. Roughly, to obtain a pseudorandom generator of bias ϵ, we need a hitting set generator of density $1 - \epsilon/d$.

Our reduction is based on results from algebraic geometry that characterize the distribution of zeros of a multivariate polynomial by properties of its factorization. For a polynomial $f \in \mathbb{F}[y_1, \ldots, y_m]$, the probability that f evaluates to zero over a random input is $(1+\delta)\phi(f)/|\mathbb{F}|$, where $\phi(f)$ is the number of irreducible factors of f that are also absolutely irreducible, and δ is small when $|\mathbb{F}|$ is a large enough polynomial of d. (For definitions of irreducibility, please see the section on terminology below.) Moreover, the value $\phi(f)$ is preserved with high probability when f is projected on a random two-dimensional affine plane H in $\mathbb{F}^m$. If we can efficiently choose a plane H that preserves the value $\phi(f)$, we can obtain an estimate for the fraction of zeros of f by counting the fraction of zeros of the restriction of f on H.

For absolutely irreducible polynomials f, Kaltofen derived certain polynomial equations over the parametrization of H such that if the equations do not vanish over a given set of values, then these values parametrize a surface that preserves $\phi(f)$. This is the principal observation that allows us to turn a hitting set generator for these polynomial equations into a pseudorandom generator for the polynomial p.

This leaves us with the problem of constructing a hitting set generator of density $1-\epsilon$ for polynomials of degree d in m variables. Our construction is based on Lemma 4.1, which shows that given a nonzero polynomial $p(y_1, \ldots, y_m)$, we can perform a substitution for the variables y_i that reduces the number of variables without making the polynomial vanish.

We mention a related problem studied by Klivans and Spielman [11]. They construct a hitting set generator of density $1 - \epsilon$ for polynomials of degree d in m variables containing no more than M monomials. Their generator

has seed length that is logarithmic in mMd/ϵ. However, this generator works only over fields of size polynomial in m. In contrast, our generator allows fields of size logarithmic in m.

We also observe that it is not difficult to obtain a hitting set generator G of *nonzero* density for polynomials of degree d over m variables over a field $\mathbb{F}$ of size at least d: The inputs of G are a set $S \subseteq [m]$ of size d and values $x_1, \ldots, x_d \in \mathbb{F}$. The outputs of G are given by $G_i(S, x_1, \ldots, x_d) = x_j$, if i is the jth element of S, and 0 if $i \notin S$. It is not difficult to see that if p is nonzero, then $p \circ G$ is nonzero for at least one input of G.

Terminology and notation For a field $\mathbb{F}$, we use $\overline{\mathbb{F}}$ to denote the algebraic closure of $\mathbb{F}$. We use $\mathbb{F}_q$ for the finite field with q elements. $\mathbb{F}[x_1, \ldots, x_n]$ is the ring of polynomials in variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{F}$. $\mathbb{F}(x_1, \ldots, x_n)$ is the field of rational functions (ratios of polynomials) over $x_1, \ldots, x_n$ with coefficients in $\mathbb{F}$. For brevity of notation, we sometimes use $x_{1\ldots n}$ to denote the list $x_1, \ldots, x_n$. (For definitions of these notions, see, e.g. [12].)

A polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$ is *irreducible* over a field extension $\mathbb{F}'$ of $\mathbb{F}$ if p cannot be written as the product of two non-constant polynomials in $\mathbb{F}'[x_1, \ldots, x_n]$. We say p is *absolutely irreducible* if it is irreducible over $\overline{\mathbb{F}}$. Two polynomials are *unassociated* if they are both nonzero and not a constant multiple of one another. We use $\phi(p)$ to denote the number of unassociated irreducible factors of p that are also absolutely irreducible.

Given a polynomial $p \in \mathbb{F}[y_1, \ldots, y_k]$ and polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$, the *composition* $p \circ (f_1, \ldots, f_k)$ is the polynomial $r \in \mathbb{F}[x_1, \ldots, x_n]$ given by

$$r(x_1, \ldots, x_n) = p(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n)).$$

For $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$, we let $A(f_1, \ldots, f_k)$ be the number of their common zeros—the number of points $(a_1, \ldots, a_n) \in \mathbb{F}^n$ such that

$$f_1(a_1, \ldots, a_n) = \cdots = f_k(a_1, \ldots, a_n) = 0.$$

We let $\mathcal{H}_n$ denote the set of all two-dimensional affine subspaces of $\mathbb{F}^n$. For $H \in \mathcal{H}_n$, let $A_H(f_1, \ldots, f_k)$ be the number of common zeros of $f_1, \ldots, f_k$ that lie in H.

Each $H \in \mathcal{H}_n$ can be parametrized as the set of points $(\omega_1 s + \eta_1 t + \nu_1, \ldots, w_n s + \eta_n t + \nu_n)$, where $\omega_{1\ldots n}, \eta_{1\ldots n}, \nu_{1\ldots n}$ are fixed elements of $\mathbb{F}$ and s, t range over $\mathbb{F}$. (Also, the nondegeneracy condition: $(\omega_1, \ldots, \omega_n)$ and $(\eta_1, \ldots, \eta_n)$ are not constant multiples of one another must hold.) For each H, let us fix a canonical parametrization of this type and define the *restriction* of $f \in \mathbb{F}[x_1, \ldots, x_n]$ on H as the polynomial

$$f|_H(s, t) = f(\omega_1 s + \eta_1 t + \nu_1, \ldots, w_n s + \eta_n t + \nu_n).$$

To avoid confusion, we will reserve this notation for properties that are independent of the particular parametrization that is chosen for H. In particular, the degree, the number of variables, the number of irreducible factors, and the number of absolutely irreducible factors of a polynomial is independent of the choice of parametrization.

The ℓ_1 *distance* between two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over a finite set Ω, denoted by $|\mathcal{D}_1 - \mathcal{D}_2|$, is the quantity $\sum_{\omega \in \Omega} |\mathcal{D}_1(\omega) - \mathcal{D}_2(\omega)|$. The *statistical distance* between $\mathcal{D}_1$ and $\mathcal{D}_2$ is the maximum of $\mathcal{D}_1(T) - \mathcal{D}_2(T)$ over all events (statistical tests) $T \subseteq \Omega$. A simple argument shows that the statistical distance equals half the ℓ_1 distance.

An (l, α) combinatorial design over a universe U is a family of subsets $S_1, \ldots, S_m$ of U such that for every i, $|S_i| < l$ and for every $i \neq j$, $|S_i \cap S_j| \leq \alpha$.

2. COUNTING ZEROS OF MULTIVARIATE POLYNOMIALS

Before we describe our pseudorandom generator for low degree polynomials, let us look at the distribution of values of a low degree polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$, when its input is chosen uniformly at random. In fact, we ask an essentially equivalent question: What is the probability that p evaluates to zero at a random point? This is a well-known question in algebraic geometry, and we review some of the results and techniques that will be helpful in our application.

Before we state the general theorem, it is helpful to look at two examples. We are interested in relating the probability that p evaluates to zero to properties of its factorization. First, let us consider the case of a nonconstant, multivariate polynomial p of degree one. Such a polynomial is an affine function of its variables, so the distribution of its values is uniform. On the other hand, a polynomial of degree one does not factor. The other example we consider is the quadratic polynomial $p(x) = x^2$, over a field $\mathbb{F}$ of characteristic other than 2. The probability that $p(x)$ takes the value $c \in \mathbb{F}$ is $2/|\mathbb{F}|$ if c is a quadratic residue, $1/|\mathbb{F}|$ if $c = 0$, and zero otherwise. This is reflected in the factorization of the polynomial $p(x) - c$: If c is a quadratic residue, then $x^2 - c$ has two distinct factors. If $c = 0$, then $x^2 - c$ has a repeated factor. If c is a nonresidue, then $x^2 - c$ does not factor, not even over the algebraic closure of $\mathbb{F}$.

These are special cases of the following Theorem, which we prove in this Section:

THEOREM 2.1. *Suppose* $|\mathbb{F}| > 3d^4 - 4d^3 + 3d^2 + 20, n \geq 2$. *For every* $f \in \mathbb{F}[x_1, \ldots, x_n]$ *of degree* d,

$$\left|A(f) - \phi(f)|\mathbb{F}|^{n-1}\right| \leq 5d^2|\mathbb{F}|^{n-3/2} + (4d^6 + 8d^3 + 40)|\mathbb{F}|^{n-2} + O(d^4|\mathbb{F}|^{n-3}).$$

To prove Theorem 2.1, we use an approach introduced by Schmidt [19]: Reduce the multivariate case to a bivariate case, which is covered by a theorem of Weil, stated below. The bivariate polynomial in question will be a restriction of the multivariate polynomial, whose number of zeros we are interesting in estimating, to a suitably chosen two-dimensional affine plane in $\mathbb{F}^n$. Using results by Kaltofen [9], we manage to avoid a part of Schmidt's analysis, and obtain better parameters, at least for our purposes. (A similar analysis was carried out by Cafure and Matera [5].)

Counting zeros of an absolutely irreducible polynomial The number of zeros of a bivariate absolutely irreducible polynomial is characterized by the following result. We note that its proof is not elementary, but an analogous result with slightly worse parameters can be obtained by elementary methods [18]. All the other results quoted in this Section have elementary proofs.

LEMMA 2.2 (WEIL [22], SCHMIDT [19]). *If* $f \in \mathbb{F}[s, t]$ *of degree* d *is absolutely irreducible, then* $|A(f) - |\mathbb{F}|| < d^2\sqrt{|\mathbb{F}|} + d$.

To apply this result to the multivariate case, we want to relate the number of zeros of a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$

to the number of zeros of a restriction of f on a suitably chosen affine plane. In fact, Schmidt considers what happens when f is restricted to a random plane H in $\mathcal{H}_n$. It is immediate that $\mathrm{E}_{H\sim\mathcal{H}_n}[A_H(f)] = A(f)|\mathbb{F}|^{n-2}$, and a simple counting argument also shows the following:

LEMMA 2.3 (SCHMIDT [19, LEMMA 6]). *For every $f \in \mathbb{F}[x_1,\ldots,x_n]$, $\mathrm{Var}_{H\sim\mathcal{H}_n}[A_H(f)] \le d|\mathbb{F}|$.*

Now, to apply Lemma 2.2 to the restriction $f|_H$ of f on a random plane H, we need to know the value $\phi(f|_H)$. For starters, let us assume that f is absolutely irreducible. This case is covered by a theorem of Kaltofen. Kaltofen's theorem implies that $f|_H$ is absolutely irreducible over most planes in $\mathcal{H}_n$. Moreover, the parametrizations of planes over which p is not absolutely irreducible must satisfy certain polynomial equations of low degree.

THEOREM 2.4 (KALTOFEN [9, THM 5]). *For every $f \in \mathbb{F}[x_1,\ldots,x_n]$ of degree $d > 0$ there exists a nonzero $\Gamma \in \overline{\mathbb{F}}[v_{1\ldots n}, w_{2\ldots n}]$ of degree $2d^2$ such that the following holds. If $v_{1\ldots n}, w_{2\ldots n} \in \overline{\mathbb{F}}$ satisfy $\Gamma(v_{1\ldots n}, w_{2\ldots n}) \neq 0$, then there exists a nonzero polynomial $\Psi \in \overline{\mathbb{F}}[z_{2\ldots n}]$ of degree $\frac{3}{2}d^4 - 2d^3 + \frac{1}{2}d^2$ such that if $z_{2\ldots n} \in \overline{\mathbb{F}}$ satisfy $\Psi(z_{2\ldots n}) \neq 0$, then the polynomial*

$$r(s,t) = f(s+v_1, w_2 s + z_2 t + v_2, \ldots, w_n s + z_n t + v_n)$$

is absolutely irreducible in $\overline{\mathbb{F}}[s,t]$.

Kaltofen's Theorem will be useful not only as a tool in the proof of Theorem 2.1, but also in the construction of the pseudorandom generator in Section 3. In fact, to prove Theorem 2.1 the following Corollary (which follows from the Schwartz-Zippel Lemma and Proposition A.1) is sufficient:

COROLLARY 2.5. *For every $f \in \mathbb{F}[x_1,\ldots,x_n]$ of degree $d > 0$, we have that*

$$\mathrm{Pr}_{H\sim\mathcal{H}_n}[f|_H \text{ is absolutely irreducible}] \ge 1 - (\tfrac{3}{2}d^4 - 2d^3 + \tfrac{3}{2}d^2 + 10)/|\mathbb{F}|.$$

Putting these results together, we obtain the following estimate for the number of zeros of a multivariate absolutely irreducible polynomial:

PROPOSITION 2.6. *Suppose $|\mathbb{F}| > 3d^4 - 4d^3 + 3d^2 + 20$. Let $f \in \mathbb{F}[x_1,\ldots,x_n]$ be absolutely irreducible. Then*

$$|A(f) - |\mathbb{F}|^{n-1}| \le 5d^2|\mathbb{F}|^{n-3/2}.$$

PROOF. If $n = 2$, this follows directly from Lemma 2.2, so let us assume $n \ge 3$. By Lemma 2.3, we have that $\mathrm{Var}_{H\sim\mathcal{H}_n}[A_H(f)] \le d|\mathbb{F}|$. By Chebyshev's inequality, it follows that

$$\Pr_{H\sim\mathcal{H}_n}[|A_H(f) - A(f)/|\mathbb{F}|^{n-2}| \le 2\sqrt{d|\mathbb{F}|}] \ge 3/4.$$

From Corollary 2.5, we have that $\mathrm{Pr}_{H\sim\mathcal{H}_n}[f|_H \text{ is a.i.}] \ge 1/2$. These two conditions imply that there exists at least one $H \in \mathcal{H}_n$ such that both $|A_H(f) - A(f)/|\mathbb{F}|^{n-2}| \le 3\sqrt{d|\mathbb{F}|}$ and $f|_H$ is absolutely irreducible. By Lemma 2.2, we have that $|A_H(f) - |\mathbb{F}|| < d^2\sqrt{|\mathbb{F}|} + d$, so by the triangle inequality

$$|A(f)/|\mathbb{F}|^{n-2} - |\mathbb{F}|| < 3\sqrt{d|\mathbb{F}|} + d^2\sqrt{|\mathbb{F}|} + d \le 5d^2\sqrt{|\mathbb{F}|}.$$

The claim follows after multiplying by $|\mathbb{F}|^{n-2}$. □

Counting zeros of an arbitrary polynomial To extend Proposition 2.6 to an arbitrary multivariate polynomial f, we will estimate the number of zeros of each irreducible factor of f separately and combine these estimates using inclusion-exclusion. To realize this plan, we need to have estimates for the number of zeros of irreducible factors of f that are not absolutely irreducible, and the number of common zeros of two irreducible polynomials f and g. Again, the counting goes by reduction to the bivariate case, and is carried out using the following two lemmas:

LEMMA 2.7 (KALTOFEN [9, COR 2]). *Let $\mathbb{F}$ be a perfect field.[4] For every irreducible $f \in \mathbb{F}[x_1,\ldots,x_n]$, and $\nu_{1\ldots n}, \omega_{2\ldots n}, \eta_{2\ldots n}$ chosen at random from $\mathbb{F}$,*

$$\Pr[r(s,t) \text{ is irreducible in } \mathbb{F}[s,t]] \ge 1 - 2d^4/|\mathbb{F}|$$

where $r(s,t) = f(s+\nu_1, \omega_2 s + \eta_2 t + \nu_2, \ldots, \omega_n s + \eta_n t + \nu_n)$.

LEMMA 2.8 (HUANG, WONG [7, LEMMA 2.1]). *Let $f \in \mathbb{F}[x_1,\ldots,x_n]$ be irreducible but not absolutely irreducible. For every $(a_1,\ldots,a_n)$ such that $f(a_1,\ldots,a_n) = 0$ and every $1 \le i \le n$,*

$$\partial f/\partial x_i(a_1,\ldots,a_n) = 0.$$

We begin with a technical lemma, which will also be used in Section 3. (The proof is in the full version of the paper.)

PROPOSITION 2.9. *Let p_1, p_2 be unassociated polynomials in $\mathbb{F}[x_1,\ldots,x_n]$ of degree d. There exists a nonzero polynomial $\Phi \in \mathbb{F}[v_{1\ldots n}, w_{2\ldots n}, z_{2\ldots n}]$ of degree $3d$ such that if $\Phi(v_{1\ldots n}, w_{2\ldots n}, z_{2\ldots n}) \neq 0$, then r_1 and r_2 are unassociated in $\mathbb{F}[s,t]$, where*

$$r_i(s,t) = p_i(s+v_1, w_2 s + z_2 t + v_2, \ldots, w_n s + z_n t + v_n)$$

for $i = 1, 2$.

PROPOSITION 2.10. *Let f and g be unassociated irreducible polynomials in $\mathbb{F}[x_1,\ldots,x_n]$ of degree d each. Then $A(f,g) \le (2d^5 + 4d^2 + 20)|\mathbb{F}|^{n-2} + O(d^3|\mathbb{F}|^{n-3})$.*

PROOF. Define the following events:

1. $S_1 \subseteq \mathcal{H}_n$ is the set of planes H such that $f|_H$ is not a constant multiple of $g|_H$,
2. $S_2 \subseteq \mathcal{H}_n$ is the set of planes H such that $f|_H$ and $g|_H$ are irreducible,
3. $S_3 \subseteq \mathcal{H}_n$ is the set of planes H such that $g|_H \neq 0$.

All these properties are independent of the parametrization of H. We have that $\mathrm{Pr}_{\mathcal{H}_n}[S_1] \ge 1 - (3d+10)/|\mathbb{F}|$ (by Propositions 2.9 and A.1), $\mathrm{Pr}_{\mathcal{H}_n}[S_2] \ge 1 - (2d^4 + 10)/|\mathbb{F}|$ (by Lemma 2.7 and Proposition A.1). For S_3, we note that a random affine plane is determined by a random choice of three distinct points in $\mathbb{F}^n$, therefore

$$\begin{aligned}\mathrm{Pr}_{\mathcal{H}_n}[\overline{S_3}] &\le \mathrm{Pr}_{x,y,z\in\mathbb{F}^n}[g(x), g(y), g(z) = 0 | x, y, z \text{ distinct}] \\ &\le \Pr[g(x), g(y), g(z) = 0] / \Pr[x, y, z \text{ distinct}] \\ &\le (d^3/|\mathbb{F}|^3)/(1 - 3/|\mathbb{F}|^n) = O(d^3/|\mathbb{F}|^3).\end{aligned}$$

If $H \in S_3$, then $\mathrm{Pr}_x[x \in A_H(f,g)] \le \mathrm{Pr}_x[x \in A_H(g)] \le d/|\mathbb{F}|$. If, moreover, $H \in S = S_1 \cap S_2 \cap S_3$, then f_H and g_H are nonzero, irreducible, and not a constant multiple of

[4] In particular, every finite field is perfect.

each other, so by the Bézout inequality in the plane, $\Pr_x[x \in A_H(f,g)] \le d^2/|\mathbb{F}|^2$. Therefore

$$\begin{aligned}
&\Pr_x[x \in A(f,g)] \\
&= \Pr_{H\sim\mathcal{H}_n, x\sim H}[x \in A(f_H, g_H)] \\
&\le \Pr_{x\sim H}[x \in A(f_H,g_H) | H \in S] \Pr_{\mathcal{H}_n}[S] \\
&\quad + \Pr_{x\sim H}[x \in A(f_H,g_H) | H \in S_3 - S] \Pr_{\mathcal{H}_n}[S_3 - S] \\
&\quad + \Pr_{x\sim H}[x \in A(f_H,g_H) | H \notin S_3] \Pr_{\mathcal{H}_n}[\overline{S_3}] \\
&\le 2d^5/|\mathbb{F}|^2 + (4d^2+20)/|\mathbb{F}|^2 + O(d^3/|\mathbb{F}|^3). \quad \square
\end{aligned}$$

For the rest of this Section, let $\alpha(d) = \alpha_{n,\mathbb{F}}(d) = (2d^5 + 4d^4 + 20)|\mathbb{F}|^{n-2} + O(d^3|\mathbb{F}|^{n-3})$.

COROLLARY 2.11. *Suppose $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ are of degree d each, f is irreducible, and f does not divide g. Then $A(f,g) \le d\alpha(d)$.*

PROOF. Let $g_1, \ldots, g_K$ be the unassociated irreducible factors of g. Since f does not divide g, f cannot be a constant multiple of g_i for any i. By Proposition 2.10, $A(f,g_i) \le \alpha(d)$. Therefore

$$A(f,g) \le \sum_{i=1}^K A(f,g_i) \le K\alpha(d) \le d\alpha(d). \quad \square$$

PROOF OF THEOREM 2.1. Let $k = \phi(f)$. Write $f_1, \ldots, f_K$ for the unassociated irreducible factors of f, and let d_i be the degree of f_i. Suppose the factors $f_1, \ldots, f_k$ are absolutely irreducible, and the factors $f_{k+1}, \ldots, f_K$ are not absolutely irreducible. We begin by estimating the quantities $A(f_i)$, for $1 \le i \le K$.

If $1 \le i \le k$, then by Proposition 2.6, we have that $|A(f_i) - |\mathbb{F}|^{n-1}| \le 5d_i^2|\mathbb{F}|^{n-3/2}$. If $k+1 \le i \le K$, then Lemma 2.8 says that every zero of f_i is also a zero of $\partial f_i/\partial x_l$, for every variable x_l. In particular, $A(f_i) \le A(f_i, \partial f_i/\partial x_l)$. There must be at least one l such that $\partial f_i/\partial x_l$ is nonzero. Also, f_i cannot divide $\partial f_i/\partial x_l$, so by Corollary 2.11, $A(f_i) \le A(f_i, \partial f_i/\partial x_l) \le d_i\alpha(d_i)$. Putting these inequalities together, we have that

$$\begin{aligned}
\left|A(f) - k|\mathbb{F}|^{n-1}\right| &\le \left|A(f) - \sum_{i=1}^K A(f_i)\right| \\
&\quad + \left|\sum_{i=1}^k A(f_i) - |\mathbb{F}|\right| + \sum_{i=k+1}^K A(f_i) \\
&\le \left|A(f) - \sum_{i=1}^K A(f_i)\right| \\
&\quad + \sum_{i=1}^k 5d_i^2|\mathbb{F}|^{n-3/2} + \sum_{i=k+1}^K d_i\alpha(d_i) \\
&\le \left|A(f) - \sum_{i=1}^K A(f_i)\right| \\
&\quad + 5d^2|\mathbb{F}|^{n-3/2} + d\alpha(d).
\end{aligned}$$

Let $d_{ij} = \max(d_i, d_j)$. By inclusion-exclusion we have that

$$\begin{aligned}
\left|A(f) - \sum_{i=1}^K A(f_i)\right| &\le \sum_{i<j} A(f_i, f_j) \\
&\le \sum_{i<j} \alpha(d_{ij}) \\
&\le d\alpha(d).
\end{aligned}$$

The second to last line follows from Proposition 2.10. $\square$

3. FROM A HITTING SET GENERATOR TO A PSEUDORANDOM GENERATOR

We now show how to obtain an efficient construction for a pseudorandom generator for low degree polynomials, assuming the existence of a good hitting set generator. In particular, we establish the following:

THEOREM 3.1. *Let $G_1 : X_1 \to \mathbb{F}^{2m-1}$ be a hitting set generator of density $1-\epsilon$ for polynomials of degree $3d^2$. Let $G_2 : X_2 \to \mathbb{F}^{m-1}$ be a hitting set generator of density $1-\epsilon$ for polynomials of degree $\max(\frac{3}{2}d^4 - 2d^3 + \frac{1}{2}d^2, 3d^2)$. Suppose that G_1 maps $x_1 \in X_1$ to $(v_1, \ldots, v_m, w_2, \ldots, w_m) \in \mathbb{F}^{2m-1}$, and G_2 maps $x_2 \in X_2$ to $(z_2, \ldots, z_m) \in \mathbb{F}^{m-1}$. Then the map $G' : X_1 \times X_2 \times \mathbb{F}^2 \to \mathbb{F}^m$ given by*

$$G'(x_1, x_2, s, t) = (s + v_1, w_2 s + z_2 t + v_2, \ldots, w_m s + z_m t + v_m)$$

is a pseudorandom generator for degree d polynomials of bias $O(\sqrt{\epsilon}d + d^2|\mathbb{F}|^{-1/2} + d^6|\mathbb{F}|^{-1})$.

To simplify notation further in the discussion, we let G denote the product of the generators G_1 and G_2. That is, $G : X_1 \times X_2 \to \mathbb{F}^{3m-2}$ takes a seed $x = (x_1, x_2)$ and outputs the concatenation of $G(x_1)$ and $G(x_2)$.

Theorem 2.4 provides a sufficient condition under which an absolutely irreducible polynomial $p \in \mathbb{F}[y_1, \ldots, y_m]$ can be "converted" into an absolutely irreducible bivariate polynomial $r \in \overline{\mathbb{F}}[s,t]$. Notice that if we can find values $v_{1\ldots m}$, $w_{2\ldots m}$, $z_{2\ldots m}$ in $\mathbb{F}$ such that $\Gamma(v_{1\ldots m}, w_{2\ldots m}, z_{2\ldots m}) \ne 0$ and $\Psi(v_{1\ldots m}, w_{2\ldots m}, z_{2\ldots m}) \ne 0$, then all the coefficients of r will be in the field $\mathbb{F}$, so that r will lie in $\mathbb{F}[s,t]$.

Our proof of pseudorandomness will proceed along the following lines. Given a polynomial $p \in \mathbb{F}[y_1, \ldots, y_m]$, we want to argue that for most values $c \in \mathbb{F}$, and for most choices $x_1 \in X_1$ and $x_2 \in X_2$, the difference $\Pr[p(y_1, \ldots, y_m) = c] - \Pr[r(s,t) = c]$ is small. For this, it would suffice to show that $\phi(p-c) = \phi(r-c)$; actually, since the events $p(y_1, \ldots, y_m) = c$ and $r(s,t) = c$ with c ranging over $\mathbb{F}$ partition their sample spaces, it will be sufficient to argue that for "most" r, $\phi(p-c) \le \phi(r-c)$. This is shown in Proposition 3.3 using results from Section 2.

To obtain the condition $\phi(p-c) \le \phi(r-c)$, we will use Proposition 2.9 to ensure that no two irreducible factors of $p-c$ that are also absolutely irreducible map to the same factors of $r-c$. We will also need to ensure that no irreducible factor of $p-c$ reduces to a constant in $r-c$:

PROPOSITION 3.2. *For every nonconstant polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$ of degree d, there exists a $\Xi \in \mathbb{F}[w_{2\ldots n}]$ of degree d such that if $\Xi(w_{2\ldots n}) \ne 0$, then $r \in \mathbb{F}[s,t]$ is not a constant, where*

$$r(s,t) = p(s + v_1, w_2 s + z_2 t + v_2, \ldots, w_m s + z_m t + v_m).$$

PROOF. View r as a polynomial in s, t over the ring of coefficients $\mathbb{F}[v_{1\ldots n}, w_{2\ldots n}, z_{2\ldots n}]$. Observe that since p is nonconstant, r contains a monomial of the form $s^i, i \ge 1$. Note that the coefficient in r of s^i for the maximum such i is nonzero and depends only on $w_{2\ldots n}$. Choose Ξ to be this coefficient. $\square$

Let $p \in \mathbb{F}[y_1, \ldots, y_m]$, and G_1, G_2 be the hitting set generators from Theorem 3.1. Define the polynomial

$$r_x(s,t) = p(s + v_1, w_2 s + z_2 t + v_2, \ldots, w_m s + z_m t + v_m),$$

where $x = (x_1, x_2)$ are the seeds of G_1 and G_2, $(v_{1\ldots m}, w_{2\ldots m})$ is the output $G_1(x_1)$, and $(z_{2\ldots m})$ is the output $G_2(x_2)$. Say that x is *good* for p if $\phi(r_x) \geq \phi(p)$.

PROPOSITION 3.3. *For every $p \in \mathbb{F}[y_1, \ldots, y_m]$ of degree d, x is good for p with probability $1 - 5\epsilon$.*

Before we proceed with the proof we observe the following useful fact: A hitting set generator $G : X \to \mathbb{F}^m$ of density $1 - \epsilon$ for degree d polynomials over $\mathbb{F}$ is also a hitting set generator of density $1 - \epsilon$ for degree d polynomials over $\overline{\mathbb{F}}$.

PROOF. Let $p_1, \ldots, p_K$ denote the distinct irreducible factors of p over $\mathbb{F}[y_1, \ldots, y_m]$, of degrees $d_1, \ldots, d_K$, respectively. Suppose that the first $k = \phi(p)$ of these factors $p_1, \ldots, p_k$ are absolutely irreducible, and the others are not. Define the following polynomials:

1. For every p_i, $1 \leq i \leq K$ let $\Xi_i \in \mathbb{F}[w_{2\ldots m}]$ be the polynomial of degree d_i from Proposition 3.2. Let $\Xi = \prod_{i=1}^{K} \Xi_i$.
2. For every p_i, $1 \leq i \leq k$, let $\Gamma_i \in \overline{\mathbb{F}}[v_{1\ldots m}, w_{2\ldots m}]$ be the polynomial of degree $2d_i^2$ from Theorem 2.4. Let $\Gamma = \prod_{i=1}^{k} \Gamma_i$.
3. For every pair of polynomials p_i, p_j, $1 \leq i < j \leq k$, let $\Phi_{ij} \in \mathbb{F}[v_{1\ldots m}, w_{2\ldots m}, z_{2\ldots m}]$ be the polynomial of degree $3\max(d_i, d_j)$ from Proposition 2.9. Let $\Phi = \prod_{1 \leq i < j \leq k} \Phi_{ij}$.

Note that Ξ has degree d, Γ has degree at most $2d^2$, and Φ has degree at most $3d^2$.

Say $x_1 \in X_1$ is *good* if all three of the following conditions hold: $\Xi(w_{2\ldots m}) \neq 0$, $\Gamma(v_{1\ldots m}, w_{2\ldots m}) \neq 0$, and $\Phi^{x_1}(z_{2\ldots m}) = \Phi(v_{1\ldots m}, w_{2\ldots m}, z_{2\ldots m}) \not\equiv 0$ (as a polynomial in $\mathbb{F}[z_{2\ldots m}]$). By the pseudorandom property of G_1, each of these three conditions holds with probability at least $1-\epsilon$, so x_1 is good with probability at least $1 - 3\epsilon$.

Now fix a good x_1. For this x_1, let $\Psi_1, \ldots, \Psi_k \in \overline{\mathbb{F}}[z_{2\ldots m}]$ denote the polynomials of degree at most $\frac{3}{2}d_i^4 - 2d_i^3 + \frac{1}{2}d_i^2$ guaranteed by Theorem 2.4. Let $\Psi = \prod_{i=1}^{k} \Psi_i$. Then Ψ is of degree at most $\sum_{i=1}^{k}(\frac{3}{2}d_i^4 - 2d_i^3 + \frac{1}{2}d_i^2) \leq \frac{3}{2}d^4 - 2d^3 + \frac{1}{2}d^2$. By the hitting set property of G_2, with probability $1-\epsilon$ over x_2, $\Psi(z_{2\ldots m}) \neq 0$. Also, with probability $1 - \epsilon$, $\Phi^{x_1}(z_{2\ldots m}) \neq 0$. Call an x_2 that satisfies both conditions *good*.

We show that if both x_1 and x_2 are good, then $\phi(r_x) \geq \phi(p)$. Fix a good pair x_1 and x_2 and for every i, define the polynomial

$$r_{x,i}(s,t) = p_i(s + v_1, w_2 s + z_2 t + v_2, \ldots, w_m s + z_m t + v_m).$$

First, we observe that since Ξ does not evaluate to zero, all the polynomials $r_{x,i}$ are nonzero. We now observe that the polynomials $r_{x,1}, \ldots, r_{x,k}$ are all absolutely irreducible (by Theorem 2.4), nonconstant (by Proposition 3.2), and unassociated (by Proposition 2.9). It follows that r_x has at least $k = \phi(p)$ unassociated absolutely irreducible factors.

Since x_1 is good with probability $1 - 3\epsilon$, and conditioned on x_1 being good x_2 is good with probability $1-2\epsilon$, it follows that $x = (x_1, x_2)$ is good with probability $1 - 5\epsilon$. □

We now prove the main Theorem of this Section.

PROOF OF THEOREM 3.1. Let p be an arbitrary polynomial of degree d in $\mathbb{F}[y_1, \ldots, y_m]$. For every $c \in \mathbb{F}$, let p^c denote the polynomial $p^c(y_1, \ldots, y_m) = p(y_1, \ldots, y_m) - c$. Let $X = X_1 \times X_2$, and for every $x \in X$ and $c \in \mathbb{F}$ define the polynomials

$$r_x(s,t) = p(s + v_1, w_2 s + z_2 t + v_2, \ldots, w_m s + z_m t + v_m),$$
$$r_x^c(s,t) = r_x(s,t) - c,$$

where the sequence $(v_{1\ldots m}, w_{2\ldots m}, z_{2\ldots m})$ is the output of G on input x. Our goal is to show that

$$\tfrac{1}{2}\sum\nolimits_{c \in \mathbb{F}} \left|\Pr[p^c(y_{1\ldots m}) = 0] - \Pr[r_x^c(s,t) = 0]\right| < O(\sqrt{\epsilon}d + \delta),$$

where $\delta = \delta(d, |\mathbb{F}|) = O(d^2|\mathbb{F}|^{-1/2} + d^6|\mathbb{F}|^{-1})$. (We may assume that $|\mathbb{F}| = \Omega(d^6)$, for otherwise the Theorem holds trivially.)

Our starting point are the estimates of Theorem 2.1, which yield (for all $c \in \mathbb{F}$)

$$|\Pr[p^c(y_{1\ldots m}) = 0] - \phi(p^c)/|\mathbb{F}|| = O(\delta/|\mathbb{F}|), \quad (1)$$
$$|\Pr[r_x^c(s,t) = 0] - \phi(r_x^c)/|\mathbb{F}|| = O(\delta/|\mathbb{F}|), \ \forall x \in X. \quad (2)$$

An immediate consequence of Equations (1) and (2) are the following two formulas, which will be useful later:

$$\left|1 - \sum\nolimits_{c \in \mathbb{F}} \phi(p^c)/|\mathbb{F}|\right| = O(\delta) \text{ and} \quad (3)$$
$$\left|1 - \sum\nolimits_{c \in \mathbb{F}} \phi(r_x^c)/|\mathbb{F}|\right| = O(\delta) \text{ for every } x \in X. \quad (4)$$

From Equation (1), it also follows that

$$\sum\nolimits_{c \in \mathbb{F}} |\Pr[p^c(y_{1\ldots m}) = 0] - \phi(p^c)/|\mathbb{F}|| = O(\delta),$$

so for the rest of the proof it will be sufficient to show that the quantity

$$\begin{aligned} &\sum\nolimits_{c \in \mathbb{F}} \left|\phi(p^c)/|\mathbb{F}| - \Pr_{x,s,t}[r_x^c(s,t) = 0]\right| \\ &\quad = \sum\nolimits_{c \in \mathbb{F}} \left|\mathrm{E}_{x \sim X}[\phi(p^c)/|\mathbb{F}| - \Pr_{s,t}[r_x^c(s,t) = 0]]\right| \\ &\quad \leq \mathrm{E}_{x \sim X}\left[\sum\nolimits_{c \in \mathbb{F}} \left|\phi(p^c)/|\mathbb{F}| - \Pr_{s,t}[r_x^c(s,t) = 0]\right|\right] \end{aligned} \quad (5)$$

is at most $\sqrt{5\epsilon}d + O(\delta)$. By Proposition 3.3, for every $c \in \mathbb{F}$, $\Pr_x[x \text{ is good for } p^c] > 1 - 5\epsilon$. In particular, it follows that $\Pr_{x,c}[x \text{ is good for } p^c] > 1 - 5\epsilon$, and

$$\Pr_x[\Pr_c[x \text{ is good for } p^c] > 1 - \sqrt{5\epsilon}] > 1 - \sqrt{5\epsilon}.$$

Let $S = \{x \in X : \Pr_c[x \text{ is good for } p^c] > 1 - \sqrt{5\epsilon}$. Recall that by our definition of "good", when $x \in S$, $\phi(r_x^c) \geq \phi(p^c)$. We will now split the analysis of the expectation (5) into two cases, depending on whether x belongs to S or not.

By the Schwartz-Zippel Lemma, for every x and c, we have the upper bound

$$\left|\phi(p^c)/|\mathbb{F}| - \Pr_{s,t}[r_x^c(s,t) = 0]\right| \leq d/|\mathbb{F}| \quad (6)$$

so that the contribution of $x \notin S$ to the expectation (5) is at most $\left(\sum_{c \in \mathbb{F}} d/|\mathbb{F}|\right) \Pr_x[x \notin S] \leq \sqrt{5\epsilon}d$.

We now handle the case $x \in S$. We will show that, for every $x \in S$,

$$\sum\nolimits_{c \in \mathbb{F}} \left|\phi(p^c)/|\mathbb{F}| - \Pr_{s,t}[r_x^c(s,t) = 0]\right| = O(\sqrt{\epsilon}d + \delta).$$

Fix $x \in S$, and let T denote the set of all $c \in \mathbb{F}$ such that x is good for p^c. Note that T will include all but a $\sqrt{5\epsilon}$ fraction of $\mathbb{F}$. We split the summation over c into the cases $c \in T$ and $c \notin T$. The contribution of the summation from

the case $c \notin T$ can be bounded by the quantity $\sqrt{5\epsilon}d$, using (6). For the case $c \in T$, we have

$$\begin{aligned}
&\sum_{c\in T}\big|\phi(p^c)/|\mathbb{F}| - \Pr_{s,t}[r_x^c(s,t)=0]\big| \\
&\quad\le \sum_{c\in T}\big(\big|\phi(r_x^c)/|\mathbb{F}| - \phi(p^c)/|\mathbb{F}|\big| \\
&\qquad\qquad + \big|\Pr_{s,t}[r_x^c(s,t)=0] - \phi(r_x^c)/|\mathbb{F}|\big|\big) \\
&\quad\le \sum_{c\in T}\big|\phi(r_x^c)/|\mathbb{F}| - \phi(p^c)/|\mathbb{F}|\big| + \sum_{c\in T} O(\delta/|\mathbb{F}|) \\
&\quad\le \sum_{c\in T}\big|\phi(r_x^c)/|\mathbb{F}| - \phi(p^c)/|\mathbb{F}|\big| + O(\delta).
\end{aligned}$$

The second to last line follows from 2. Since for all $c \in T$, x is good for p^c, it follows that the quantity $\phi(r_x^c)/|\mathbb{F}| - \phi(p^c)/|\mathbb{F}|$ is always nonnegative, so that

$$\begin{aligned}
&\sum_{c\in T}\big|\phi(r_x^c)/|\mathbb{F}| - \phi(p^c)/|\mathbb{F}|\big| \\
&\quad= \sum_{c\in T}\big(\phi(r_x^c)/|\mathbb{F}| - \phi(p^c)/|\mathbb{F}|\big) \\
&\quad= \big(1 - \sum_{c\in\mathbb{F}}\phi(p^c)/|\mathbb{F}|\big) - \big(1 - \sum_{c\in\mathbb{F}}\phi(r_x^c)/|\mathbb{F}|\big) \\
&\qquad + \sum_{c\notin T}\big(\phi(r_x^c)/|\mathbb{F}| - \phi(p^c)/|\mathbb{F}|\big) \\
&\quad\le \big|1 - \sum_{c\in\mathbb{F}}\phi(p^c)/|\mathbb{F}|\big| + \big|1 - \sum_{c\in\mathbb{F}}\phi(r_x^c)/|\mathbb{F}|\big| \\
&\qquad + \sum_{c\notin T}\big|\phi(r_x^c)/|\mathbb{F}| - \phi(p^c)/|\mathbb{F}|\big| \\
&\quad\le O(\delta) + O(\delta) + \sqrt{5\epsilon}d.
\end{aligned}$$

The last line of inequalities follows from Equations (4), (3), and (6). □

4. COMBINATORIAL CONSTRUCTIONS

In this section we introduce combinatorial objects that will be used in the construction of hitting set generators for polynomials. We begin by showing a connection between hitting set generators for low degree polynomials and parity check matrices of codes.

LEMMA 4.1. *Let $p \in \mathbb{F}[y_1,\ldots,y_m]$ be a polynomial of total degree at most d with M monomials, q be a prime, and $H \in \mathbb{F}_q^{n\times m}$ be the parity check matrix of a linear code over $\mathbb{F}_q$ with minimum distance $2d+1$. Let*

$$f_j(x_1,\ldots,x_n) = \prod_{i=1}^{n} x_i^{H_{i,j}}.$$

Then the polynomial $r = p\circ(f_1,\ldots,f_m)$ has M monomials. In particular, if p is nonzero, then r is nonzero.

PROOF. Consider two arbitrary terms $A = y_1^{\alpha_1}\ldots y_m^{\alpha_m}$ and $B = y_1^{\beta_1}\ldots y_m^{\beta_m}$, where $\sum_{i=1}^m \alpha_i \le d$ and $\sum_{i=1}^m \beta_i \le d$. Now perform the substitution $y_j \rightsquigarrow f_j(x_1,\ldots,x_n)$ and call the resulting terms A' and B', respectively. Suppose that $A' = B'$. Then for all $1 \le i \le n$,

$$\sum_{j=1}^{n} H_{i,j}(\alpha_j - \beta_j) = 0 \tag{7}$$

over the integers. Let T denote the largest integer such that q^T is a common factor of $\alpha_j - \beta_j$ over all j. Define a vector $v \in \mathbb{F}^m$ by $v_j = q^{-T}(\alpha_j - \beta_j) \pmod q$. By construction, $v \neq 0$. Moreover, v cannot have Hamming weight more than $2d$ because there can be at most d nonzero α_j and d nonzero β_j. On the other hand, it follows from equation (7) that $Hv = 0$ over $\mathbb{F}_q$. This contradicts the fact that H is a sum-check matrix of a code of minimum distance $2d+1$.

To finish the proof, we observe that p is a linear combination of M terms of total degree at most d. Since any two terms of p map to distinct terms of r, the polynomial r has exactly M monomials. □

There are several known efficient constructions of matrices of codes with good minimum distance. To obtain a construction with good parameters we use BCH codes over nonbinary alphabets. (The relevant concepts about BCH codes are described in Appendix B.) Let q be a prime between $\frac{1}{2}\log m$ and $\log m$, and let l be the smallest integer such that $N = q^l \ge m$. Choose H to be the the first m columns of the parity check matrix of the BCH code $BCH_q(N, 2d+1)$ (see Appendix B). By construction, $H \subseteq \mathbb{F}_q^{2dl\times m}$ has minimum distance at least $2d+1$. Substituting the values for q and l in terms of m, we obtain the following lemma:

LEMMA 4.2. *For every $m > 0$ and prime q, with $\frac{1}{2}\log m < q \le \log m$, there exists a parity check matrix $H \in \mathbb{F}_q^{n\times m}$ of a code over $\mathbb{F}_q$ of minimum distance at least $2d+1$ with $n = 2d(\log m/\log\log m + O(1))$. Moreover H, is constructible in time $\tilde{O}(md)$.*

We now consider the case of generators where every element of output may depend on only a constant number of elements in the input. This requires the construction of a parity check matrix H with few nonzero entries in every column.

In the following Lemma, we make use of a standard construction to generate a d-wise independent set of variables $(X_1,\ldots,X_m)$ over a prime field $\mathbb{F}_q$: Choose $(A_0,\ldots,A_{d-1}) \in \mathbb{F}_q^d$ uniformly at random and let $X_t = \sum_{i=0}^{d-1} A_i t^i$. Given the values $A_0,\ldots,A_{d-1}$, each X_t can be computed in time $O(d\log^2 q)$ and space $O(\log q)$.[5]

LEMMA 4.3. *For every $c > 0$, $d > 0$ and $n > 0$, there exists a matrix $H \in \mathbb{F}_2^{n\times m}$ with the following properties:*

1. *$m = \Omega((e\sqrt{2}/2cd)^c(n-c)^{c/2})$.*
2. *H is the parity check matrix of a linear code of distance at least $2d+1$.*
3. *H is computable in time $O\big(\big(2m\binom{n}{c}\big)^{2d}\big)$ and in space $\tilde{O}(cd\log n)$.*
4. *Every column of H has exactly c ones.*

PROOF. Let $W_w \subseteq \mathbb{F}_2^n$ denote the collection of vectors of Hamming weight exactly w. Choose the columns of H from a $2d$-wise independent family over domain W_c of size $\binom{n}{c} \ge m$. Call the resulting distribution on $n\times m$ matrices $\mathcal{H}$. The columns of $H \sim \mathcal{H}$ are distributed uniformly over all vectors in W_c, and the number of sample points in $\mathcal{H}$ is $\binom{n}{c}^{2d}$.

Call a matrix H *good* if it is a parity check matrix of a code of distance at least $2d+1$. We will show that a

[5]In fact, we will need a d-wise independent set over a domain D that does not necessarily have a prime number of elements. One way to achieve this is to embed D into some $\mathbb{F}_q$, where $|D| \le q < 2|D|$, and identify each element of D with one or two elements of $\mathbb{F}_q$. Note that the distribution over D will not be uniform, but this will not make a difference in the asymptotic calculations so for sake of clarity we ignore the issue.

random matrix $H \sim \mathcal{H}$ is good with nonzero probability. To construct a good matrix, we exhaustively search all matrices in $\mathcal{H}$ until we find a good one. To test if a particular matrix H, is good, we compute all products Hx, where $x \in \mathbb{F}_2^m$ has Hamming weight between 1 and $2d$, and reject if any of these products evaluate to zero. Using standard implementations of $2d$-wise independent spaces, this can be done within the advertised time and space complexities.

Let p_w denote the probability that for a particular $x \in W_w$, we have $Hx = 0$. Then by a union bound,

$$\Pr_{H \sim \mathcal{H}}[H \text{ is not good}] \leq \sum_{w=2}^{2d} \binom{m}{w} p_w. \tag{8}$$

We now bound p_w. Consider the $[n] \times [w]$ matrix consisting of the columns of H indexed by the one entries of x. We can interpret this matrix as the adjacency matrix of a bipartite graph G with $[n]$ vertices on the left, and $[w]$ vertices on the right, each of degree c. If $Hx = 0$, then each left vertex of G must have even degree. In particular, it is possible to pair up the edges of G so that each pair of edges shares the same left vertex. Consider a particular such pairing of edges, say $(e_1, f_1), \ldots, (e_{wc/2}, f_{wc/2})$. We bound the probability of this pairing. Let P_i denote the event that e_i and f_i share the same left vertex. Even when conditioned on $P_1, \ldots, P_{i-1}$, the probability of P_i is at most $1/(n-c)$, so that

$$\Pr[P_1 \wedge \cdots \wedge P_{wc/2}] \leq \frac{1}{(n-c)^{wc/2}}.$$

On the other hand, the number of possible pairings of the edges into wc pairs is $(wc)!/2^{wc/2}$, so that

$$p_w \leq \frac{(wc)!}{[2(n-c)]^{wc/2}}.$$

Substituting into (8), and using Stirling's estimate for the factorial, we conclude that H is good with probability less than one as long as $m = \Omega((e\sqrt{2}/2cd)^c (n-c)^{c/2})$. □

5. HITTING SET GENERATORS FOR LOW-DEGREE POLYNOMIALS

By Theorem 3.1, any hitting set generator for low degree polynomials with good density gives rise to a pseudorandom generator. We turn to investigate the construction of hitting set generators in two models of computation: uniform arithmetic circuits, and arithmetic circuits where every element of the output depends only on a constant number of elements in the input.

Note that the construction in Theorem 3.1 has the following property: If G is a circuit of size s that is a hitting set generator in either of the models under consideration, then G' is a circuit of size $s + O(m)$ in the same model, where m is the number of field elements output by G.

Let $\mathcal{F}_{m,d}$ denote the family of nonzero polynomials over $\mathbb{F}$ of degree d over m variables.

THEOREM 5.1. *For every integer $m > 0$, $d > 0$, fraction $\epsilon > 0$, and set $S \subseteq \mathbb{F}$ of size at least $d^2 \log^2 m/\epsilon$, there exists a hitting set generator $G : S^n \to \mathbb{F}^m$ of density $1 - \epsilon$ for $\mathcal{F}_{m,d}$, where $n = 2d(\log m/\log\log m + O(1))$. Moreover, G can be represented by an arithmetic circuit over $\mathbb{F}$ of size $\tilde{O}(md)$ that is constructible in time $\tilde{O}(md)$.*

PROOF. Let H be the matrix from Lemma 4.2. Let $G = (G_1, \ldots, G_m)$, where $G_j(x_1, \ldots, x_n) = \prod_{i=1}^n x_i^{H_{i,j}}$.

By Lemma 4.1, for every $p \in \mathcal{F}_{m,d}$, the polynomial $r = p \circ G$ is nonzero. By construction, each G_j can have degree at most nq, so r has degree at most dnq. By the Schwartz-Zippel Lemma, it follows that r vanishes on at most an ϵ fraction of the points in S. □

Note that the seed length of G in bits (for optimal S) is $n \log |S| = O(d \log m \log(d/\epsilon))$. We observe that any hitting set generator for $\mathcal{F}_{m,d}$ must have seed length at least $\Omega(d \log m)$, as by interpolation we can construct a nonzero polynomial in $\mathcal{F}_{m,d}$ that vanishes on an arbitrary set of this size.

We now turn to the construction of generators where every element in the output depends on c elements of the input. By the same argument as in the proof of Theorem 5.1, we obtain the following:

THEOREM 5.2. *For every integer $m > 0$, $d > 0$, fraction $\epsilon > 0$, and set $S \subseteq \mathbb{F}$ of size at least cd/ϵ, there exists a hitting set generator $G : S^n \to \mathbb{F}^m$ of density at least $1 - \epsilon$ for $\mathcal{F}_{m,d}$, where $n = O(c^2 d^2 m^{2/c})$, and each output element of G depends on at most c inputs. Moreover, G can be represented by an arithmetic circuit over $\mathbb{F}$ of size $O(mc)$ that is constructible in time $O(m^{4d})$.*

We note the following lower bound in this model:

THEOREM 5.3. *For every field $\mathbb{F}$ and hitting set generator $G : \mathbb{F}^n \to \mathbb{F}^m$ of nonzero density against linear tests where every output element depends on at most c input elements, we have $m \leq \binom{n}{c} |\mathbb{F}|^c$.*

PROOF. Suppose that $m > \binom{n}{c} |\mathbb{F}|^c$. Then there must exist a set $D \subseteq [n]$ of size c such that more than $|\mathbb{F}|^c$ of the functions $G_1, \ldots, G_m$ depend only on inputs in D. However, the space of functions $\mathbb{F}^D \to \mathbb{F}$ has dimension $|\mathbb{F}|^c$ as a linear space over $\mathbb{F}$, so there must be a nontrivial linear dependence between these functions. Contradiction. □

6. PROOFS OF THE MAIN THEOREMS

PROOF OF THEOREM 1.1. We choose G_1 to be a hitting set generator of density $\epsilon^2/16d^2$ for polynomials of degree $3d^2$ in $2m-1$ variables, and G_2 to be a hitting set generator of density $\epsilon^2/16d^2$ for polynomials of degree $\max(\frac{3}{2}d^4 - 2d^3 + \frac{1}{2}d^2, 3d^2)$ in $m-1$ variables. By Theorem 5.1, we can take $G_1 : S^{n/2} \to \mathbb{F}^m$ and $G_2 : S^{n/2} \to \mathbb{F}^m$, where S has size $d^{10} \log^2 m \cdot 1/\epsilon^2$, and $n = O(d^4 \log m/\log\log m)$. Applying Theorem 3.1 to G_1 and G_2, we obtain a pseudorandom generator $G : S^n \times \mathbb{F}^2 \to \mathbb{F}^m$ for degree d polynomials of bias $O(\epsilon + d^2|\mathbb{F}|^{-1/2} + d^6|\mathbb{F}|^{-1}$. The arithmetic circuit size of G is the sum of the circuit sizes of G_1 and G_2 plus $O(m)$. □

PROOF OF THEOREM 1.2. We choose G_1 to be a hitting set generator of density $\epsilon^2/3d^2$ for polynomials of degree $3d^2$ in $2m-1$ variables, and G_2 to be a hitting set generator of density $\epsilon^2/3d^2$ for polynomials of degree $\max(\frac{3}{2}d^4 - 2d^3 + \frac{1}{2}d^2, 3d^2)$ in $m-1$ variables. Moreover we require that each output of G_1 and G_2 depends on at most $(c-2)/3$ inputs. By Theorem 5.2, we can take $G_1 : S^{n/2} \to \mathbb{F}^m$ and $G_2 : S^{n/2} \to \mathbb{F}^m$, where S has size cd^6/ϵ^2, and $n = O(c^2 d^8 m^{6/(c-2)})$. Applying Theorem 3.1 we obtain the desired pseudorandom generator G. The arithmetic circuit size follows, and since each output of G is of the form $\omega_i s + \eta_i t + \nu_i$, it depends on at most $2 + 3 \cdot (c-2)/3 = c$ inputs. □

7. OTHER APPLICATIONS

An improved hitting set generator for sparse polynomials Klivans and Spielman [11] studied the problem of derandomizing polynomial identity tests for sparse polynomials. Their main result can be interpreted as a construction of a hitting set generator for this class of tests. Let Let $\mathcal{F}_{M,m,d}$ be the family of all nonzero polynomials over a field $\mathbb{F}$ with at most M monomials, m variables, and degree d.

THEOREM 7.1 ([11, THEOREM 4]). *For every $\epsilon > 0$, if $|\mathbb{F}| \geq (md/\epsilon)^6$ then there is a hitting set generator for $\mathcal{F}_{M,m,d}$ of density $1-\epsilon$ and seed length $O(\log(Mmd/\epsilon))$ that runs in time polynomial in m, $\log d$ and $\log 1/\epsilon$.*

Using Theorem 5.1, we can obtain the following improvement in the case when the number of variables is substantially larger than the degree:

THEOREM 7.2. *For every $\epsilon > 0$, if $\mathbb{F}$ has size at least $(d \log m/\epsilon)^{O(1)}$, then there exists a hitting set generator for $\mathcal{F}_{M,m,d}$ of density $1-\epsilon$ with seed length $O(\log(Md \log m/\epsilon))$ that runs in time polynomial in m, $\log d$ and $\log 1/\epsilon$.*

PROOF. Let $G : \mathbb{F}^n \to \mathbb{F}^m$ be the generator from Theorem 5.1. Note that if p is in $\mathcal{F}_{M,m,d}$, then $p \circ G$ is in $\mathcal{F}_{M,n,d'}$, where $n = O(d \log m/\log\log m)$ and $d' = O(d^2 \log^2 m)$. Now let G' be the generator for $\mathcal{F}_{M,n,d'}$ from Theorem 7.1. Then the composition $G \circ G'$ is a generator for $\mathcal{D}_{M,m,d}$ with the advertised parameters. □

An arithmetic hitting set generator for the binary field We show a construction of an arithmetic hitting set generator for low degree polynomials over the binary field. Our construction is similar to those described in Section 4, but requires somewhat stronger properties. We need the following construction of combinatorial designs used by Nisan and Widgerson [17]:

LEMMA 7.3. *For every $k > 0$, there is a $(k \log_2 m, \log_2 m)$ combinatorial design $(S_1, \ldots, S_m)$ over the universe $[n]$, with $n = O(k^2 \log m)$. Moreover, the design can be constructed in time $m^{O(k^2)}$.*

We also need the following version of the Schwartz-Zippel lemma for binary fields. A polynomial is *multilinear* if the individual degree of all its variables is either zero or one.

LEMMA 7.4. *Let p be a nonzero multilinear polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$ of total degree at most d. Then*

$$\Pr[p(x_1, \ldots, x_n) \neq 0] \geq 2^{-d},$$

for $(x_1, \ldots, x_n)$ chosen uniformly at random.

Given $p \in \mathbb{F}_2[x_1, \ldots, x_n]$, the *multilinearization* of p is the unique multilinear polynomial $r \in \mathbb{F}_2[x_1, \ldots, x_n]$ such that $p(x_1, \ldots, x_n) = r(x_1, \ldots, x_n)$ for all $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$. The multilinearization of a monomial $x_{i_1}^{\alpha_1} \ldots x_{i_k}^{\alpha_k}$, where $\alpha_1, \ldots, \alpha_k > 0$ the monomial $x_{i_1} \ldots x_{i_k}$. Note that multilinearization is linear with respect to addition of polynomials.

Let $\mathcal{F}_{m,d}$ denote the set of nonzero multilinear polynomials over $\mathbb{F}_2$ in m variables of total degree at most d.

THEOREM 7.5. *There exists a hitting set generator for $\mathcal{F}_{m,d}$ of density at least m^{-2d^2} with seed length $O(d^2 \log m)$ that is computable by an arithmetic circuit over $\mathbb{F}_2$ of size $O(md^2 \log m)$ and constructible in time $m^{O(d^2)}$.*

PROOF. Let $(S_1, \ldots, S_m)$ be the combinatorial design from Lemma 7.3 with parameter $k = 2d$. We define the generator $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ by

$$G_j(x_1, \ldots, x_n) = \prod_{i \in S_j} x_i.$$

Given a polynomial $p \in \mathcal{F}_{m,d}$ in variables $y_1, \ldots, y_m$, $p \circ G$ is a polynomial of degree at most $2d^2 \log_2 m$ over $\mathbb{F}_2$. Let r denote the multilinearization of $p \circ G$. We argue that r must be nonzero. For this, it is sufficient to show that any two distinct terms in p give rise to distinct terms in r. Without loss of generality, assume that the two distinct terms in r are $A = y_1, \ldots, y_p$ and $B = y_{b+1} \ldots y_q$, where $b > 0$, $p \leq d$, and $q - b \leq d$. Let A' and B' denote the terms obtained after performing the substitution $y_j = \prod_{i \in S_j} x_i$.

Let $S = (S_2 \cup \cdots \cup S_p) \cup (S_{b+1} \cup \cdots \cup S_q)$. We show that there exists an index $k \in [n]$ such that $k \in S_1 - S$:

$$\begin{aligned} |S_1 - S| &\geq |S_1| - \sum_{i=2}^{p} |S_1 - S_i| - \sum_{i=b+1}^{q} |S_1 - S_i| \\ &\geq 2d \log_2 m - (d-1) \log_2 m - d \log_2 m > 0. \end{aligned}$$

It follows that the variable x_k has degree one in the term A', but has degree zero in the term B'. Since this property is preserved by multilinearization, the corresponding terms in r will be distinct.

Since $r(x_1, \ldots, x_n)$ is nonzero and is of degree at most $2d^2 \log_2 m$, by Lemma 7.4 r does not vanish on at least a m^{-2d^2} fraction of its inputs. □

Acknowledgments I thank Dragos Ghioca, Elchanan Mossel, Bjorn Poonen, Luca Trevisan, Emanuele Viola, Hoeteck Wee, and Avi Wigderson for helpful discussions, and the anonymous referees for helpful comments.

8. REFERENCES

[1] N. Alon, O. Goldreich, J. Hastad, and R. Peralta. Simple constructions of almost k-wise independent random variables. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*, pages 544–553, 1990.

[2] A. Andreev, A. Clementi, and J. Rolim. A new general derandomization method. *Journal of the ACM*, 45(1):179–213, 1998.

[3] B. Applebaum, Y. Ishai, and E. Kushilevitz. Cryptography in NC^0. In *Proceedings of the 45th IEEE Symposium on Foundations of Computer Science*, pages 166–175, 2004.

[4] E. Ben-Sasson, M. Sudan, S. Vadhan, and A. Wigderson. Randomness-efficient low degree tests and short PCPs via epsilon-biased sets. In *Proceedings of the 35th ACM Symposium on Theory of Computing*, pages 612–621, 2003.

[5] A. Cafure and G. Matera. Improved explicit estimates on the number of solutions of equations over a finite field. `arXiv:math.NT/0405302 v1`, 2004.

[6] M. Cryan and P. Miltersen. On pseudorandom generators in NC^0. In *Proceedings of the MFCS'01*, 2001.

[7] M. D. Huang and Y. C. Wong. Solvability of systems of polynomial congruences modulo a large prime. *Computational Complexity*, 8:227–257, 1999.

[8] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. In *Proceedings of the 35th ACM Symposium on Theory of Computing*, pages 355–364, 2003.

[9] E. Kaltofen. Effective noether irreducibility forms and applications. *Jornal of Computer and System Sciences*, 50(2):274–295, 1995.

[10] S. Kalyanaraman and C. Umans. On obtaining pseudorandomness from error-correcting codes. Manuscript, 2005.

[11] A. Klivans and D. Spielman. Randomness efficient identity testing. In *Proceedings of the 33rd ACM Symposium on Theory of Computing*, pages 216–223, 2001.

[12] S. Lang. *Algebra*. Addison-Wesley, Third edition, 1993.

[13] M. Luby, B. Veličković, and A. Wigderson. Deterministic approximate counting of depth-2 circuits. In *Proceedings of the 2nd Israeli Symposium on Theory of Computing and Systems*, pages 18–24, 1993.

[14] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[15] E. Mossel, A. Shpilka, and L. Trevisan. On epsilon-biased generators in NC_0. In *Proceedings of the 44th IEEE Symposium on Foundations of Computer Science*, pages 136–145, 2003.

[16] J. Naor and M. Naor. Small-bias probability spaces: efficient constructions and applications. In *Proceedings of the 22nd ACM Symposium on Theory of Computing*, pages 213–223, 1990.

[17] N. Nisan and A. Wigderson. Hardness vs. randomness. *Jornal of Computer and System Sciences*, 49(2):149–167, 1994.

[18] W. A. Schmidt. Zur methode von Stepanov. *Acta Arithmetica*, 24:247–267, 1973.

[19] W. M. Schmidt. A lower bound for the number of solutions of equations over finite fields. *Journal of Number Theory*, 6(6):448–480, 1974.

[20] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[21] E. Viola. Pseudorandom bits for constant depth circuits with one arbitrary symmetric gate. In *Proceedings of the 20th IEEE Conference on Computational Complexity*, 2005. To appear.

[22] A. Weil. Sur les courbes algébriques et les variétés qui s'en déduisent. *Actualites Scientifiques et Industrielles*, 1041, 1948.

[23] R. E. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of EUROSAM 79*, pages 216–226, 1979.

APPENDIX

A. A TECHNICAL PROPOSITION

Let $\mathcal{P}$ be a property of polynomials $g \in \mathbb{F}[s,t]$. We say that $\mathcal{P}$ is *independent of parametrization* if for any affine transformation $T(s,t) = (a_1 s + b_1 t + c_1, a_2 s + b_2 t + c_2)$, $a_i, b_i, c_i \in \mathbb{F}$ such that $a_1 b_2 - a_2 b_1 \neq 0$, $\mathcal{P}$ holds for $g(T(s,t))$ if and only if $\mathcal{P}$ holds for $g(s,t)$.

The following Proposition is used in the proofs of Section 2. (The proof is in the full version of the paper.)

PROPOSITION A.1. *Assume $n \geq 2$. Let $\mathcal{P}$ be any property of polynomials in $\mathbb{F}[s,t]$ that is independent of parametrization, and $f \in \mathbb{F}[x_1, \ldots, x_n]$. Suppose that the polynomial $g(s,t) = f(s+\nu_1, \omega_2 s + \eta_2 t + \nu_2, \ldots, \omega_n s + \eta_n t + \nu_n)$ satisfies $\mathcal{P}$ with probability $1-\epsilon$ over random $\nu_{1\ldots n}, \omega_{2\ldots n}, \nu_{2\ldots n} \in \mathbb{F}$. Then*

$$\Pr_{H \sim \mathcal{H}_n}[f|_H \text{ satisfies } \mathcal{P}] \geq 1 - \epsilon - 10|\mathbb{F}|^{-1}.$$

B. BCH CODES

In this section we recall the definition of non-binary BCH codes through their parity check matrices, and state certain properties that are useful for our application. The properties that we need are standard and can be found, for example, in the book by MacWilliams and Sloane [14].

Let q be a prime, d, l, be positive integers, $N = q^l$, and α a generator of the multiplicative group $\mathbb{F}_N^\times$. The *(primitive) BCH code* $BCH_q(N,d)$ over $\mathbb{F}_q$ is the $\mathbb{F}_q$ kernel of the matrix $G \in \mathbb{F}_N^{(d-1)\times N}$ given by $G_{i,j} = \alpha^{i(j-1)}$. Note that the code is a linear subspace of $\mathbb{F}_q$. Since the matrix G has full rank over $\mathbb{F}_N$, it follows that $BCH_q(M,d)$ has minimum distance at least d over $\mathbb{F}_q$. Next, we show that the co-dimension of $BCH_q(M,d)$ over $\mathbb{F}_q$ is at most $l(d-1)$; to do so, we exhibit a specific parity check matrix $H \in \mathbb{F}_q^{l(d-1)\times N}$ for $BCH_q(N,d)$ of rank at least d.

We think of $\mathbb{F}_N$ as an l-dimensional $\mathbb{F}_q$-vector space by identifying each element $a_0 + a_1\alpha + \cdots + a_{l-1}\alpha^{l-1} \in \mathbb{F}_N$ with the vector $(a_0, \ldots, a_{l-1}) \in \mathbb{F}_q^N$. Then multiplication by $x \in \mathbb{F}_m$ is a linear map in $\mathbb{F}_q^N$. Let $M_x \in \mathbb{F}^{l\times l}$ be the matrix representing this linear map with respect to the standard basis. The following lemma is easy to verify:

LEMMA B.1. *Let H be the matrix obtained from G by replacing the i,jth entry $G_{i,j}$ with the first column of $M_{G_{i,j}}$. Then H has rank at least d over $\mathbb{F}_q^{l(d-1)\times N}$.*

For given q, l and d, the matrix H can be constructed in time $\tilde{O}(Ndl^3)$: A generator α for $\mathbb{F}_N$ (represented by a minimal polynomial r_α) can be found in time $O(m)$, and for every i,j, the matrix $M_{G_{i,j}}$ can be computed as the $i(j-1)$-th power of M_α, which can be done in time $\tilde{O}(l^2)$.