Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 175 (2013)

HITTING SETS FOR LOW-DEGREE POLYNOMIALS WITH OPTIMAL DENSITY

VENKATESAN GURUSWAMI AND CHAOPING XING

Abstract. We give a length-efficient puncturing of Reed-Muller codes which preserves its distance properties. Formally, for the Reed-Muller code encoding n-variate degree-d polynomials over $\mathbb{F}_q$ with $q \gtrsim d/\delta$, we present an explicit (multi)-set $S \subseteq \mathbb{F}_q^n$ of size $N = \mathrm{poly}(n^d/\delta)$ such that every nonzero polynomial vanishes on at most δN points in S. Equivalently, we give an explicit hitting set generator (HSG) for degree-d polynomials of seed length $\log N = O(d \log n + \log(1/\delta))$ with "density" $1-\delta$ (meaning every nonzero polynomial is nonzero with probability at least $1-\delta$ on the output of the HSG). The seed length is optimal up to constant factors, as is the required field size $\Omega(d/\delta)$.

Plugging our HSG into a construction of Bogdanov (STOC'05) gives explicit pseudorandom generators for n-variate degree-d polynomials with error ε and seed length $O(d^4 \log n + \log(1/\varepsilon))$ whenever the field size satisfies $q \gtrsim d^6/\varepsilon^2$.

Our approach involves concatenating previously known HSGs over large fields with multiplication friendly codes based on algebraic curves. This allows us to bring down the field size to the optimal bounds. Such multiplication friendly codes, which were first introduced to study the bilinear complexity of multiplication in extension fields, have since found other applications, and in this work we give a further use of this notion in algebraic pseudorandomness.

1. Introduction

The Reed-Muller code $\mathcal{RM}(q, d, n)$ consists of the evaluations of n-variate polynomials over $\mathbb{F}_q$ of total degree at most d at all points in $\mathbb{F}_q^n$, where $\mathbb{F}_q$ denotes the field with q elements. It is one of classic families of algebraic codes; the binary ($q = 2$) case was introduced back in 1954 and has been extensively studied in the coding theory literature. Reed-Muller codes over large fields ($q > d$) have found many fascinating applications in complexity theory due to their rich algebraic structure, which endows them with valuable local testability, self-correctability, and list-decodability properties (see [19] for a survey). When $d < q$, which is the parameter regime of focus in this paper, the Reed-Muller code is a linear code with dimension $\binom{n+d}{d}$ and relative distance $1 - d/q$. For $d \ll q$, the relative distance is excellent; however, the rate of the code is rather poor as roughly n^d message symbols get encoded into q^n codeword symbols.

Standard probabilistic arguments show that one can improve the rate of the Reed-Muller code by "puncturing" it to a subset $\mathcal{S} \subseteq \mathbb{F}_q^n$ of $\approx n^d/\delta$ positions so that the resulting code still has relative distance at least $1 - \delta$, for $\delta \gtrsim d/q$. Said differently, let $P_q(n, d)$ denote the set of n-variate polynomials over $\mathbb{F}_q$ of total degree at most d. One can have a *hitting set generator* (HSG) $\mathcal{G} : \{1, 2, \ldots, N\} \to \mathbb{F}_q^n$ with seed length $\log N \leqslant O(d \log n + \log(1/\delta))$ such

Venkatesan Guruswami is with Computer Science Department, Carnegie Mellon University, Pittsburgh, PA 15213, USA. *email:* guruswami@cmu.edu.

Chaoping Xing is with Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore. *email:* xingcp@ntu.edu.sg.

ISSN 1433-8092

that for every nonzero $f \in P_q(n,d)$, $\Pr_{i\in[N]}[f(\mathcal{G}(i)) = 0] \leqslant \delta$. We say that such a map $\mathcal{G}$ is a HSG of *density* $1-\delta$.

As is typical in pseudorandomness, the challenge is to match this performance with a *deterministically* constructed puncturing $\mathcal{S}$ of the Reed-Muller code (or equivalently, an explicit HSG). For simplicity of description below, let us assume that $n \geqslant q$. As $\delta \geqslant d/q$, we can restrict attention to HSGs with seed length $O(d \log n)$ of density $1-O(d/q)$, or equivalently a punctured version of the Reed-Muller code with code length $n^{O(d)}$ that has relative distance $1-O(d/q)$ (i.e., nearly as large as the original $1-d/q$ bound). Note that when $d = 1$, we are simply asking for a linear code with relative distance close to $1-1/q$, and many such explicit codes with good rate are known – one can have a relative distance of $1-1/q-\varepsilon$ for any desired $\varepsilon > 0$ with code length $\mathrm{poly}(n/\varepsilon)$ or even $n/\varepsilon^{O(1)}$ (see, for instance, [16, 1, 11]; in fact one can ensure that every nonzero codeword has a fraction $1/q \pm \varepsilon$ of each field element). Our main result (Theorem 4.2) is an explicit length-efficient puncturing of Reed-Muller codes preserving its distance properties:

Theorem 1.1 (Main; stated here for $n \geqslant q$)**.** *There is an explicit multiset $\mathcal{S} \subseteq \mathbb{F}_q^n$ with $|\mathcal{S}| = N \leqslant n^{O(d)}$ such that for every nonzero degree-d n-variate polynomial f over $\mathbb{F}_q$, f vanishes on at most a fraction $\delta \leqslant 2d/q$ of the points in $\mathcal{S}$. Given an index $i \in \{1,2,\ldots,N\}$, the i'th element of $\mathcal{S}$ can be computed in* $\mathrm{poly}(n)$ *time.*

One can even take $\delta \leqslant d/q + O(d/q^2)$ in the above result (see Remark 2 after Theorem 4.2). In other words, we construct an explicit HSG of density $1-O(d/q)$ for the space $P_q(n,d)$ of polynomials, with seed length $O(d \log n)$. We also note that *both* the required field size (which is $\Omega(d/\delta)$) and seed length are optimal up to constant factors.

Various constructions of hitting set generators for $P_q(n,d)$ with seed length $O(d \log n)$ were known before, but the best result (implicit in [12]) still needed a field size that was super-linear in d/δ. For more details on previous work on HSGs, see Section 1.2.

Derandomized length-efficient versions of the Reed-Muller code which preserve its distance are interesting in their own right, and also have applications to *pseudorandom generators* (PRGs) that fool low-degree polynomials. Specifically, Bogdanov [2] reduced the problem of constructing PRGs for degree-d polynomials to the problem of constructing HSGs for degree-$\mathrm{poly}(d)$ polynomials with density close to 1. Plugging our HSGs from Theorem 1.1 as a black-box into Bogdanov's reduction yields the following corollary for PRGs:

Theorem 1.2. *For field size $q \geqslant \Omega(d^6/\varepsilon^2)$, there is an explicit pseudorandom generator with seed length $O(d^4 \log n + \log(1/\varepsilon))$ that fools polynomials in $P_q(n,d)$ with error $\varepsilon > 0$, and that is computable in time* $\mathrm{poly}(n, d, \log q)$*,*

1.1. **Our Techniques.** The idea behind our hitting set construction is quite simple. We start with known optimal seed length hitting sets over a large enough extension field (say $\mathbb{F}_{q^k}$) of $\mathbb{F}_q$. We then reduce the field size to $\mathbb{F}_q$ by encoding $\mathbb{F}_{q^k}$ into a vector in $\mathbb{F}_q^m$ using a "multiplication friendly" inner code of large relative distance. The seed length of the overall HSG equals the sum of the seed length of the original HSG and $\log m$, and the density is at least $1-\rho-\varsigma$ if the original HSG has density $1-\rho$ and the inner code has relative distance $1-\varsigma$.

Multiplication friendly codes are linear codes with the property that the encoding of a product of d field elements equals the coordinate-wise product of the encodings of those elements. Such codes can be constructed using algebraic curves and they were first introduced in the context of the bilinear complexity of multiplication in extension fields in a famous

work [6]. In this work, we give a new use of such codes to construct good puncturings of Reed-Muller codes.

The specific instantiations of our concatenation approach is to start with a construction of Klivans and Spielman [13], bring down the field size to $O(d^2/\delta^2)$ using certain algebraic-geometric codes, followed by reduction to the optimal $\Theta(d/\delta)$ bound using Reed-Solomon codes. Alternately one can start with a construction due to Lu [12], and reduce the field size to $\Theta(d/\delta)$ in a single step using Reed-Solomon codes. We next discuss these and other prior works on hitting set constructions.

1.2. **Prior work.** Constructing PRGs for low-degree polynomials has a rich history, starting with early work on ε-biased sets for fooling linear polynomials [16, 1, 15, 2, 3, 14, 20]. The best generator for constant degree polynomials is due to Viola [20], which achieves a seed length of $O(d \log n + d2^d \log(1/\varepsilon))$ by summing d independent low-bias generators for the linear case. Our contribution to PRGs follows simply by plugging HSGs into Bogdanov's reduction in [2], so below we only discuss works on constructing hitting sets.

Constructing hitting sets (of positive density) is equivalent to the problem of black-box polynomial identity testing where the goal is to ascertain if an input n-variate low-degree polynomial is identically zero, given oracle access to polynomial (that allows querying its value at any desired point in $\mathbb{F}_q^n$). The set of query points presented to the oracle must form a hitting set in order for the algorithm to correctly identify nonzero polynomials.

Dvir and Shpilka presented noisy interpolation sets for degree-d polynomials which yield punctured Reed-Muller codes of relative distance bounded away from 0 (albeit exponentially small in d), along with efficient decoding algorithms for such codes [9]. We next turn to puncturings of Reed-Muller codes with large relative distance (or equivalently, hitting sets with density close to 1) which is our focus in this work.

Klivans and Spielman gave a randomness efficient polynomial identity test [13, Thm 4] which yields a density $(1-\delta)$ hitting set of size $\mathrm{poly}(n^d/\delta)$ provided $q \geqslant (nd/\delta)^6$. Their approach was based on reduction to a univariate problem via an isolation lemma. Subsequently, in his work on PRGs for low-degree polynomials [2], Bogdanov used BCH codes to reduce the number of variables from n to about $\approx d \log n$ and constructed a hitting set (again with $\mathrm{poly}(n^d/\delta)$ elements) over smaller fields of size $q \geqslant (d \log n)^2/\delta$.

Lu [12] extended Bogdanov's approach by reducing the number of variables in mutiple ways (instead of the single BCH code based reduction in [2]). While Lu focuses on HSGs with positive density rather than density close to 1, one can pick parameters in the construction of [12, Sec. III] to construct HSGs with density $1-\delta$ over a reduced field size of $q \geqslant (d/\delta)^{1+c}$ for any $c > 0$ (the constant in the seed length will get multiplied by $1/c$). Equivalently, one can get density $1-\delta$ for $\delta \geqslant (d/q)^{1+c}$, compared to the optimal $\delta = \Theta(d/q)$ bound. One can also pick parameters in Lu's construction to work with $q = O(d/\delta)$, but the seed length will incur a multiplicative $\log(d/\delta)$ factor and thus not be optimal up to constant factors. Thus, it was not possible to get *both* seed length and field size optimal up to constant factors prior to our work.

Recently, Cohen and Ta-Shma [7] put forth an approach for constructing hitting sets using algebraic-geometric codes (in a very different way compared to our use in multiplication friendly codes). Their approach works when the field size is at least $\Omega(d^2/\delta^2)$ (which is slightly worse than Lu's bound) but the time to compute the HSG has an exponential dependence on d.

Upon completion of our work, we learned about the independent work of Bshouty [4] who takes a very similar approach to reduce the field size in hitting sets (and several other algebraic and combinatorial constructs). In his terminology, a *tester* for a family of functions $\mathcal{F}$ reducing $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$ is a map $L : \mathbb{F}_{q^t} \to \mathbb{F}_q^m$ such that if $f(\alpha) \neq 0$ for $f \in \mathcal{F}$ and $\alpha \in \mathbb{F}_{q^t}$, then $f(L(\alpha)_i) \neq 0$ for at least one coordinate $i \in \{1, 2, \ldots, m\}$. Using algebraic function fields, Bshouty constructs testers for the family of low-degree polynomials, which by definition allow one to construct hitting sets over $\mathbb{F}_q$ based on a hitting set over an extension field $\mathbb{F}_{q^t}$. The construction idea is similar to ours, though it is not abstracted via the notion of multiplication friendly pairs. Also, the work does not explicitly address the density of hitting sets (such statements can, however, be deduced by modifications to the parameters and proofs).

1.3. **Organization.** We begin with preliminaries on punctured Reed-Muller codes and hitting set/pseudorandom generators for polynomials, and a simple lower bound on seed length and field size for HSGs, in Section 2. In Section 3 we describe multiplication friendly codes, their construction from algebraic curves, and our main use of these codes in constructing punctured Reed-Muller codes via concatenation. We instantiate the concatenation approach with various components to deduce our optimal density hitting sets in Section 4. The result for PRGs obtained by plugging in our HSG into Bogdanov's reduction appears in Section 5. Finally, we conclude with some open questions in Section 6.

2. Preliminaries

Let $\mathbb{F}_q$ denote the finite field with q elements. We denote by $\mathbf{x}$ the variable vector $(x_1, \ldots, x_n)$. The multivariate polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$ is denoted by $\mathbb{F}_q[\mathbf{x}]$. For a vector $I = (e_1, \ldots, e_n) \in \mathbb{Z}^n_{\geqslant 0}$, we denote by $\mathbf{x}^I$ the monomial $\prod_{i=1}^n x_i^{e_i}$. Thus, we can write a polynomial of total degree at most d by $f(\mathbf{x}) = \sum_{\mathrm{wt}_L(I) \leqslant d} a_I \mathbf{x}^I$, where $a_I \in \mathbb{F}_q$ and $\mathrm{wt}_L(I) = \sum_{i=1}^n e_i$ is the Lee weight. A polynomial in $\mathbb{F}_q[\mathbf{x}]$ is called a degree-d polynomial if its total degree is at most d. In the setting throughout the paper, we assume that $d < q$.

For an integer N, we denote $[N] := \{1, 2, \ldots, N\}$. Also, for positive quantities a, b, we use $a \gtrsim b$ to mean $a \geqslant Cb$ for some absolute constant C. Unless specified otherwise, all logarithms in this paper will be to base 2.

Definition 1. *The Reed-Muller code $\mathcal{RM}(q, d, n)$ is defined by $\{(f(\mathbf{u}))_{\mathbf{u} \in \mathbb{F}_q^n} : \ f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}];\ \deg(f(\mathbf{x})) \leqslant d\}$, where $\deg(f(\mathbf{x}))$ denotes the total degree of $f(\mathbf{x})$.*

$\mathcal{RM}(q, d, n)$ is a q-ary $[q^n, \binom{n+d}{d}, q^n(1 - d/q)]$-linear code. The relative minimum distance of $\mathcal{RM}(q, d, n)$ is approximately 1 if $q \gg d$.

To define our punctured Reed-Muller codes, we adopt the definition of multiset and simple set from [9]. For N vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N \in \mathbb{F}_q^n$ (may not be distinct), the subset $\mathcal{S} = \{\mathbf{u}_1, \ldots, \mathbf{u}_N\}$ is called a multiset. If all $\mathbf{u}_i$ are distinct, $\mathcal{S}$ is called a simple set.

Definition 2. *Let $\mathcal{S}$ be a multiset of $\mathbb{F}_q^n$. The* extended punctured Reed-Muller code *with support $\mathcal{S}$, denoted $\mathcal{RM}_{\mathcal{S}}(q, d, n)$, is defined by $\{(f(\mathbf{u}))_{\mathbf{u} \in \mathcal{S}} : \ f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}];\ \deg(f(\mathbf{x})) \leqslant d\}$.*

The length of $\mathcal{RM}_{\mathcal{S}}(q, d, n)$ is clearly $|\mathcal{S}|$. However, we do not know the dimension and minimum distance of $\mathcal{RM}_{\mathcal{S}}(q, d, n)$ for an arbitrary subset $\mathcal{S}$ of $\mathbb{F}_q^n$. Note that $\mathcal{RM}_{\mathcal{S}}(q, d, n)$ is indeed a punctured code from the Reed-Muller code $\mathcal{RM}(q, d, n)$ if $\mathcal{S}$ is simple. However, $\mathcal{RM}_{\mathcal{S}}(q, d, n)$ may not be a usual punctured Reed-Muller code for a multiset $\mathcal{S}$.

Definition 3. *For a real $\delta \in (0,1)$, a function $\mathcal{G} : [N] \to \mathbb{F}_q^n$ is called a* hitting set generator *(HSG) of density $1-\delta$ for degree-d polynomials over $\mathbb{F}_q$ if for every non-zero degree-d polynomial $f(\mathbf{x})$, one has $\Pr_{i\in[N]}[f(\mathcal{G}(i)) = 0] \leqslant \delta$, i.e., $\mathrm{wt}_H(f(\mathcal{G}(1)), \ldots, f(\mathcal{G}(N))) \geqslant N(1-\delta)$, where wt_H stands for the Hamming weight. The number $\log N$ is called the seed length of the hitting set generator $\mathcal{G}$.*

It is straightforward to verify that hitting set generators and extended punctured Reed-Muller codes are actually equivalent. More precisely, we have the following result.

Proposition 2.1. *There exists a q-ary extended punctured Reed-Muller code with parameters $[N, \binom{n+d}{d}, \geqslant N(1-\delta)]$ if and only if there exists a hitting set generator $\mathcal{G}$ of density $1-\delta$ for degree-d polynomials over $\mathbb{F}_q$ with seed length $\log N$.*

Proof. Let $\mathcal{RM}_{\mathcal{S}}(q,d,n)$ be a q-ary extended punctured Reed-Muller code with parameters $[N, \binom{n+d}{d}, \geqslant N(1-\delta)]$. Write $\mathcal{S} = \{\mathbf{u}_1, \ldots, \mathbf{u}_N\}$. Since the dimension of $\mathcal{RM}_{\mathcal{S}}(q,d,n)$ is $\binom{n+d}{d}$ which is the same as the dimension of the space of all degree-d polynomials, it is clear that the vector $(f(\mathbf{u}_1), \ldots, f(\mathbf{u}_N))$ is nonzero for any nonzero degree d polynomial $f(\mathbf{x}) \in \mathbb{F}_q[x]$. Consider the map $\mathcal{G} : [N] \to \mathbb{F}_q^n$ defined by $i \mapsto \mathbf{u}_i$. Then $\mathrm{wt}_H(f(\mathcal{G}(1)), \ldots, f(\mathcal{G}(N))) = \mathrm{wt}_H(f(\mathbf{u}_1), \ldots, f(\mathbf{u}_N)) \geqslant N(1-\delta)$.

Conversely, assume that there exists a hitting set generator $\mathcal{G}$ of density $1-\delta$ for degree-d polynomials over $\mathbb{F}_q$ with seed length $\log N$. Let $\mathcal{S} = \{\mathcal{G}(i) : i \in [N]\}$ and consider the extended punctured Reed-Muller code $\mathcal{RM}_{\mathcal{S}}(q,d,n)$. Then it is easy to see that $\mathcal{RM}_{\mathcal{S}}(q,d,n)$ is a q-ary $[N, \binom{n+d}{d}, \geqslant N(1-\delta)]$-linear code. □

The following result shows that, if there exists a q-ary extended punctured Reed-Muller code $\mathcal{RM}_{\mathcal{S}}(q,d,n)$ with parameters $[N, \binom{n+d}{d}, \geqslant N(1-\delta)]$, then the ground field size q and code length N cannot be too small.

Proposition 2.2. *If there exists an extended punctured Reed-Muller code $\mathcal{RM}_{\mathcal{S}}(q,d,n)$ with parameters $[N, \binom{n+d}{d}, \geqslant N(1-\delta)]$, then $q \geqslant d/\delta$ and $N \gtrsim \binom{n+d}{d}/\delta$ (i.e., $\log N \geqslant \Omega(d \log n + \log(1/\delta))$ when $d \ll n$).*

Proof. Let $\mathcal{S} = \{\mathbf{u}_1, \ldots, \mathbf{u}_N\}$ with $\mathbf{u}_i = (u_{i1}, \ldots, u_{in})$ for $1 \leqslant i \leqslant N$. For an element $\alpha \in \mathbb{F}_q$, denote by N_α the cardinality of the set $\{i \in [N] : u_{i1} = \alpha\}$. Then we have $\sum_{\alpha\in\mathbb{F}_q} N_\alpha = N$. Label elements of $\mathbb{F}_q$ as $\alpha_1, \ldots, \alpha_q$. Without loss of generality, we may assume that $N_{\alpha_1} \geqslant N_{\alpha_2} \geqslant \cdots \geqslant N_{\alpha_q}$. Hence, $dN_{\alpha_j} \leqslant \sum_{i=1}^d N_{\alpha_i}$ for any $d+1 \leqslant j \leqslant q$. This gives

$$N = \sum_{i=1}^{q} N_{\alpha_i} \leqslant \sum_{i=1}^{d} N_{\alpha_i} + \frac{q-d}{d} \sum_{i=1}^{d} N_{\alpha_i} = \frac{q}{d} \sum_{i=1}^{d} N_{\alpha_i}. \tag{1}$$

Consider the polynomial $f(\mathbf{x}) = \prod_{i=1}^d (x_1 - \alpha_i)$. Then $f(\mathbf{x})$ has at least $\sum_{i=1}^d N_{\alpha_i}$ zeros in $\mathcal{S}$, i.e, $\mathrm{wt}_H(f(\mathbf{u}_1), \ldots, f(\mathbf{u}_N)) \leqslant N - \sum_{i=1}^d N_{\alpha_i} \leqslant N(1-d/q)$ by (1). The desired result on field size q follows from that fact that the minimum distance of $\mathcal{RM}_{\mathcal{S}}(q,d,n)$ is at least $N(1-\delta)$.

Finally, applying the Singleton bound gives $N+1 \geqslant \binom{n+d}{d} + N(1-\delta)$, i.e, $N \geqslant (\binom{n+d}{d} - 1)/\delta$. □

There is a close relation between hitting set generators and pseudorandom generators as shown in [2]. Before giving the precise statement of [2], we first define pseudorandom generators.

Definition 4. *Let ε be a real in $(0,1)$. A function $\mathcal{G} : [N] \to \mathbb{F}_q^n$ is called an ε-bias pseudorandom generator for degree-d polynomials over $\mathbb{F}_q$ if for every degree d polynomial $f \in \mathbb{F}_q[\mathbf{x}]$, the output distribution of $f(\mathbf{u})$ for a uniformly random $\mathbf{u} \in \mathbb{F}_q^n$ is ε-close in statistical distance to the distribution $f(\mathcal{G}(s))$ for a uniformly random $s \in [N]$.*

Below we quote Bogdanov's result from [2] on constructing PRGs using HSGs.

Proposition 2.3. *Let $\mathcal{G}_1 : [M] \to \mathbb{F}_q^{2n-1}$ be a hitting set generator of density $1-\delta$ for degree-$3d^2$ polynomials over $\mathbb{F}_q$. Let $\mathcal{G}_2 : [N] \to \mathbb{F}_q^{n-1}$ be a hitting set generator of density $1-\delta$ for degree-$3d^4$ polynomials over $\mathbb{F}_q$. Then the function $\mathcal{G} : [M] \times [N] \times \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q^n$ given by*

$$\mathcal{G}(i,j,s,t) \mapsto (s + v_1, w_2 s + z_2 t + v_2, \ldots, w_n s + z_n t + v_n)$$

is a pseudorandom generator for degree-d polynomials of bias $O(\sqrt{\delta} d + d^2/\sqrt{q} + d^6/q)$, where $\mathcal{G}_1(i) = (v_1, \ldots, v_n, w_2, \ldots, w_n)$ and $\mathcal{G}_2(j) = (z_2, \ldots, z_n)$.

3. Concatenation via multiplication friendly pairs

We have already shown in Section 2 that a q-ary extended punctured Reed-Muller code with parameters $[N, \binom{n+d}{d}, \geqslant N(1-\delta)]$ is equivalent to a hitting set generator $\mathcal{G}$ of density $1-\delta$ for degree-d polynomials over $\mathbb{F}_q$ with seed length $\log N$. In this section, we present a concatenation of extended punctured Reed-Muller codes over larger fields via multiplication friendly pairs to produce extended punctured Reed-Muller codes over smaller fields.

3.1. **Multiplication friendly pairs.** Multiplication friendly pairs were first introduced by D.V. Chudnovsky and G.V. Chudnovsky [6] as bilinear multiplication algorithms to study complexity in extension fields. Following the brilliant work by D.V. Chudnovsky and G.V. Chudnovsky, Shparlinski, Tsfasman and Vlăduţ [17] systematically studied this idea and extended the result in [6]. Recently, multiplication friendly pairs were used to study multiplicative secrets sharing [5]. Both of the above applications used only bilinear multiplication friendly pairs, while we use high order multiplication friendly pairs in this section. High order multiplication friendly pairs were implicitly used to study strongly multiplicative secret sharing to get very efficient zero-knowledge for circuit satisfiability in [8].

For d vectors $\mathbf{c}_i = (c_{i1}, c_{i2}, \ldots, c_{im}) \in \mathbb{F}_q^m$ $(i = 1, 2, \ldots, d)$, we denote by $\mathbf{c}_1 * \mathbf{c}_2 * \cdots * \mathbf{c}_d$ the coordinate-wise product $(\prod_{i=1}^d c_{i1}, \prod_{i=1}^d c_{i2}, \ldots, \prod_{i=1}^d c_{im})$. In particular, we denote by $\mathbf{c}^{*d}$ the vector $(c_1^d, \cdots, c_n^d)$ if $\mathbf{c} = (c_1, \ldots, c_n)$.

For an $\mathbb{F}_q$-linear code C, we denote by C^{*d} the linear code

$$\mathrm{Span}\{\mathbf{c}_1 * \mathbf{c}_2 * \cdots * \mathbf{c}_d : \ \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_d \in C\}.$$

Definition 5. *A pair (π, ψ) is called a $(d,k,m)_q$-multiplication friendly pair if π is an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q^m$ and ψ is an $\mathbb{F}_q$-linear map from $\mathbb{F}_q^m$ to $\mathbb{F}_{q^k}$ such that $\pi(1) = (1, \ldots, 1)$ and $\psi(\pi(\alpha_1) * \cdots * \pi(\alpha_d)) = \alpha_1 \cdots \alpha_d$ for all $\alpha_i \in \mathbb{F}_q$. A $(2,k,m)_q$-multiplication friendly pair is also called a bilinear multiplication friendly pair.*

We have an additional requirement in the above definition of multiplication friendly pairs compared with the original definition [6, 17], namely we require that $\pi(1) = (1, \ldots, 1)$. This ensures that (π, ψ) is a $(d,k,m)_q$-multiplication friendly pair whenever (π, ψ) is a $(t,k,n)_q$-multiplication friendly pair for $t \geqslant d$. This is because

$$\psi(\pi(\alpha_1) * \cdots * \pi(\alpha_d)) = \psi(\pi(\alpha_1) * \cdots * \pi(\alpha_d) * \pi(1) * \cdots * \pi(1)) = \alpha_1 \cdots \alpha_d \ ,$$

where there are $(t-d)$ $\pi(1)$'s in the above formula.

Lemma 3.1. *If (π,ψ) is a $(d,k,m)_q$-multiplication friendly pair, then π is injective.*

Proof. Suppose that π is not injective. Then there exists a nonzero element $\alpha \in \mathbb{F}_{q^k}$ such that $\pi(\alpha)=\mathbf{0}$. Hence $0=\psi(\mathbf{0})=\psi(\pi(\alpha)*\pi(1)*\cdots*\pi(1))=\alpha$, which is a contradiction. □

The construction of multiplication friendly pairs in [6] is through algebraic curves over finite fields and variants of this construction have been extensively studied in literature. In fact, the only way to construct asymptotically good multiplication friendly pair is through algebraic curves over finite field [6, 17, 5]. Furthermore, most of these constructions focus on the bilinear case, i.e., $d=2$. Also, there is an additional requirement in Definition 5 for our purpose. For completeness, we present a construction of $(d,k,m)_q$-multiplication friendly pair via algebraic curves over finite fields, or equivalently global function fields over finite fields. For a function field $F/\mathbb{F}_q$ and a rational place P_∞ and an integer $a \geqslant 0$, we define the Riemann-Roch space $\mathcal{L}(aP_\infty)$ to be the set of functions of F that have at most a poles at P_∞ and no poles at any other place. By the Riemann-Roch theorem, $\mathcal{L}(aP_\infty)$ is a finite dimensional $\mathbb{F}_q$-vector space with dimension at least $a-g+1$, where g is the genus of F. We refer to [18] for detailed background on function fields.

Lemma 3.2. *Let $F/\mathbb{F}_q$ be a function field of genus g with at least $m+1$ distinct rational places $P_\infty, P_1, \ldots, P_m$ and a place Q of degree k. If $2g-1+k<m/d$, then there exists a $(d,k,m)_q$-multiplication friendly pair (π,ψ) such that $(\pi(\mathbb{F}_{q^k}))^{*d}$ is a q-ary linear code with minimum distance at least $m-d(2g-1+k)$.*

Proof. Consider the $\mathbb{F}_q$-linear map ϕ from $\mathcal{L}((2g-1+k)P_\infty)$ to the residue class field F_Q defined by $f \mapsto f(Q)$, where $f(Q)$ stands for the residue class in F_Q. Then the kernel of ϕ is $\mathcal{L}((2g-1+k)P_\infty - Q)$ and hence the image of ϕ has dimension $\dim_{\mathbb{F}_q}\mathcal{L}((2g-1+k)P_\infty) - \dim_{\mathbb{F}_q}\mathcal{L}((2g-1+k)P_\infty - Q) = k$. This implies that ϕ is surjective. It is clear that $\phi(1)$ is mapped the multiplicative identity 1 of F_Q.

Choose k functions $\{f_1,\ldots,f_k\}$ from $\mathcal{L}((2g-1+k)P_\infty)$ such that $\{\phi(f_1),\ldots,\phi(f_k)\}$ forms an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^k}$. Let V be the $\mathbb{F}_q$-subspace of $\mathcal{L}((2g-1+k)P_\infty)$ spanned by $\{f_1,\ldots,f_k\}$. Then ϕ derives an $\mathbb{F}_q$-isomorphism from V to F_Q as vector spaces. Let τ denote the $\mathbb{F}_q$-linear isomorphism from F_Q to V which is the inverse of ϕ.

First of all, note that $\tau(x)(Q)=\tau(\phi(x))=x$ for any $x \in F_Q$. Thus, one has $\alpha_1\cdots\alpha_d = \tau(\alpha)(Q)\cdots\tau(\alpha_d)(Q) = (\tau(\alpha_1)\cdots\tau(\alpha_d))(Q)$ for all $\alpha_i \in F_Q$. Consider the $\mathbb{F}_q$-linear map π from $\mathbb{F}_Q$ to $\mathbb{F}_q^n$ defined by $x \mapsto (\tau(x)(P_1),\ldots,\tau(x)(P_m))$. Then $\pi(1)=(1(P_1),\ldots,1(P_m))=(1,\ldots,1)$.

We consider an $\mathbb{F}_q$-linear map χ from $\mathcal{L}(d(2g-1+k)P_\infty)$ to $\mathbb{F}_q^m$ defined by $f \mapsto (f(P_1),\ldots,f(P_m))$. The kernel of χ is $\mathcal{L}(d(2g-1+k)P_\infty - \sum_{i=1}^m P_i)$ which is 0 since $d(2g-1+k)<m$. Therefore, it is injective and hence we can define ψ to be the $\mathbb{F}_q$-linear map from image of χ to F_Q by sending $\mathbf{u}$ to $\chi^{-1}(\mathbf{u})(Q)$. We can extend ψ to an $\mathbb{F}_q$-linear map from $\mathbb{F}_q^n$ to F_Q.

Now for any $\alpha_1,\ldots,\alpha_d \in F_Q$, we have

$$\begin{aligned}
\psi(\pi(\alpha_1)*\cdots*\pi(\alpha_d)) &= \psi(\tau(\alpha_1)(P_1)\cdots\tau(\alpha_d)(P_1),\ldots,\tau(\alpha_1)(P_m)\cdots\tau(\alpha_d)(P_m)) \\
&= \psi((\tau(\alpha_1)\cdots\tau(\alpha_d))(P_1),\ldots,(\tau(\alpha_1)\cdots\tau(\alpha_d))(P_m)) \\
&= (\tau(\alpha_1)\cdots\tau(\alpha_d))(Q) \\
&\quad \text{(note that } (\tau(\alpha_1)\cdots\tau(\alpha_d)) \in \mathcal{L}(d(2g-1+k)P_\infty)) \\
&= \alpha_1\cdots\alpha_d.
\end{aligned}$$

Finally, if $\sum a\pi(\alpha_1) * \cdots * \pi(\alpha_d) \in \pi(\mathbb{F}_{q^k})^{*d}$ is not zero, then $\psi(\sum a\pi(\alpha_1) * \cdots * \pi(\alpha_d)) = \sum a\alpha_1 \cdots \alpha_d \in \mathbb{F}_Q$ is not zero as well since ψ is injective on $\mathcal{L}(d(2g-1+k)P_\infty)$. On the other hand,

$$\sum a\pi(\alpha_1) * \cdots * \pi(\alpha_d) = \left(\tau\left(\sum a\alpha_1 \cdots \alpha_d\right)(P_1), \ldots, \tau\left(\sum a\alpha_1 \cdots \alpha_d\right)(P_m)\right)$$

and $\tau(\sum a\alpha_1 \cdots \alpha_d) \in \mathcal{L}(d(2g-1+k)P_\infty)$. Hence, $\sum a\pi(\alpha_1) * \cdots * \pi(\alpha_d)$ has at most $d(2g-1+k)$ zeros. This completes the proof. □

Example 3.3. Consider the rational function field $F/\mathbb{F}_q$. Then the genus of F is 0. If $k \geqslant 2$ and $q \geqslant m > d(k-1)$, then there exists a $(d,k,m)_q$-multiplication friendly pair (π, ψ) such that $(\pi(\mathbb{F}_{q^k}))^{*d}$ is a q-ary linear code of length m and relative minimum distance $1 - d(k-1)/m$.

Example 3.4. Let q be a square. We consider a tower of function fields over $\mathbb{F}_q$ which was introduced by Garcia and Stichtenoth [10]. The tower $(K_1, K_2, K_3, \ldots)$ is given by $K_e := \mathbb{F}_q(x_1, \ldots, x_e)$, with

$$x_{i+1}^{\sqrt{q}} + x_{i+1} = \frac{x_i^{\sqrt{q}}}{x_i^{\sqrt{q}-1} + 1} \qquad \text{for } \ i = 1, \ldots, e-1.$$

Let $F = K_e$. Then the number of rational places of F satisfies $N(F) \geqslant q^{(e-1)/2}(q - \sqrt{q}) + 1$. Moreover, $N(F)/g(F) \to \sqrt{q} - 1$. If k is large enough, then there are roughly q^k/k places of degree k by the Hasse-Weil bound [18]. Thus, there exists an $(d,k,m)_q$-multiplication friendly pair (π, ψ) such that $(\pi(\mathbb{F}_{q^k}))^{*d}$ is a q-ary linear code of length m and relative minimum distance $1 - d(2g(F) + k - 1)/m$, where $m \leqslant q^{(e-1)/2}(q - \sqrt{q})$.

3.2. **Extended punctured Reed-Muller codes via concatenation.** In this subsection, we concatenate extended punctured Reed-Muller codes over larger fields via multiplication friendly pairs to produce extended punctured Reed-Muller codes over smaller fields.

Let π be an $\mathbb{F}_q$-isomorphism between $\mathbb{F}_{q^k}$ and a q-ary $[m,k]$-linear code C. For a column vector $\mathbf{v} = (v_1, \ldots, v_n)^T \in \mathbb{F}_{q^k}^n$, we obtain an $n \times m$ matrix

$$\pi(\mathbf{v}) = \begin{pmatrix} \pi(v_1) \\ \cdot \\ \cdot \\ \cdot \\ \pi(v_n) \end{pmatrix}.$$

Denote by $\pi_i(\mathbf{v})$ the i-th column of $\pi(\mathbf{v})$ for $i = 1, 2, \ldots, m$. For $I = (e_1, \ldots, e_n) \in \mathbb{Z}_{\geqslant 0}^n$, we denote by $(\pi(\mathbf{v}))^I$ the vector

$$\begin{aligned} ((\pi_1(\mathbf{v}))^I, \ldots, (\pi_m(\mathbf{v}))^I) &= \left(\prod_{j=1}^n \pi_1(v_j)^{e_j}, \ldots, \prod_{j=1}^n \pi_m(v_j)^{e_j}\right) \\ &= (\pi_1(v_1), \ldots, \pi_m(v_1))^{*e_1} * \cdots * (\pi_1(v_n), \ldots, \pi_m(v_n))^{*e_n} \\ &= \pi(v_1)^{*e_1} * \cdots * \pi(v_n)^{*e_n} \ . \end{aligned}$$

Thus, if (π, ψ) is a $(d, k, m)_q$-multiplication friendly pair and $I = (e_1, \ldots, e_n) \in \mathbb{Z}^n_{\geqslant 0}$ with $\mathrm{wt}_L(I) \leqslant d$, then

$$\psi\left((\pi(\mathbf{v}))^I\right) = \prod_{j=1}^{n} v_j^{e_j} = \mathbf{v}^I$$

for any $\mathbf{v} = (v_1, \ldots, v_n)^T \in \mathbb{F}^n_{q^k}$.

Theorem 3.5. *If there exist a q^k-ary extended punctured Reed-Muller code $\mathcal{RM}_{\mathcal{S}}(q^k, d, n)$ with parameters $[M, \binom{n+d}{d}, \geqslant M(1-\rho)]$ and a $(d, k, m)_q$-multiplication friendly pair (π, ψ) such that $(\pi(\mathbb{F}_{q^k}))^{*d}$ has relative minimum distance at least $1 - \varsigma$, then one can construct a q-ary extended punctured Reed-Muller code $\mathcal{RM}_{\mathcal{T}}(q, d, n)$ with parameters $[mM, \binom{n+d}{d}, \geqslant mM(1-\rho-\varsigma)]$ for some multiset $\mathcal{T}$ of $\mathbb{F}^n_q$.*

Proof. Let $\mathcal{S} = \{\mathbf{u}_1, \ldots, \mathbf{u}_M\}$ with $\mathbf{u}_i \in \mathbb{F}^n_{q^k}$. Each $\mathbf{u}_i$ is viewed as a column vector. Let $\mathcal{T} = \{\pi_i(\mathbf{u}_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant M\}$. Then $\mathcal{T}$ is a multiset of $\mathbb{F}^n_q$.

Let $f(X)$ be a nonzero degree-d polynomial over $\mathbb{F}_q$. Then $|\{j \in [M] : f(\mathbf{u}_j) = 0\}| \leqslant \rho M$. Write $f(X) = \sum_{\mathrm{wt}_L(I) \leqslant d} a_I X^I$ with $I = (e_1, \ldots, e_n)$. Then

$$f(\pi_i(\mathbf{u}_j)) = \sum_{\mathrm{wt}_L(I) \leqslant d} a_I (\pi_i(\mathbf{u}_j))^I \ .$$

Hence,

$$(f(\pi_1(\mathbf{u}_j)), \ldots, f(\pi_m(\mathbf{u}_j))) = \sum_{\mathrm{wt}_L(I) \leqslant d} a_I ((\pi_1(\mathbf{u}_j))^I, \ldots, (\pi_m(\mathbf{u}_j))^I) = \sum_{\mathrm{wt}_L(I) \leqslant d} a_I (\pi(\mathbf{u}_j))^I)$$

and

$$\psi\left(f(\pi_1(\mathbf{u}_j)), \ldots, f(\pi_m(\mathbf{u}_j))\right) = \sum_{\mathrm{wt}_L(I) \leqslant d} a_I \psi((\pi(\mathbf{u}_j))^I) = f(\mathbf{u}_j) \ .$$

This implies that $(f(\pi_1(\mathbf{u}_j)), \ldots, f(\pi_m(\mathbf{u}_j)))$ is a nonzero vector and hence its Hamming weight is at least $(1-\varsigma)m$ as long as $f(\mathbf{u}_j)$ is not zero.

Thus, the total number of zeros of $\{f(\pi_i(\mathbf{u}_j)) : 1 \leqslant j \leqslant M,\ 1 \leqslant i \leqslant m\}$ is at most $\rho mM + (1-\rho)\varsigma mM \leqslant (\rho + \varsigma)mM$. The desired result follows. □

4. Good extended punctured Reed-Muller codes

In this section, we give efficient constructions of good extended punctured Reed-Muller codes through some known extended punctured Reed-Muller codes over larger fields.

In [12], a hitting set generator with nice parameters was constructed. As stated there, the result ensured positive density when the field size is at least d^{1+c} for any $c > 0$. By choosing parameters in the proof of Theorem 1 of [12] appropriately, specifically picking the prime p in that construction to be $\Theta(d/\delta)$, one can get density $(1-\delta)$ hitting sets provided the field size satisfies $q \gtrsim d^2/\delta^2$.[1] This yields the following result, stated in the equivalent language of extended punctured Reed-Muller codes.

[1] In fact, one can work with $q \gtrsim (d/\delta)^{1+c}$ for any $c > 0$, but our alphabet reduction works just as well with the quadratic bound.

Proposition 4.1. *(see* [12, Theorem 1]*) Let δ be a real in $(0,1)$. Given any $n, d \in \mathbb{Z}_{>0}$ and any finite field $\mathbb{F}_\ell$ such that $\ell \geqslant d^2/\delta^2$, there is an explicit ℓ-ary extended punctured Reed-Muller code with parameters $[M, \binom{n+d}{n}, (1-\delta)M]$ for $\log M = O(d \log n + \log(1/\delta))$. Furthermore, given an index i, $\alpha \in \mathbb{F}_\ell^n$ which is the i'th element of the puncturing multiset can be constructed in time $\mathrm{poly}(n, d, \log \ell)$.*

By combining Proposition 4.1 and Theorem 3.5 with Example 3.3, we immediately obtain our main result.

Theorem 4.2 (Main)**.** *Let δ be a real in $(0,1)$. Then for any $n, d \in \mathbb{Z}_{>0}$ and prime power $q \geqslant 2d/\delta$, there is a q-ary extended punctured Reed-Muller code with parameters $[N, \binom{n+d}{n}, (1-\delta)N]$ with $\log N = O(d \log n + \log(1/\delta))$. The i'th element of this puncturing can be constructed in $\mathrm{poly}(n, d, \log q)$ time.*

Proof. Let $m = \lceil \frac{2d}{\delta} \rceil$. Since $m \leqslant q$, by Example 3.3, there a $(d, 2, m)_q$-multiplication friendly pair (π, ψ) such that $(\pi(\mathbb{F}_{q^2}))^{*d}$ is a q-ary linear code of length m and relative minimum distance at least $1 - d/m \geqslant 1 - \delta/2$. By Proposition 4.1, there is a q^2-ary extended punctured Reed-Muller code with parameters $[M, \binom{n+d}{n}, (1-\delta/2)M]$ with $\log M = O(d \log n + \log(1/\delta))$. Thus, the desired result on the seed length follows from Theorem 3.5.

The hitting set generator in Proposition 4.1 can be computed in time $\mathrm{poly}(n, d, \log q)$. For any desired $j \in [m]$, the $\mathbb{F}_q$-symbol in the j'th location of multiplication friendly code used in Theorem 4.2 can be computed in time $\mathrm{poly}(\log q)$. Thus, the extended punctured Reed-Muller code given in Theorem 4.2 can be computed in $\mathrm{poly}(n, d, \log q)$ time, as claimed. □

Remark 1. By Proposition 2.2, both the seed length and field size in Theorem 4.2 are best possible up to constant factors.

Remark 2 (Punctured codes of distance $1 - d/q - o(d/q)$). Theorem 4.2 gives a punctured Reed-Muller code over $\mathbb{F}_\ell$ of relative distance $1 - O(d/\ell)$. By taking these codes over the field $\mathbb{F}_\ell = \mathbb{F}_{q^2}$, and concatenating them again with the $(d, 2, q)_q$-multiplication friendly pair of Example 3.3, we can get a q-ary extended punctured Reed-Muller code with parameters $[N, \binom{n+d}{d}, (1-\zeta)N]$ for $\zeta \leqslant d/q + O(d/q^2)$ and $N \leqslant \mathrm{poly}(n^d/\zeta)$.

Alternate concatenation scheme. Theorem 4.2 already gives an extended punctured Reed-Muller with the best possible parameters up to constant factors. Next, we are going to obtain the same result using an earlier construction in [13], to illustrate that our concatenation approach does not require very strong parameters as a starting point.

Proposition 4.3. *(see* [13, Theorem 4]*) For every $\delta > 0$, if ℓ is at least $(nd/\delta)^6$, then there is an explicit ℓ-ary extended punctured Reed-Muller code with parameters $[M, \binom{n+d}{n}, (1-\delta)M]$ with $\log M = O(d \log n + \log(1/\delta))$.*

To bring down the field size of the extended punctured Reed-Muller code in Proposition 4.3, we have to concatenate it with an asymptotically good multiplication friendly pair as the field size in Proposition 4.3 depends on n.

Proposition 4.4. *Let δ be a real in $(0,1)$. Then for any $n, d \in \mathbb{Z}_{>0}$ and prime power square r with $r = \Theta(d^2/\delta^2)$, there is an explicit r-ary extended punctured Reed-Muller code with parameters $[K, \binom{n+d}{n}, (1-\delta)K]$ with $\log K = O(d \log n + \log(1/\delta))$.*

Proof. Consider $\ell = r^k$-ary extended punctured Reed-Muller code with parameters $[M, \binom{n+d}{n}, (1-\delta/2)M]$ with $\log M = O(d \log n + \log(1/\delta))$ and $\ell \leqslant (nd/\delta)^{O(1)}$, promised by Proposition 4.3. Then $k = O((\log d + \log n - \log \delta)/\log r)$. Consider a $(d, k, m)_r$-multiplication friendly pair given in Example 3.4 and apply Theorem 3.5, we get a r-ary extended punctured Reed-Muller code with parameters $[mM, \binom{n+d}{n}, (1-\delta)mM]$ for degree-d polynomials with the following parameters: field size r and seed length $\log m + \log M = \log m + O(d \log n/\delta)$ and density $1 - \delta/2 - d(k/m + 2/(\sqrt{r} - 1))$. Thus, if $m = \Theta(kd/\delta)$ and $r = \Theta(d^2/\delta^2)$, we get the desired result. □

Remark 3. (i) The hitting set generator in [13, Theorem 4] can be constructed in time $\mathrm{poly}(n, d, \log q)$.

(ii) The multiplication friendly pair used in Proposition 4.4 can be computed in time $\mathrm{poly}(r^k)$ by searching for a degree k place by brute force.

(iii) Thus, any desired location of the puncturing underlying the extended punctured Reed-Muller code constructed in Proposition 4.4 can be computed in time $\mathrm{poly}(nd/\delta, \log q)$.

As in Theorem 4.2, by concatenating the extended punctured Reed-Muller code given in Proposition 4.4 with the Reed-Solomon based $(d, 2, m)_q$ multiplication friendly pair of Example 3.3, we can obtain a similar result to Theorem 4.2 via this alternate approach.

5. Hitting set generator and pseudorandom generator

In this section, we first turn the result on extended punctured Reed-Muller codes given in Section 4 into a result on hitting set generator. Then by the reduction result of Proposition 2.3, we obtain a pseudorandom generator with the best-known parameters.

First, it follows from Theorem 4.2 and Proposition 2.1 that we have the following result on hitting set generators.

Theorem 5.1. *If $q \gtrsim d/\delta$, then there exists a hitting set generator $\mathcal{G} : [N] \to \mathbb{F}_q^n$ of density $1 - \delta$ for degree-d polynomials with seed length $\log N = O(d \log n + \log(1/\delta))$ that can be computed in time $\mathrm{poly}(n, d, \log q)$.*

Finally, we apply Bogdanov's reduction of Proposition 2.1 to Theorem 5.1 to obtain:

Theorem 5.2. *For any $\varepsilon \in (0, 1)$ and a prime power q with $q \gtrsim d^6/\varepsilon^2$, one can get an ε-bias pseudorandom generator $\mathcal{G} : [N] \to \mathbb{F}_q^n$ for degree-d polynomials with seed length $\log N = O(d^4 \log n + \log(1/\varepsilon))$ that can be computed in time $\mathrm{poly}(n, d, \log q)$.*

6. Concluding remarks

We conclude with some natural open questions raised by our work:

(1) Can one construct explicit puncturings of $\mathcal{RM}(q, d, n)$ which have relative distance $1 - d/q - \varepsilon$ for any desired $\varepsilon > 0$, and block length $\mathrm{poly}(n^d/\varepsilon)$? In this work, we achieved this for $\varepsilon \gtrsim d/q^2$. More ambitiously, can one construct pseudorandom generators with seed length $O(d \log n + \log(1/\varepsilon))$ over arbitrary fields $\mathbb{F}_q$, or at least when $q > d$?

(2) Can one efficiently decode any of the explicit puncturings of $\mathcal{RM}(q, d, n)$ given here or in the literature? In the terminology of [9], can one construct noisy interpolation sets that can correct a fraction ρ of errors bounded away from 0 as d increases (say, $\rho = 1/4$)?

(3) Can one apply our field size reduction approach directly to pseudorandom generators to get PRGs over smaller fields?

Acknowledgments

Research of the first author is supported in part by United States National Science Foundation grant number CCF-0963975, and a Packard Fellowship. The work of the second author is partially supported by the Singapore Ministry of Education under Tier 1 grant RG20/13 and the Singapore A*STAR SERC under Research Grant 1121720011.

We thank Gil Cohen for useful discussions about parameter choices in the hitting set construction of [12], Ariel Gabizon for pointing us to the related independent work [4], and Nader Bshouty for useful feedback and discussions about our write-up.

References

[1] N. Alon, O. Goldreich, J. Håstad, and R. Peralta, Simple Construction of Almost k-wise Independent Random Variables. *Random Struct. Algorithms* 3(3): 289-304 (1992)

[2] A. Bogdanov, Pseudorandom generators for low degree polynomials, In *Proceedings of the 37th annual STOC*, pages 21-30, 2005.

[3] A. Bogdanov and E. Viola, Pseudorandom Bits for Polynomials. *SIAM J. Comput.* 39(6): 2464-2486 (2010)

[4] N. H. Bshouty, Testers and their applications, In *Proceedings of Innovations in Theoretical Computer Science (ITCS)*, pages 327-352, January 2014.

[5] H. Chan, I. Cascudo, R. Cramer and C. Xing, Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over Any Fixed Finite Field, In *Proceeding of 29th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5677, pp. 466-486, August 2009.

[6] D. V. Chudnovsky and G. V. Chudnovsky, Algebraic complexities and algebraic curves over finite fields. *Proc. Natl. Acad. Sci.* USA, vol. 84, no. 7, pp. 1739–1743, April 1987.

[7] G. Cohen and A. Ta-Shma, Pseudorandom Generators for Low Degree Polynomials from Algebraic Geometry Codes, *Electronic Colloquium on Computational Complexity (ECCC)*, TR13-155, (2013).

[8] R. Cramer, I. Damgaard and V. Pastro. Amortized Complexity of Zero-Knowledge Protocols for Multiplicative Relations, *Proceedings of 6th International Conference on Information Theoretic Security (IC-ITS)*, Springer Verlag LNCS, vol. 7412, pp. 62-79, 2012.

[9] Z. Dvir and A. Shpilka, Noisy Interpolating Sets for Low Degree Polynomials, *Theory of Computing*, vol. 7, pp. 1-18, 2011

[10] A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound, *Invent. Math.* 121, pp. 211-222, 1995.

[11] V. Guruswami and M. Sudan, List decoding algorithms for certain concatenated codes, In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 181-190, 2000.

[12] C. J. Lu, Hitting set generators for sparse polynomials over any finite fields, In *Proceedings of the 27th Annual Conference on Computational Complexity (CCC)*, pages 280-286, 2012.

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

[14] S. Lovett, Unconditional pseudorandom generators for low degree polynomials, In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 557-562, 2008.

[15] M. Luby, B. Velickovic, and A. Wigderson, Deterministic Approximate Counting of Depth-2 Circuits. In *Proceedings of the 2nd Israel Symposium on Theory of Computing Systems*, pages 18-24, 1993.

[16] J. Naor and M. Naor, Small-Bias Probability Spaces: Efficient Constructions and Applications, *SIAM J. Comput.* 22(4): 838-856 (1993)

[17] I. Shparlinski, M. Tsfasman and S. Vlăduţ, Curves with many points and multiplication in finite fields. *Lecture Notes in Math., vol. 1518*, Springer-Verlag, Berlin, 1992, pp. 145-169.

[18] H. Stichtenoth, *Algebraic function fields and codes,* Springer Verlag, 1993. (New edition: 2009).

[19] L. Trevisan, Some Applications of Coding Theory in Computational Complexity, *Electronic Colloquium on Computational Complexity (ECCC)*, TR04-043, (2004).

[20] E. Viola. The Sum of D Small-Bias Generators Fools Polynomials of Degree D. *Computational Complexity* 18(2): 209-217 (2009)

ECCC ISSN 1433-8092

http://eccc.hpi-web.de