arXiv:1604.01925v1 [cs.IT] 7 Apr 2016

On Multi-Point Local Decoding of Reed-Muller Codes

Ronald Cramer[*], Chaoping Xing[†] and Chen Yuan[‡]

Abstract

Reed-Muller codes are among the most important classes of locally correctable codes. Currently local decoding of Reed-Muller codes is based on decoding on lines or quadratic curves to recover one single coordinate. To recover multiple coordinates simultaneously, the naive way is to repeat the local decoding for recovery of a single coordinate. This decoding algorithm might be more expensive, i.e., require higher query complexity.

In this paper, we focus on Reed-Muller codes with evaluation polynomials of total degree $d \lesssim \sigma\sqrt{q}$ for some $\sigma \in (0,1)$. By introducing a local decoding of Reed-Muller codes via the concept of codex that has been used for arithmetic secret sharing [6, 7], we are able to locally recover arbitrarily large number k of coordinates simultaneously at the cost of querying $O(k\sqrt{q})$ coordinates, where q is the code alphabet size. It turns out that our local decoding of Reed-Muller codes shows (*perhaps surprisingly*) that accessing k locations is in fact cheaper than repeating the procedure for accessing a single location for k times. In contrast, by repetition of local decoding for recovery of a single coordinate, one has to query $\Omega(k\sqrt{q}\log k/\log q)$ coordinates for $k = q^{\Omega(\sqrt{q})}$ (and query $O(kq)$ coordinates for $k = q^{O(\sqrt{q})}$, respectively). Furthermore, our decoding success probability is $1-\epsilon$ with $\epsilon = O\left(\left(\frac{1}{\sqrt{q}}\right)^k\right)$. To get the same success probability from repetition of local decoding for recovery of a single coordinate, one has to query $O(k^2\sqrt{q}\log k/\log q)$ coordinates (or $O(k^2q)$ coordinates for $k = q^{O(\sqrt{q})}$, respectively). In addition, our local decoding also works for recovery of one single coordinate as well and it gives a better success probability than the one by repetition of local decoding on curves. The main tool to realize codex is based on algebraic function fields (or more precisely, algebraic geometry codes). Our estimation of success error probability is based on error probability bound for t-wise linearly independent variables given in [2].

[*] CWI, Amsterdam and Mathematical Institute, Leiden University (email: Ronald.Cramer@cwi.nl)

[†] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore (email: xingcp@ntu.edu.sg)

[‡] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore (email: ych04@hotmail.com)

1 Introduction

In some applications such as transmission of information over noise channels or data storage, people are often interested in a portion of data. Thus, one needs to decode only this portion of data in stead of the whole data. However, classical error-correcting codes are generally used to recover the whole information. Thus, it is demanded to have a special class of error-correcting codes, i.e., locally decodable (correctable) codes.

Although locally decodable (correctable) codes have been studied for about two decades, Reed-Muller codes and their variants are still among the most important classes of locally correctable codes. Therefore, local decoding of Reed-Muller codes plays significant role in this topic. There are various decodings of Reed-Muller codes such as local decoding, list decoding or local list decoding in literature [1, 4, 11, 15, 19, 20]. Among these decodings, there are basically two local decoding methods, i.e., decoding on lines and quadratic curves. Though decoding on quadratic curves can be generalized to decoding on higher power curves, it does not appear in literature. Almost all locally correctable codes including Reed-Muller codes focus on correction of one single coordinate [1, 3, 11, 15, 16, 17, 18, 23]. To recover multiple coordinates together, the naive way is to repeat these locally decodings. However, this idea does not work well when locally recovering a large number of coordinates simultaneously is demanded (see Subsection 1.5 below).

In this paper, we introduce a local decoding of Reed-Muller codes via the concept of codex that has been used for arithmetic secret sharing [6, 7]. Furthermore, realization of codex is through algebraic function field (or algebraic geometry codes). In literature, there is a construction of locally decodable (correctable) codes via algebraic function fields (or algebraic curves) with large automorphism groups [3, 13]. However, usage of algebraic curves in the present paper is not for purpose of construction of locally correctable codes, but locally decoding of Reed-Muller codes.

As the main consequence of our local decoding, we are able to locally correct arbitrarily large number k of coordinates simultaneously at the cost of querying $O(k\sqrt{q})$ coordinates, where q is the code alphabet size. This is not achievable by all other existing local decodings of Reed-Muller codes. In addition, our local decoding also works for recovery of one single coordinate as well. In this case, there is a trade-off between code dimension and success probability.

1.1 Locally correctable codes

In order to state our result more accurately, let us introduce locally correctable codes first.

Definition 1.1 A subset C of $\mathbb{F}_q^N$ is called a q-ary (r, δ, ϵ)-locally correctable code of length N if there exists a randomized algorithm $\mathcal{A}$ such that (i) for any $i \in [N]$ and $\mathbf{c} \in C$, $\mathbf{y} \in \mathbb{F}_q^N$ with $\mathrm{wt}_H(\mathbf{c}, \mathbf{y}) \le \delta N$, one has $\Pr[\mathcal{A}^{\mathbf{y}}(i) = c_i] \ge 1 - \epsilon$, where the probability is taken over random coin tosses of the algorithm $\mathcal{A}$ (note that c_i stands for the i-th coordinate of $\mathbf{c}$ and $\mathcal{A}^{\mathbf{y}}(i)$ stands for the output of $\mathcal{A}$ from $\mathbf{y}$ for the position at i); (ii) $\mathcal{A}$ makes at most r queries to $\mathbf{y}$.

The above definition is only for recovery of one single coordinate (or point). We can generalize it to a locally correctable code with recovery of multiple coordinates (or points).

Definition 1.2 A subset C of $\mathbb{F}_q^N$ is called a q-ary $(k; r, \delta, \epsilon)$-locally correctable code of length N if there exists a randomized algorithm $\mathcal{A}$ such that (i) for any $S \subseteq [N]$ with $|S| \le k$, and $\mathbf{c} \in C$, $\mathbf{y} \in \mathbb{F}_q^N$ with $\mathrm{wt}_H(\mathbf{c}, \mathbf{y}) \le \delta N$, one has $\Pr[\mathcal{A}^{\mathbf{y}}(S) = \mathbf{c}_S] \ge 1 - \epsilon$, where the probability is taken over random coin tosses of the algorithm $\mathcal{A}$ (note that $\mathbf{c}_S$ stands for the projection of $\mathbf{c}$ to S and $\mathcal{A}^{\mathbf{y}}(S)$ stands for the output of $\mathcal{A}$ from $\mathbf{y}$ for the positions at S); (ii) $\mathcal{A}$ makes at most r queries to $\mathbf{y}$.

Thus, a $(1; r, \delta, \epsilon)$-locally correctable code is an (r, δ, ϵ)-locally correctable code.

1.2 Reed-Muller codes

We denote by $\mathbf{x}$ the variable vector $(x_1, \dots, x_m)$. The multivariate polynomial ring $\mathbb{F}_q[x_1, \dots, x_m]$ is denoted by $\mathbb{F}_q[\mathbf{x}]$. For a vector $I = (e_1, \dots, e_m) \in \mathbb{Z}_{\geq 0}^m$, we denote by $\mathbf{x}^I$ the monomial $\prod_{i=1}^m x_i^{e_i}$. Thus, we can write a polynomial of total degree at most d by $f(\mathbf{x}) = \sum_{\mathrm{wt}_L(I) \leq d} a_I \mathbf{x}^I$, where $a_I \in \mathbb{F}_q$ and $\mathrm{wt}_L(I) = \sum_{i=1}^m e_i$ 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 $d < q$.

Definition 1.3 The Reed-Muller code $\mathrm{RM}(q, d, m)$ is defined by $\{(f(\mathbf{u}))_{\mathbf{u} \in \mathbb{F}_q^m} : f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}]; \deg(f(\mathbf{x})) \leq d\}$, where $\deg(f(\mathbf{x}))$ denotes the total degree of $f(\mathbf{x})$.

The dimension of the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $\binom{m+d}{d}$. In this paper, we focus on the case where $d \lesssim \sigma\sqrt{q}$ for a fixed real $\sigma \in (0, 1)$.

1.3 Known results

The simplest local decodings of Reed-Muller codes is called decoding on lines [23, Propositions 2.5]. The decoding on line can be generalized to decoding on quadratic curves [23, Proposition 2.6]. Both these decodings are very special cases of our codex decoding where a Reed-Solomon code with pairwise independent variables is used (see Example 4.1(i) and (ii)).

Proposition 1.4 *Let $0 < \sigma, \delta < 1$ be positive real. Let m and d be positive integers. Let q be a prime power.*

(i) *If $d \leq \sigma(q-1) - 1$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $(q-1, \delta, 2\delta/(1-\sigma))$-locally correctable for all positive real with $\delta < \frac{1-\sigma}{2}$.*

(ii) *If $d \leq \sigma(q-1)/2 - 1/2$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $\left(q-1, \delta, \epsilon = O_{\delta,\sigma}\left(\frac{1}{q}\right)\right)$-locally correctable for all positive real with $\delta < \frac{1-\sigma}{2}$, where the implied constant in $O_{\delta,\sigma}\left(\frac{1}{q}\right)$ is given in Example 4.1(ii).*

The purpose of (ii) in Proposition 1.4 is to increase the success probability of local decoding. As σ, δ are constant and q is usually large, Proposition 1.4(ii) gives much better success probability at the cost of a slightly smaller dimension.

As we are interested in the case where $d \lesssim \sigma\sqrt{q}$, we can reduce the query complexity in Proposition 1.4. We only consider modification of Proposition 1.4(ii) as Proposition 1.4(i) does not give an interesting result for our comparison.

Proposition 1.5 *Let $0 < \sigma, \delta < 1$ be a positive real. Let m and d be positive integers. Let q be a prime power with $d \leq \sigma\sqrt{q}/2 - 1/2$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $\left(\sqrt{q}, \delta, \epsilon = O_{\delta,\sigma}\left(\frac{1}{\sqrt{q}}\right)\right)$-locally correctable for all positive real with $\delta < \frac{1-\sigma}{2}$, where the implied constant in $O_{\delta,\sigma}\left(\frac{1}{\sqrt{q}}\right)$ is given in Example 4.1(ii).*

Although it does not appear in literature, generalization of local decoding on quadratic curves is quite straightforward in the following way. Assume that $f(\mathbf{u})_{\mathbf{u} \in \mathbb{F}_q^m}$ is transmitted and we want to recover $f(\mathbf{w})$ at position $\mathbf{w}$. Choose t independently random vectors $\mathbf{v}_1, \dots, \mathbf{v}_t$ and consider the degree t curve $\mathbf{w} + \sum_{i=1}^t x^i \mathbf{v}_i$. By using the error probability bound for t-wise independence (see Lemma 2.10), we obtain the following result (see Example 4.1(iii)).

Proposition 1.6 *Let $0 < \sigma, \delta < 1$ be a positive real and let $t \geq 4$ be an integer. Let m and d be a positive integer. Let q be a prime power such that $d \leq \sigma(q-1)/t - 1/t$; then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $\left(q-1, \delta, \epsilon = O\left(\left(\frac{\lambda_{\delta,\sigma} t}{q}\right)^t\right)\right)$-locally correctable for all positive real with $\delta < \frac{1-\sigma}{2}$, where $\lambda_{\delta,\sigma} = \frac{\sqrt{8}}{1-\sigma-2\delta}$ as given in Example 4.1(iii).*

In particular, by taking $t = \lfloor\sqrt{q}\rfloor$, the Reed-Muller code $\mathrm{RM}(q,d,m)$ *with* $d \le \sigma\sqrt{q}$ *is* $\left(q-1, \delta, O\left(\left(\frac{\lambda_{\delta,\sigma}}{\sqrt{q}}\right)^{\sqrt{q}}\right)\right)$*-locally correctable.*

Compared with decoding on lines in Proposition 1.4, local decoding on quadratic curves in Proposition 1.5 gives better probability. The local decoding on higher power curves in Proposition 1.6 gives the best probability

1.4 Our results

We consider both single point decoding and multiple point local decoding. For single point local decoding, we apply Hermitian codes and algebraic geometry codes from the Garcia-Stichtenoth tower (the results from Reed-Solomon codes are already given in Propositions 1.4-1.6); while for multiple point local decoding, we apply all three classes of codes, namely Reed-Solomon codes, Hermitian codes and algebraic geometry codes from the Garcia-Stichtenoth tower.

Theorem 1 [see Theorem 4.4] *Let $\sigma, \delta < 1$ be a positive reals satisfying $\delta < \frac{1-\sigma}{2}$. Let $t \ge 4$, m and d be positive integers. Let q be a square prime power. Let $e \ge 1$ be integer and let c be a positive constant. If $4 \le t \le cq^{e/2}$ and $d \le \sigma(\sqrt{q}-1)/(2+c)-1$, then the Reed-Muller code* $\mathrm{RM}(q,d,m)$ *is* $\left(q^{e/2}(\sqrt{q}-1)-1, \delta, \epsilon = O\left(\left(\frac{\lambda_{\delta,\sigma} t}{q^{e/2+1/2}}\right)^t\right)\right)$*-locally correctable, where $\lambda_{\delta,\sigma}$ is given in Proposition* 1.6 *and the exact formula of ϵ is given in Theorem 4.4.*

In particular, by taking $t = \lfloor q^{e/2}\rfloor$ (and replace σ by 3σ), the Reed-Muller code $\mathrm{RM}(q,d,m)$ *with* $d \le \sigma\sqrt{q}$ *is* $\left(t\sqrt{q}, \delta, O\left(\left(\frac{\mu_{\delta,\sigma}}{\sqrt{q}}\right)^t\right)\right)$*-locally correctable for $\delta < \frac{1-3\sigma}{2}$, where $\mu_{\delta,\sigma} = \frac{\sqrt{8}}{1-3\sigma-2\delta}$ (note that t can be arbitrarily large as e can be arbitrarily large).*

For local decoding to recover multiple coordinates, we only state the result based on the Garcia-Stichtenoth tower. We refer to Theorem 4.5 for local decoding of recovering multiple coordinates based on Reed-Solomon and Hermitian codes.

Theorem 2 [see Theorem 4.5(v)] *Let q be a prime power which is a square. Let $d > 1, t, m, k$ be positive integers. Let δ, σ be two reals in $(0,1)$ with $\delta < \frac{1-\sigma}{2}$. For two positive constants c and b, if $t \le cn/\sqrt{q}$ and $k \le bn/\sqrt{q}$, $k+n \le q^{e/2}(\sqrt{q}-1)$ and $d < \frac{\sigma\sqrt{q}}{b+c+2}$, then the Reed-Muller code* $\mathrm{RM}(q,d,m)$ *is an $(k;n,\delta,\epsilon)$-locally correctable code with* $\epsilon = 8\left(\frac{4t\delta+4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{n}\right)^t$.

In particular, by taking $k = t = \lfloor n/2\sqrt{q}\rfloor$ and $n = \left\lfloor \frac{\lfloor 2\sqrt{q}\rfloor}{1+\lfloor 2\sqrt{q}\rfloor} \times q^{e/2}(\sqrt{q}-1)\right\rfloor$ (and replace σ by 3σ), the Reed-Muller code $\mathrm{RM}(q,d,m)$ *with* $d \le \sigma\sqrt{q}$ *is* $\left(t\sqrt{q}, \delta, O\left(\left(\frac{\mu_{\delta,\sigma}}{\sqrt{q}}\right)^t\right)\right)$*-locally correctable for $\delta < \frac{1-3\sigma}{2}$, where $\mu_{\delta,\sigma} = \frac{\sqrt{8}}{1-3\sigma-2\delta}$ (note that t can be arbitrarily large as e can be arbitrarily large).*

1.5 Comparison

Let us compare our results given in Subsection 1.4 with the known results (or those derived from the known results). Note that we focus on the case where $d \lesssim \sigma\sqrt{q}$ for a real $\sigma \in (0,1)$. Let us start with multiple point local decoding.

(i) To obtain a k-multiple point local decoding from the single point decoding given in Proposition 1.5, one can repeat local decoding k times to get a $(k; k\sqrt{q}, \delta, \epsilon)$-locally correctable code with $\epsilon = O_{\sigma,\delta}\left(\frac{k}{\sqrt{q}}\right)$. Therefore, this method does not work when $k > \sqrt{q}$.

(ii) The other way is to first repeat local decoding to correct $f(\mathbf{u})$ at the same point $\mathbf{u}$ to increase probability, and then repeat the above procedure to correct multiple points with meaningful probability. Let us analyze this decoding idea in detail. To increase decoding success probability of the local decoding in Proposition 1.5, we can repeat local correction of $f(\mathbf{u})$ at $\mathbf{u}$ for s times. Denote by Y_i a binary random variable such that $Y_i = 1$ if the local decoding algorithm outputs a wrong answer in the i-th round and $Y_i = 0$ otherwise. It follows that $\Pr[X_i = 1] = b = \frac{\gamma_{\sigma,\delta}}{\sqrt{q}}$, where $\gamma_{\sigma,\delta} = \frac{\delta-\delta^2}{1-\sigma-2\delta}$ (see Example 4.1(ii) for this constant). Thus, we have

$$\Pr\left[\sum_{i=1}^{s} Y_i \geq \frac{s}{2}\right] = \sum_{i\geq s/2} \binom{s}{i} b^i(1-b)^{s-i} = O\left((2\sqrt{\gamma_{\sigma,\delta}})^s \left(\frac{1}{\sqrt{q}}\right)^{s/2}\right). \tag{1.1}$$

Therefore, we conclude that the Reed-Muller code $\mathrm{RM}(q,d,m)$ is $\left(s\sqrt{q},\delta,\epsilon'\right)$-locally correctable, where ϵ' is given in (1.1). By repeating the above decoding procedure to correct k points, we can also conclude that the Reed-Muller code $\mathrm{RM}(q,d,m)$ is $\left(k; ks\sqrt{q},\delta,k\epsilon'\right)$-locally correctable. To make the probability meaningful, one requires $k\epsilon' < 1$, i.e., $s = \Omega(\log k/\log q)$. This implies that the Reed-Muller code $\mathrm{RM}(q,d,m)$ is $(k; \Omega(kq\log k/\log q), \delta, O(1))$-locally correctable.

Similarly, if we do the same local decoding by applying Proposition 1.6, we conclude that the Reed-Muller code $\mathrm{RM}(q,d,m)$ is $\left(k; \Omega(k\sqrt{q}\log k/\log q), \delta, O(1)\right)$-locally correctable for $k = q^{\Omega(\sqrt{q})}$ (note that we take $t = \Theta(\sqrt{q})$ in Proposition 1.6 in order to get the same bound $d \lesssim \sigma\sqrt{q})$). For $k = q^{O(\sqrt{q})}$, repeating the decoding algorithm of Proposition 1.6 for k times directly yields a $(k; kq, \delta, O(1))$-locally correctable code $\mathrm{RM}(q,d,m)$.

(iii) By applying k-multiple point local decodings in Theorem 2, the number k is unbounded. This means that we can recover any number k of coordinates simultaneously with a high probability. At meanwhile, the number of queries is $O(\sqrt{q}k)$ (this is by no means possible for all other local decodings). By repeating local decoding described in (ii), to correct k points simultaneously, the query complexity given in (ii) is $\Omega(k\sqrt{q}\log k/\log q)$. This means that our local decoding of Reed-Muller codes shows (*perhaps surprisingly*) that accessing k locations is in fact cheaper than repeating the procedure for accessing a single location for k times. In addition, the decoding success probability in Theorem 2 is $1-\epsilon$ with $\epsilon = O\left(\left(\frac{\mu_{\sigma,\delta}}{\sqrt{q}}\right)^k\right)$. To get the same success probability from the repeating decoding algorithm discussed in the above (ii), the query complexity in (ii) becomes $O(k^2\sqrt{q}\log k/\log q)$ or $O(k^2 q)$ for $k = q^{O(\sqrt{q})}$, respectively.

Now we compare our local decoding of correcting one single coordinate with the one given in Proposition 1.5.

By the above (ii) in this subsection, we know that by applying repeating local decoding from Proposition 1.5 the Reed-Muller code $\mathrm{RM}(q,d,m)$ is $\left(s\sqrt{q}, \delta, O\left(\left(\frac{4\gamma_{\sigma,\delta}}{\sqrt{q}}\right)^{s/2}\right)\right)$-locally correctable. Thus, Theorem 1 gives the same number of queries, but a better success probability.

1.6 Our techniques

The main idea of our local decoding is realized through codex introduced in [6, 7]. A codex is nicely implemented in our local decoding because of several properties of codex: (i) a codex has high randomness and uniformity; (ii) a codex provides independent variables that are needed in local decoding of Reed-Muller codes; (iii) a codex also allows correction of errors. On the other hands, there are not many ways to construct codex. As far as we know, the only way to construct codex is through algebraic curves with many rational points (or more precisely algebraic geometry codes). We apply three classes of curves, i.e., projective line, Hermitian curve and the Garcia-Stichtenoth tower, to construction of codex and realize our local decoding. As for error probability, we make use of the error probability bound for t-wise linearly independent variables given in [2].

1.7 Organization

The paper is organized as follows. In Section 2, we introduce some preliminaries including definition of codex, some properties of codex, a construction of codex through algebraic geometry codes, error probability bounds and introduction to Hermitain curves the Garcia-Stichenoth tower. Our local decoding algorithm of Reed-Muller codes through codex is presented in Section 3. Finally we apply various codex to decoding algorithm in Section 3 to obtain our main results in Section 4.

2 Preliminaries

2.1 Codex

The concept of codex was first introduced in [6, 7, 9] for purpose of arithmetic secret sharing. A special case of codex in this paper was implicitly introduced in [8, 5].

Let $\mathbb{F}_q$ be a finite field of q elements. $\mathbb{F}_q^*$ denotes the multiplicative group of $\mathbb{F}_q$. Let n, t, d, r be positive integers with $d \geq 2$ and $1 \leq t < r \leq n$. Vectors in the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$ are denoted in boldface. If $\mathbf{u} \in \mathbb{F}_q^n$, its coordinates are denoted as $(u_i)_{i=1}^n$. Define $\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_q^n$. The standard inner-product on $\mathbb{F}_q^n$ is denoted $\langle \cdot, \cdot \rangle$. If $A \subset \{1, \ldots, n\}$ is non-empty, π_A denotes projection of $\mathbb{F}_q^n$ onto the A-indexed coordinates, i.e., $\pi_A(\mathbf{u}) = (u_i)_{i \in A}$ for all $\mathbf{u} \in \mathbb{F}_q^n$.

Definition 2.1 For $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, $\mathbf{u} * \mathbf{v}$ denotes the vector $(u_1 v_1, \ldots, u_n v_n) \in \mathbb{F}_q^n$. For an $\mathbb{F}_q$-linear code $C \subset \mathbb{F}_q^n$, the $\mathbb{F}_q$-linear code $C^{*d} \subset \mathbb{F}_q^n$, the *$d$-th power of C*, is defined as the $\mathbb{F}_q$-linear subspace generated by all terms of the form $\mathbf{c}_1 * \cdots * \mathbf{c}_d$ with $\mathbf{c}_1, \ldots, \mathbf{c}_d \in C$.

Note that if $\mathbf{1} \in C$, then $C = C^{*1} \subset C^{*2} \subset \ldots \subset C^{*d}$.

Consider the following special case of an arithmetic secret sharing scheme (SSS for short) which, in turn, is a special case of an arithmetic codex [7].

Definition 2.2 An $(n, t, d, r; \mathbb{F}_q^k/\mathbb{F}_q)$-codex is a pair (C, ψ) such that the following conditions are satisfied.

(i) $C \subset \mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear code and $\psi : C \longrightarrow \mathbb{F}_q^k$ is a surjective $\mathbb{F}_q$-vector space morphism.

(ii) It is *unital*, i.e., $\mathbf{1} \in C$ and $\psi(\mathbf{1}) = \mathbf{1}$.

(iii) (*t-privacy with uniformity*) For each $A \subset \{1, \ldots, n\}$ with $|A| = t$, the projection map

$$\pi_{\psi,A} : C \longrightarrow \mathbb{F}_q^k \times \mathbb{F}_q^t, \qquad \mathbf{c} \mapsto (\psi(\mathbf{c}), \pi_A(\mathbf{c}))$$

is surjective.

(iv) (*(d, r)-product reconstruction*) The map ψ extends uniquely to an $\mathbb{F}_q$-linear map $\psi : C^{*d} \longrightarrow \mathbb{F}_q^k$ such that the following holds.

(a) ψ satisfies the multiplicative relation

$$\psi(\mathbf{c}_1 * \cdots * \mathbf{c}_d) = \psi(\mathbf{c}_1) * \cdots * \psi(\mathbf{c}_d) \in \mathbb{F}_q^k,$$

for all $\mathbf{c}_1, \ldots, \mathbf{c}_d \in C$.

(b) ψ is r-wise determined, i.e., $\psi(\mathbf{z}) = \mathbf{0}$, for all $\mathbf{z} \in C^{*d}$ with $\pi_B(\mathbf{z}) = \mathbf{0}$ for some $B \subset \{1, \ldots, n\}$ with $|B| = r$.

Remark 2.3 (i) *Uniqueness* of ψ needs not be required separately, as it is implied by existence. Also note that, in fact, $\psi(\mathbf{c}_1 * \cdots * \mathbf{c}_{d'}) = \psi(\mathbf{c}_1) * \cdots * \psi(\mathbf{c}_{d'})$ for all $\mathbf{c}_1, \ldots, \mathbf{c}_{d'} \in C$ and all integers d' with $1 \leq d' \leq d$.

(ii) Given the above codex, we can define an arithmetic SSS, where each coordinate of $\mathbf{c}$ is a share and $\psi(\mathbf{c})$ is the secret (please refer to [7] for the details).

The following lemma is implied by t-privacy with uniformity (see [9, Chapter 12]).

Lemma 2.4 *Suppose $\mathcal{C} = (C, \psi)$ is an $(n, t, d, r; \mathbb{F}_q^k/\mathbb{F}_q)$-codex. Let $\mathbf{s} \in \mathbb{F}_q^k$. Suppose $A \subset \{1, \ldots, n\}$ with $|A| = t$. If $\mathbf{c} \in C$ is selected uniformly at random such that $\psi(\mathbf{c}) = \mathbf{s}$, then $\pi_A(\mathbf{c}) \in \mathbb{F}_q^t$ is uniformly random.*

Lemma 2.5 *Suppose $\mathcal{C} = (C, \psi)$ is an $(n, t, d, r; \mathbb{F}_q^k/\mathbb{F}_q)$-codex. If $\mathbf{z}+\mathbf{e} = \mathbf{z}'+\mathbf{e}'$ for some $\mathbf{z}, \mathbf{z}' \in C^{*d}$ and some $\mathbf{e}, \mathbf{e}' \in \mathbb{F}_q^n$ with $w_{\mathrm{H}}(\mathbf{e}) \leq \frac{n-r}{2}$ and $w_{\mathrm{H}}(\mathbf{e}') \leq \frac{n-r}{2}$, then $\psi(\mathbf{z}) = \psi(\mathbf{z}')$.*

In other words, there is "$\frac{n-r}{2}$-error correction in C^{*d} for the secret." It follows directly from (d, r)-product reconstruction: $\mathbf{z}, \mathbf{z}'$ agree in at least r coordinates (see [9, Chapter 12]).

2.2 A construction of codex

As far as we know, the only way to construct codex with $t = \Omega(n)$ is through algebraic geometry codes. In this subsection, we briefly introduce algebraic geometry codes and show how to construct codex.

For the convenience of reader, we start with some definitions and notations. The reader may refer to [21, 22].

An *algebraic function field* over $\mathbb{F}_q$ in one variable is a field extension $F \supset \mathbb{F}_q$ such that F is a finite algebraic extension of $\mathbb{F}_q(x)$ for some $x \in F$ that is transcendental over $\mathbb{F}_q$. It is assumed that $\mathbb{F}_q$ is its full field of constants, i.e., the algebraic closure of $\mathbb{F}_q$ in F is $\mathbb{F}_q$ itself.

Let $\mathbb{P}_F$ denote the set of places of F. A divisor is a formal sum $G = \sum_{P \in \mathbb{P}_F} a_P P$, where a_P are integers and are equal to zero except for finitely many P. For a divisor G of F, we define the Riemann-Roch space by $\mathcal{L}(G) := \{f \in F^* : \operatorname{div}(f) + G \geq 0\} \cup \{0\}$. Then $\mathcal{L}(G)$ is a finite dimensional space over $\mathbb{F}_q$ and its dimension $\dim_{\mathbb{F}_q}(G)$ is determined by the Riemann-Roch theorem which gives

$$\dim_{\mathbb{F}_q}(G) = \deg(G) + 1 - g(F) + \ell(K - G),$$

where K is a canonical divisor of degree $2g(F) - 2$, and $g(F)$ is the genus of F. Therefore, we always have that $\dim_{\mathbb{F}_q}(G) \geq \deg(G) + 1 - g(F)$ and the quality holds if $\deg(G) \geq 2g(F) - 1$.

Let k, t, n be positive integers. Suppose $Q_1, \ldots, Q_k, P_1 \ldots, P_n$ are distinct rational places of a function field F and denote by $\mathcal{Q}$ and $\mathcal{P}$ the set $\{Q_1, \ldots, Q_k\}$ and $\{P_1, \ldots, P_n\}$, respectively. Let G be a divisor of F such that $\operatorname{Supp}(G) \cap (\mathcal{P} \cup \mathcal{Q}) = \emptyset$. We define an algebraic geometry code of length $k + n$ as follows

$$C(G; \mathcal{Q} + \mathcal{P}) = \{(f(Q_1), \ldots, f(Q_k), f(P_1), \ldots, f(P_n) : f \in \mathcal{L}(G))\} \subseteq \mathbb{F}_q^k \times \mathbb{F}_q^n.$$

We also denote by $C(G; \mathcal{P})$ the code obtained from $C(G; \mathcal{Q}+\mathcal{P})$ by puncturing the first k positions.

Proposition 2.6 *Let F be a function field of genus $g(F)$ with two disjoint sets $\mathcal{Q} = \{Q_1, \ldots, Q_k\}$ and $\mathcal{P} = \{P_1, \ldots, P_n\}$ of rational places. Let $t \geq 1$, $d \geq 2, r \geq 1$ satisfy $n \geq r > d(2g(F) + k + t - 1)$. For a positive divisor G with $\deg(G) = 2g(F) + k + t - 1$ and $\operatorname{Supp}(G) \cap (\mathcal{P} \cup \mathcal{Q}) = \emptyset$, let C be the code $C(G; \mathcal{P})$ and define the map ψ from C to $\mathbb{F}_q^k$ given by $(f(P_1), \ldots, f(P_n)) \mapsto (f(Q_1), \ldots, f(Q_k))$ (note that the function f is uniquely determine by $(f(P_1), \ldots, f(P_n))$). Then (C, ψ) is an $(n, t, d, r; \mathbb{F}_q^k/\mathbb{F}_q)$-codex.*

Proof. It is clear that ψ is $\mathbb{F}_q$-linear and unital. To prove that ψ is subjective, we consider the kernel of ψ. The kernel clearly has dimension $\dim_{\mathbb{F}_q}(G - \sum_{i=1}^{k} Q_i)$ which is equal to $\deg(G) - k - g(F) + 1$ by the Riemann-Roch Theorem. Thus, the image of ψ has dimension $\dim_{\mathbb{F}_q}(G) - (\deg(G) - k - g(F) + 1) = k$. This implies that ψ is surjective. As $\deg(G) - (t + k) = 2g(F) - 1$, one can show t-privacy with uniformity in the same way.

Finally, we verify that it is (d, r)-product reconstruction. For a function $f \in \mathcal{L}(G) \subseteq F$, we denote by $\mathbf{b}_f$ and $\mathbf{c}_f$ the words $(f(Q_1), \dots, f(Q_k))$ and $(f(P_1), \dots, f(P_n))$, respectively. Thus, one has $\psi(\mathbf{c}_f) = \mathbf{b}_f$ for any $f \in \mathcal{L}(G)$. Furthermore, for d codewords $\mathbf{c}_{f_1} * \cdots * \mathbf{c}_{f_d}$ in $C(G, \mathcal{P})$ we have $\psi(\mathbf{c}_{f_1} * \cdots * \mathbf{c}_{f_d}) = \psi(\mathbf{c}_{f_1 \cdots f_d}) = \mathbf{b}_{f_1 \cdots f_d} = \mathbf{b}_{f_1} * \cdots * \mathbf{b}_{f_d} = \psi(\mathbf{c}_{f_1}) * \cdots * \psi(\mathbf{c}_{f_d})$. Now for $\mathbf{z} \in C^{*d}$, we have $\mathbf{z} \in C(dG, \mathcal{P})$. Thus, there exists a function $h \in \mathcal{L}(dG)$ such that $\mathbf{z} = \mathbf{c}_h$. If $\pi_B(\mathbf{z}) = 0$, i.e., $h \in \mathcal{L}(dG - \sum_{i \in B} P_i)$, then we must have $h = 0$ since $d \deg(G) < r = |B|$. Hence, $\psi(\mathbf{z}) = \mathbf{0}$.

This completes the proof. $\triangle$

Example 2.7 Consider the rational function field $F = \mathbb{F}_q(x)$, then $g(F) = 0$. Let $\mathcal{Q}$ and $\mathcal{P}$ be the set $\{0\}$ and $\mathbb{F}_q \setminus \{0\}$. In this case, $k = 1$ and $n = q - 1$.

(i) Choose $t = 1$, then for any $1 < d < r \leq q - 1$, there exists is a $(q - 1, 1, d, r; \mathbb{F}_q/\mathbb{F}_q)$-codex.

(ii) Choose $t = 2$, then for any $1 < 2d < r \leq q - 1$, there exists is a $(q - 1, 2, d, r; \mathbb{F}_q/\mathbb{F}_q)$-codex.

2.3 A property of codex

Let (C, ψ) be an $(n, t, d, r, \mathbb{F}_q^k/\mathbb{F}_q)$-codex. Let m be a positive integer. For each integer $e \geq 1$ and each polynomial $f(\mathbf{x}) \in \mathbb{F}_q[x_1, \dots, x_m]$ with $\deg(f(\mathbf{x})) \leq d$. Define the map $f^{(e)} : \mathbb{F}_q^{e \times m} \longrightarrow \mathbb{F}_q^e$; $(\mathbf{u}_1, \dots, \mathbf{u}_m) \mapsto (f(u_{1j}, \dots, u_{mj}))_{i=1}^{e}$, where u_{ij} denotes the j-th coordinate of $\mathbf{u}_i$ $(i = 1, \dots, m$, $j = 1, \dots, r)$. Note that $f(u_1, \dots, u_m) = f^{(1)}(u_1, \dots, u_m)$.

For codewords $\mathbf{c}_1, \dots, \mathbf{c}_m \in C \subseteq \mathbb{F}_q^n$, we have

$$f^{(n)}(\mathbf{c}_1, \dots, \mathbf{c}_m) = (f(\mathbf{c}_{(1)}), \dots, f(\mathbf{c}_{(m)}) = (\cdots, \sum_{\mathrm{wt}_L(I) \leq d} a_I \mathbf{c}_{(j)}^I, \cdots) = \sum_{\mathrm{wt}_L(I) \leq d} a_I (\cdots, \mathbf{c}_{(j)}^I, \cdots), \tag{2.1}$$

where $\mathbf{c}_{(j)}^I = \prod_{i=1}^m c_{ij}{}^{e_i}$ for $I = (e_1, e_2, \dots, e_m)$. This implies that $f^{(n)}(\mathbf{c}_1, \dots, \mathbf{c}_m) \in C^{*d}$. Furthermore, we have

$$\psi(f^{(n)}(\mathbf{c}_1, \dots, \mathbf{c}_m)) = \sum_{\mathrm{wt}_L(I) \leq d} a_I \psi(\cdots, \mathbf{c}_{(j)}^I, \cdots) = f^{(k)}(\psi(\mathbf{c}_1), \dots, \psi(\mathbf{c}_m)).$$

2.4 Bounds on error probability

In this subsection, we study sum of t-wise independent variables that will be used in local decoding of Reed-Muller codes. For our purpose, let us consider binary random variables that take values either 0 or 1.

Definition 2.8 Binary random variables $X_1, X_2, \dots, X_n$ are said *t-wise independent* if for any $a_1, a_2, \dots, a_t \in \{0, 1\}$ and any t indices $1 \leq i_1 < i_2 < \cdots < i_t \leq n$, one has $\Pr[X_{i_1} = a_1, \dots, X_{i_t} = a_t] = \prod_{i=1}^t \Pr[X_{i_i} = a_i]$.

We are going to bound the deviation from the mean of the sum $X = X_1 + \cdots + X_n$. Let us first consider the case $t = 2$ where Chebyshev's inequality is employed.

Lemma 2.9 *Let $X_1, \dots, X_n$ be pairwise independent binary random variables taking values in $\{0, 1\}$ and satisfy $\Pr(X_i = 1) = \delta$ for all $1 \leq i \leq n$. Then, for any $A > 0$, $\Pr[|X - \delta n| \geq A] \leq \frac{(\delta - \delta^2)n}{A^2}$.*

Proof. Define $X = \sum_{i=1}^n X_i$. By linearity of expectation, $\mathrm{E}[X] = \sum_{i=1}^n \mathrm{E}[X_i] = \delta n$. Since the X_i's are pairwise independent, linearity of variance holds here as well. This implies

$$\mathrm{Var}(X) = \sum_{i=1}^{M} \mathrm{Var}[X_i] = \sum_{i=1}^{n} (\mathrm{E}[X_i^2] - \mathrm{E}[X_i]^2) = (\delta - \delta^2)n.$$

Then by Chebyshev's Inequality, we have

$$\mathrm{Prob}[|X - \mathrm{E}[X]| \geq A] \leq \frac{\mathrm{Var}(X)}{A^2} = \frac{(\delta - \delta^2)n}{A^2}.$$

This completes the proof. △

For $t \geq 4$, we have the following *Second t-wise Independence Tail Inequality* .

Lemma 2.10 (see [2]) *Let $t \geq 4$ be an even integer. Suppose $X_1, \ldots, X_n$ are t-wise independent random variables over $\{0,1\}$. Let $X := \sum_{i=1}^n X_i$ and define $\mu := E[X]$ be the expectation of the sum. Then, for any $A > 0$, $Pr[|X - \mu| \geq A] \leq 8 \left(\frac{t\mu + t^2}{A^2}\right)^{t/2}$.*

2.5 Two classes of function fields

In this subsection, we introduce two classes of algebraic curves (or equivalently function fields) that will be used to construct our codex in Section 3, namely Hamitian curves and the Garcia-Stichtenoth tower. The reader may refer to [10] and [21, Sections 6.4 and 7.2] for the details.

For a function F of genus $g(F)$ over $\mathbb{F}_q$, the number $N(F)$ of rational places of F is upper bounded by the Hasse-Weil bound $q + 1 + 2g(F)\sqrt{q}$. F is called maximal if $N(F)$ achieves the Hasse-Weil bound, i.e., $N(F) = q + 1 + 2g(F)\sqrt{q}$. One of maximal function fields is called the Hermitian function field. It is defined over $\mathbb{F}_q$ with $q = r^2$ for some prime power r and its equation is given by

$$y^r + y = x^{r+1}.$$

The function field of this curve is $F = \mathbb{F}_q(x, y)$. There are totally $q^{3/2} + 1$ rational places for this function field. One of them is the point "at infinity", denoted by ∞. The other places are given by $(\alpha, \beta) \in \mathbb{F}_q$ satisfying $\beta^r + \beta = \beta^{r+1}$. These are called "finite" rational places. The genus of this function field is $g(F) = r(r-1)/2$.

The other class of function fields is also defined over $\mathbb{F}_q$ with $q = r^2$ for some prime power r. It is asymptotically optimal and recursively defined by the following equations

$$x_{i+1}^r + x_{i+1} = \frac{x_i^r}{1 + x_i^{r-1}}, \quad i = 1, 2 \ldots$$

with x_1 being a transcendental element over $\mathbb{F}_q$. The function field $\mathbb{F}_q(x_1, x_2, \ldots, x_e)$ is denoted by F_e. The genus $g_e := g(F_e)$ is at most r^e. There is one place over the pole of x_1 called "point at infinity". Furthermore, for each element $\alpha \in \mathbb{F}_q \setminus \{\alpha \in \mathbb{F}_q : \alpha^r + \alpha = 0\}$, there are exactly r^{e-1} places over it. Thus, the number $N(F_e)$ of rational places of F_e is at least $r^e(r-1)+1$. Thus, one has $\lim_{e\to\infty} N(F_e)/g(F_e) \geq r - 1 = \sqrt{q} - 1$. By the Vlăduţ-Drinfeld bound [22]. We must have $\lim_{e\to\infty} N(F_e)/g(F_e) = \sqrt{q} - 1$.

3 Local Decoding of Reed-Muller Codes

In this section, we analyze local decoding of Reed-Muller codes to recover multiple coordinates simutanously.

3.1 Decoding algorithm

Let $\mathrm{RM}(q, d, m)$ be the q-ary Reed-Muller code. We denote by $\mathbf{a}_f$ the codeword of $\mathrm{RM}(q, d, m)$ generated by the polynomial $f(\mathbf{x})$. Let $N = q^m$ and $\delta \in (0, 1)$. Suppose $\mathbf{a}_f$ is transmitted and there are at most δN error positions, i.e., there exists a vector $\mathbf{b} \in \mathbb{F}_q^N$ with $\mathrm{wt}_{\mathrm{H}}(\mathbf{b}) \le \delta N$ such that the received word is $\tilde{\mathbf{a}} := \mathbf{a}_f + \mathbf{b} \in \mathbb{F}_q^N$.

In other words, $\tilde{\mathbf{a}}$ is a corruption of the codeword $\mathbf{a}_f$ by an error vector $\mathbf{b}$ of relative Hamming weight at most δ. Assume that we are going to recover $\mathbf{a}_f$ at positions $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k \in \mathbb{F}_q^m$. Write $\tilde{\mathbf{a}} = (\tilde{a}_{\mathbf{u}})_{\mathbf{u} \in \mathbb{F}_q^m}$ and $\mathbf{w}_i = (w_{i,1}, w_{i,2}, \ldots, w_{i,m})$ for $i = 1, 2, \ldots, k$.

Local Decoding Algorithm

1. Choose an $(n, t, d, \sigma n, \mathbb{F}_q^k/\mathbb{F}_q)$-codex $\mathcal{C} = (C, \psi)$ with a real $0 < \sigma < 1$;
2. For $i = 1, \ldots, m$, select $\mathbf{c}_i \in C \subset \mathbb{F}_q^n$ uniformly at random (and independently of everything else) such that $\psi(\mathbf{c}_i) = (w_{1,i}, \ldots, w_{k,i})$;
3. Query $\tilde{\mathbf{a}} = (\tilde{a}_{\mathbf{u}})_{\mathbf{u} \in \mathbb{F}_q^m}$ at positions $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathbb{F}_q^m$, where $\mathbf{v}_j$ denotes collection of the j-th coordinate of the codewords $\mathbf{c}_1, \ldots, \mathbf{c}_m$;
4. Find a codeword $(z_1, z_2, \ldots, z_n) \in C^{*d}$ such that the Hamming distance between $(z_1, z_2, \ldots, z_n) \in C^{*d}$ and $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ is at most $(n - \sigma n)/2$.
5. If no such a codeword $(z_1, z_2, \ldots, z_n)$ in Step 4 is found, output "fail". Otherwise, output $(f(\mathbf{w}_1), f(\mathbf{w}_2), \ldots, f(\mathbf{w}_k)) = \psi(z_1, z_2, \ldots, z_n)$.

Now, we analyze the above algorithm.

First, $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are t-wise independent and uniformly random distributed in $\mathbb{F}_q^m$ by Lemma 2.4.

Suppose that a codeword $(z_1, z_2, \ldots, z_n) \in C^{(d)}$ is found such that the Hamming distance between $(z_1, z_2, \ldots, z_n) \in C^{*d}$ and $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ is at most $(n - \sigma n)/2$. Then by Lemma 2.5, we have $\psi(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)) = \psi(z_1, z_2, \ldots, z_n)$ as long as the Hamming distance between $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n))$ and $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ is at most $(n - \sigma n)/2$.
By Subsection 2.3, it holds that $f^{(n)}(\mathbf{c}_1, \ldots, \mathbf{c}_m) = (f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)) \in C^{*d}$ and
$f^{(k)}(\psi(\mathbf{c}_1), \ldots, \psi(\mathbf{c}_m)) = (f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k))$. Thus, we can recover $(f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k))$ as follows.

$$\begin{aligned}(f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k)) &= f(\psi(\mathbf{c}_1), \ldots, \psi(\mathbf{c}_m)) = \psi(f^{(n)}(\mathbf{c}_1, \ldots, \mathbf{c}_m)) \\ &= \psi(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)) = \psi(z_1, z_2, \ldots, z_n).\end{aligned}$$

Now the probability of successfully recovering $(f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k))$ is equal to the probability of successfully finding a codeword $(z_1, z_2, \ldots, z_n)$ such that the Hamming distance between $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ and $(z_1, z_2, \ldots, z_n)$ is at most $(n - \sigma n)/2$.. This probability is at least the probability that there are at most $(n - \sigma n)/2$ corrupted positions for $\mathbf{a}_f$ among $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.

Denote by E the set of coordinates $\mathbf{u}$ such that $\mathbf{b}_{\mathbf{u}} \neq 0$. For $j = 1, \ldots, n$, define the binary random variable X_j such that $X_j = 1$ if $\mathbf{v}_j \in E$ and $X_j = 0$ otherwise. Then $X_1, \ldots, X_n$ are t-wise independent and $\mathrm{Prob}(X_j = 1) = \delta$ for $j = 1, \ldots, n$. Put $X = \sum_{i=1}^n X_i$. By Lemma 2.5, if $|E \cap \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}| \le (n - \sigma n)/2$, one can correctly recover $\psi(z_1, z_2, \ldots, z_n)$ from $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$.

Thus, by the above identity it implies that one can correctly recover $(f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k))$ with probability at least $1 - \Pr(X \le (n - \sigma n)/2)$ by querying $\tilde{\mathbf{a}} = (\tilde{a}_{\mathbf{u}})_{\mathbf{u} \in \mathbb{F}_q^m}$, at coordinates $\mathbf{v}_1, \ldots, \mathbf{v}_n$.

Summarizing the above analysis, we get the following local decoding of Reed-Muller codes.

Theorem 3.1 *If there exists an $(n, t, d, \sigma n, \mathbb{F}_q^k/\mathbb{F}_q)$-codex with a real $0 < \sigma < 1$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = \Pr(X > (n - \sigma n)/2)$, where X is defined above.*

4 The main results

Next we are going to analyze the probability in Theorem 3.1 for various codex to obtain our main results.

4.1 Single point decoding

In this section, we consider local decoding to recover only a single coordinate via codex from Reed-Muller codes.

Example 4.1 For the rational function field $F = \mathbb{F}_q(x)$, we have $g(F) = 0$. Let $\mathcal{Q}$ and $\mathcal{P}$ be the set $\{0\}$ and $\mathbb{F}_q \setminus \{0\}$. In this case, $k = 1$ and $n = q - 1$.

(i) Choose $t = 1$, then for any real $0 < \sigma \leq 1$ and $1 < d \leq \sigma(q-1)+1$, there exists is a $(q-1, 1, d, \sigma(q-1); \mathbb{F}_q/\mathbb{F}_q)$-codex. By Markov's inequality the probability that $(1-\sigma)(q-1)/2$ or more of the queries go to corrupted locations is at most $2\delta/(1-\sigma)$. Thus, the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an $(q-1, \delta, 2\delta/(1-\sigma))$-locally decodable code. This is exactly the same decoding given in [23, Proposition 2.5].

(ii) Choose $t = 2$, then for any real $0 < \sigma \leq 1$ and $1 < d \leq \sigma(q-1)/2 - 1/2$, there exists is a $(q-1, 2, d, \sigma(q-1); \mathbb{F}_q/\mathbb{F}_q)$-codex. In Lemma 2.9, let A be $(1-\sigma)(q-1)/2 - \delta(q-1)$, we obtain

$$\epsilon = \Pr[X > (1-\sigma)(q-1)/2] \leq \frac{(\delta - \delta^2)(q-1)}{((1-\sigma)(q-1)/2 - \delta(q-1))^2} = \frac{\delta - \delta^2}{(1-\sigma-2\delta)^2} \times \frac{1}{q-1}. \quad (4.1)$$

Thus, the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an $(q-1, \delta, \epsilon)$-locally decodable code with ϵ given in (4.1). This is exactly the same decoding on curves given in [23, Proposition 2.6]. Note that we should replace σ in our formula by $2\sigma'$ to be consistent with those in [23, Proposition 2.6]

(iii) Let $t \geq 4$. For any real $0 < \sigma \leq 1$ and $1 < d \leq \sigma(q-1)/t - 1/t$, there exists is a $(q-1, t, d, \sigma(q-1); \mathbb{F}_q/\mathbb{F}_q)$-codex. It is clear that the expectation of X is $\mu = \delta n$. In Lemma 2.10, put $A = (1-\sigma)(q-1)/2 - \delta(q-1)$, by Lemma 2.10 we obtain

$$\epsilon = \Pr[X > (1-\sigma)(q-1)/2] \leq 8\left(\frac{4t\delta + 4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{q-1}\right)^t. \quad (4.2)$$

Thus, the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an $(q-1, \delta, \epsilon)$-locally decodable code with ϵ given in (4.2). It is easy to see from (4.2) that $\epsilon \leq 8\left(\frac{\lambda_{\sigma,\delta} t}{q}\right)^t$, where $\lambda_{\sigma,\delta} = \frac{\sqrt{8}}{1-\sigma-2\delta}$.

Remark 4.2 For sufficiently large q, by choice of a suitable t, local decoding in Example 4.1(iii) gives much better probability than those in Example 4.1(i) and (ii).

In the rest of this section we are going to apply codex from algebraic geometry codes to get local decoding of Reed-Muller codes. We first apply codex from the Hermitian function field.

Theorem 4.3 *Let q be a square prime power. For any real $0 < \sigma, \delta \leq 1$ and integers $t \geq 4$, $d > 1$ satisfying $\sigma < 1 - 2\delta$ and $d \leq \sigma q^{3/2}/(t + q - \sqrt{q}) - 1$, the Reed-Muller code $\mathrm{RM}(q, d, m)$ is a $\left(q^{3/2} - 1, \delta, \epsilon\right)$-locally detectable code with $\epsilon \leq 8\left(\frac{4t\delta + 4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{q^{3/2}-1}\right)^t$.*

Proof. Consider the Hermitian function field over $\mathbb{F}_q$ defined in Subsection 2.5. Let $\mathcal{Q} = \{(0,0)\}$ and let $\mathcal{P}$ be the set consisting of all "finite" points except for $(0,0)$. Then for any real $0 < \sigma \leq 1$ and integers $t \geq 4$, $d > 1$ satisfying $d \leq \sigma q^{3/2}/(t + q - \sqrt{q})$, there exists a $(q^{3/2} -$

$1, t, d, \sigma(q^{3/2}-1), \mathbb{F}_q/\mathbb{F}_q)$-codex. In Lemma 2.10, put $A = (1-\sigma)(q^{3/2}-1)/2 - \delta(q^{3/2}-1)$, we obtain

$$\epsilon = \Pr[X > (1-\sigma)(q^{3/2}-1)/2] \leq 8\left(\frac{4t\delta+4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{q^{3/2}-1}\right)^t. \qquad (4.3)$$

Thus, the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(q^{3/2}-1, \delta, \epsilon)$-locally decodable code with ϵ given in (4.3). The desired result follows. △

Finally, we apply codex from the Garcia-Stichtenoth tower.

Theorem 4.4 *Let q be a square prime power and let $e \geq 2$. Fix real $0 < \sigma, \delta \leq 1$ and a positive constant c. If integers $4 \leq t \leq cq^e$, $d > 1$ satisfy $\sigma < 1 - 2\delta$ and $d \leq \sigma\sqrt{q}/(2+c) - 1$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $\left(q^{e/2}(\sqrt{q}-1)-1, \delta, \epsilon\right)$-locally detectable code with $\epsilon \leq 8\left(\frac{4t\delta+4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{q^{e/2}(\sqrt{q}-1)-1}\right)^t$.*

Proof. Consider the Garcia-Stichtenoth tower over $\mathbb{F}_q$ defined in Subsection 2.5. Let $\mathcal{Q}$ be a single "finite" rational place set and let $\mathcal{P}$ be the a consisting of other $n := q^{e/2}(\sqrt{q}-1)-1$ "finite" rational place. Then $d(2g(F)+1+t-1) < \sigma n < n$ and hence by Proposition 2.6, there exists an $(n, t, d, \sigma n, \mathbb{F}_q/\mathbb{F}_q)$-codex. In Lemma 2.10, put $A = (1-\sigma)n/2 - \delta n$. Hence, we obtain

$$\epsilon = \Pr[X > (1-\sigma)n/2] \leq 8\left(\frac{4t\delta+4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{n}\right)^t. \qquad (4.4)$$

Thus, the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an (n, δ, ϵ)-locally decodable code with ϵ given in (4.4). The desired result follows. △

4.2 Multiple-point local decoding of Reed-Muller codes

In this subsection, we analyze local decoding of Reed-Muller codes to recover multiple coordinates simultaneously. Again we apply Reed-Solomon codes, Hermtian codes and algebraic geometry codes based on the Garcia-Stichtenoth tower, respectively. The proofs are almost identical with those in the previous subsection except for replacing $\mathcal{Q}$ of a single point set by a k-point set. We state the results without proof below.

Theorem 4.5 *Let q be a prime power. Let $d > 1, t, m, k$ be positive integers. Let δ, σ be two reals in $(0,1)$ with $\delta < \frac{1-\sigma}{2}$.*

(i) **(Reed-Solomon code with $t = 1$)** *If $k + n \leq q$ and $d < \frac{\sigma n}{k}$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = \frac{2\delta}{1-\sigma}$.*

(ii) **(Reed-Solomon code with $t = 2$)** *If $k + n \leq q$ and $d < \frac{\sigma n}{k+2}$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = \frac{\delta-\delta^2}{(1-\sigma-2\delta)^2} \times \frac{1}{n}$.*

(iii) **(Reed-Solomon code with $t \geq 4$)** *If $k + n \leq q$ and $d < \frac{\sigma n}{k+t}$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = 8\left(\frac{4t\delta+4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{n}\right)^t$.*

(iv) **(Hermitian code with $t \geq 4$)** *Let q be a square. If $k+n \leq q^{3/2}$ and $d < \frac{\sigma n}{k+t+q-\sqrt{q}}$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = 8\left(\frac{4t\delta+4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{n}\right)^t$.*

(v) **(GS tower code with $t \geq 4$)** *Let q be a square and let $e \geq 2$. For two positive constants c and b, if $t \leq cn$ and $k \leq bn$, $k + n \leq q^{e/2}(\sqrt{q}-1)$ and $d < \frac{\sigma\sqrt{q}}{b+c+2}$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = 8\left(\frac{4t\delta+4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{n}\right)^t$.*

References

[1] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron, Testing Reed-Muller codes, IEEE Transactions on Information Theory, Vol. 51, no. 11, (2005), pp. 4032-4039.

[2] M. Bellare and J. Rompel, Randomness-efficient oblivious sampling, Proceedings of FOCS'94 (1994), pp. 276-287.

[3] E. Ben-Sasson, A. Gabizon, Y. Kaplan, S. Kopparty and S. Saraf, A new family of locally correctable codes based on degree-lifted algebraic geometry codes, Proceeding STOC'13, (2013), pp. 833-842.

[4] A. Bhowmick, S. Lovett, The List Decoding Radius of Reed-Muller Codes over Small Fields, Proceedings of STOC'15 (2015), pp. 277-285

[5] H. Chen, R. Cramer, *Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields,* CRYPTO'06(2006), 521-536.

[6] R. Cramer, The Arithmetic Codex: Theory and Applications, Advances in Cryptology, EUROCRYPT'11, LNCS 6632 (2011), pp. 1-1.

[7] I. Cascudo, R. Cramer and C. Xing, The arithmetic codex, Proceedings of Information Theory Workshop, (2012), pp. 75-79.

[8] R. Cramer, I. Damgård, U. M. Maurer, *General Secure Multi-party Computation from any Linear Secret-Sharing Scheme,* Proceedings of EUROCRYPT'00 (2000), 316-334

[9] R. Cramer, I. Damgård and I. Nielsen, *Secure Multiparty Computation and Secret Sharing,* Cambridge University Press, 2015.

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

[11] P. Gopalan, A Fourier-Analytic Approach to Reed-Muller Decoding, Proceedings of FOCS'10 (2010), pp. 685-694.

[12] P. Gopalan , A. R. Klivans and D. Zuckerman, List-decoding reed-muller codes over small fields, Proceedings of STOC'08 (2008), pp. 265-274.

[13] A. Guo, High rate locally correctable codes via lifting, arXiv:1304.1202, 2014.

[14] A. Guo, S. Kopparty and M. Sudan, New affine-invariant codes from lifting, Proceedings of ITCS'13, (2013), pp. 529-540.

[15] V. Guruswami, L. Jin and C. Xing, Efficient list decoding of punctured Reed-Muller codes, CoRR abs/1508.00603 (2015)

[16] S. Hoory, N. Linial and A. Wigderson, Expander graphs and their applications, Bulletin of AMS, 43(4) (2006), pp. 439-561.

[17] S. Kopparty, S. Saraf and S, Yekhanin, High-rate codes with sublinear-time decoding, J. ACM, 61(5):28 (2014).

[18] O. Meir. Locally correctable and testable codes approaching the singleton bound. Electronic Colloquium on Computational Complexity (ECCC), 21:107, 2014.

[19] R. Pellikaan and X. Wu, List decoding of q-ary Reed-Muller codes, IEEE Transactions on Information Theory, Vol.50 (2004), pp.679-682.

[20] R. Saptharishi, A. Shpilka and B. L. Volk, Efficiently decoding Reed-Muller codes from random errors, http://arxiv.org/abs/1503.09092.

[21] H. Stictenoth, *Algebraic Function Fields and Codes,* GTM254, Spring, Berlin, 2009.

[22] M .A. Tsfasman and S. G. Vladut, *Algebraic-geometric codes,* Kluwer, Dordrecht, 1991.

[23] S. Yekhanin, *Locally Decodable Codes,* Foundations and Trends in Theoretical Computer Science: Vol. 6: No. 3 (2012), pp. 139-255