Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 169 (2020)

Efficient List-Decoding with Constant Alphabet and List Sizes

Zeyu Guo   Noga Ron-Zewi*
Department of Computer Science, University of Haifa
zguotcs@gmail.com   noga@cs.haifa.ac.il

Abstract

We present an explicit and efficient algebraic construction of capacity-achieving list decodable codes with *both* constant alphabet and constant list sizes. More specifically, for any $R \in (0,1)$ and $\epsilon > 0$, we give an algebraic construction of an infinite family of error-correcting codes of rate R, over an alphabet of size $(1/\epsilon)^{O(1/\epsilon^2)}$, that can be list decoded from a $(1-R-\epsilon)$-fraction of errors with list size at most $\exp(\mathrm{poly}(1/\epsilon))$. Moreover, the codes can be encoded in time $\mathrm{poly}(1/\epsilon, n)$, the output list is contained in a linear subspace of dimension at most $\mathrm{poly}(1/\epsilon)$, and a basis for this subspace can be found in time $\mathrm{poly}(1/\epsilon, n)$. Thus, both encoding and list decoding can be performed in *fully polynomial-time* $\mathrm{poly}(1/\epsilon, n)$, except for pruning the subspace and outputting the final list which takes time $\exp(\mathrm{poly}(1/\epsilon)) \cdot \mathrm{poly}(n)$. In contrast, prior explicit and efficient constructions of capacity-achieving list decodable codes either required a much higher complexity in terms of $1/\epsilon$ (and were additionally much less structured), or had super-constant alphabet or list sizes.

Our codes are quite natural and structured. Specifically, we use algebraic-geometric (AG) codes with evaluation points restricted to a subfield, and with the message space restricted to a (carefully chosen) linear subspace. Our main observation is that the output list of AG codes with subfield evaluation points is contained in an affine shift of the image of a *block-triangular-Toeplitz* (BTT) *matrix*, and that the list size can potentially be reduced to a constant by restricting the message space to a BTT *evasive subspace*, which is a large subspace that intersects the image of any BTT matrix in a constant number of points. We further show how to explicitly construct such BTT evasive subspaces, based on the explicit subspace designs of Guruswami and Kopparty (*Combinatorica*, 2016), and composition.

1 Introduction

An *error-correcting code* is a map $C : \Sigma^k \to \Sigma^n$, which encodes a k-symbol *message* over an *alphabet* Σ into an n-symbol *codeword* over Σ. One main parameter of interest of an error-correcting code is the *rate* $R = k/n$, which measures the amount of redundancy in the encoding. Naturally, it is desirable that the rate R is as large as possible to minimize the overhead in encoding. Another important parameter is the *(relative) distance* δ, defined as the smallest *(relative) Hamming distance*[1] $\mathrm{dist}(C(x), C(y))$ between the encodings of any pair of distinct messages $x, y \in \Sigma^k$. The importance of the distance parameter arises from the following observation: if we are given $w \in \Sigma^n$ such that $\mathrm{dist}(w, C(x)) < \frac{\delta}{2}$ for some message $x \in \Sigma^k$, then this x is *uniquely determined*. Thus, a large distance allows one to *unambiguously* retrieve the original

*Research supported in part by ISF grant 735/20.

[1]The *(relative) Hamming distance* $\mathrm{dist}(z, w)$ between a pair of strings $z, w \in \Sigma^n$ is the fraction of coordinates on which z and w differ.

ISSN 1433-8092

message in the presence of some error or corruption. Other desirable properties of an error-correcting code are that its alphabet size would be small (ideally, a *constant*, independent of the codeword length), and that it admits efficient ($\mathrm{poly}(n)$-time) encoding and decoding algorithms.

Clearly, there is a qualitative trade-off between the above parameters: the largest the distance δ is, the smallest the rate R must be. Quantitatively, the *Singleton bound* states that any code must satisfy that $\delta \leq 1 - R$. This bound is precisely matched by the classical family of *Reed-Solomon* (RS) *codes* [RS60]. Given a finite field $\mathbb{F}_q$, and n distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the *Reed-Solomon code* $\mathsf{RS}_q(n,k)$ *with evaluation points* $\alpha_1, \ldots, \alpha_n$ maps a message $(f_0, f_1, \ldots f_{k-1}) \in \mathbb{F}_q^k$, viewed as the coefficients of a polynomial $f = \sum_{i=0}^{k-1} f_i X^i \in \mathbb{F}_q[X]_{<k}$, to the evaluation table $(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_q^n$.

A disadvantage of RS codes is that by definition, their alphabet size q must be at least the codeword length n. To match the Singelton bound over a *constant-size* alphabet, independent of the codeword length n, one can resort to *algebraic-geometric* (AG) *codes* that achieve a distance of $\delta = 1 - R - \epsilon$ over a constant-size alphabet (depending on ϵ) [Sti09]. Moreover, both RS and AG codes can be efficiently encoded and decoded up to half their minimum distance [Pet60, BW87, JLJ$^+$89].

List decoding. In *list decoding,* the fraction of errors α is large enough so that unique recovery of the message x is impossible (that is, $\alpha > \frac{\delta}{2}$). Instead, the goal is, given a received word w, to return a short list $\mathcal{L}$ with the guarantee that $x \in \mathcal{L}$ for any message x with $\mathrm{dist}(w, C(x)) \leq \alpha$. Besides being a fundamental concept in coding theory, list decoding has found diverse applications in theoretical computer science, for example in cryptography [GL89], learning theory [KM93], average-to-worst-case reductions [CPS99, GRS00], hardness amplification [BFNW93, STV01, Tre03], and pseudo-randomness [TZ04, GUV09, DKSS13, TU12, GRX18].

The *list-decoding capacity theorem* states that the maximal fraction of errors for which list decoding with non-trivial list sizes is possible is $\alpha \leq 1 - R$. Moreover, it is not hard to show that a random code of rate R and alphabet-size $\exp(1/\epsilon)$ is with high probability list decodable from a $(1 - R - \epsilon)$-fraction of errors with list size as small as $O(1/\epsilon)$. So in principle, by allowing a small (constant-size) list, one can correct twice as many errors than in the unique decoding setting! However, matching these bounds with an explicit and efficient construction (ideally, encodable and list decodable in *fully polynomial-time*[2] $\mathrm{poly}(1/\epsilon, n)$) turned out to be more challenging than in the unique decoding setting.

Capacity-achieving list decodable codes. The celebrated work of Guruswami and Sudan [Sud97, GS99] showed that RS codes can be efficiently list decoded beyond half their minimum distance (up to the so-called *Johnson bound*), which gave the first family of error-correcting codes that are efficiently list decodable beyond the unique decoding radius. Only a decade later, the seminal work of Guruswami and Rudra [GR08] showed that *folded Reed-Solomon* (FRS) *codes* – a remarkably simple variant of RS codes – can be efficiently list decoded up to list-decoding capacity. FRS codes are obtained from RS codes (with the evaluation points ordered according to their power in the multiplicative group of the field) by dividing the codewords coordinates in the latter code into consecutive blocks of length $m = \Theta(1/\epsilon^2)$, and then viewing each such block of coordinates as a single symbol over a larger alphabet.

Once more, a disadvantage of FRS codes is their large alphabet – on the order of $n^{\Theta(1/\epsilon^2)}$ – which is even larger than that of the corresponding RS codes. Moreover, the list size obtained by the algorithm of Guruswami and Rudra was also a very large polynomial on the order of $n^{\Theta(1/\epsilon)}$, and this also dictated a similar running time for the list decoding algorithm. Starting with the breakthrough result of Guruswami

[2]Note that in the list decoding setting, at least $\Omega(n/\epsilon)$ time is required to output the list. Moreover, the alphabet size must be at least $\exp(\Omega(1/\epsilon))$, and so the bit-length of the input is at least $\Omega(n/\epsilon)$.

and Rudra [GR08], there has been a long line of work attempting to construct explicit and efficient capacity-achieving list decodable codes with smaller alphabet and list sizes. Next, we briefly describe the main results of this line of work, and we refer the reader to Table 1 below for a summary of parameters.

Reducing list size. Towards reducing the list size, Guruswami and Wang [GW13] devised a new "linear-algebraic" list decoding algorithm for FRS codes, with the surprising property that the output list is contained in a low-dimensional subspace of *constant* dimension $O(1/\epsilon)$. In the same work, Guruswami and Wang further observed that, utilizing this property, one can potentially reduce the list size to a constant by restricting the message space of FRS codes to a *subspace evasive set*, which is a large set that intersects any constant dimensional subspace in a constant number of points. Guruswami and Wang showed that such objects exist probabilistically, and raised the question of searching for an explicit construction.

The above program was subsequently carried out by Dvir and Lovet [DL12], who gave an algebraic construction of subspace evasive sets with the required properties. Combined with the linear-algebraic list decoding algorithm of [GW13], this resulted in a subcode of FRS codes that can be efficiently encoded (in time $\mathrm{poly}(1/\epsilon, n)$), and efficiently list decoded up to capacity with constant list size $L = (1/\epsilon)^{O(1/\epsilon)}$ (in time $\mathrm{poly}(L, n)$). Lastly, Kopparty, Ron-Zewi, Saraf, and Wootters [KRSW18] have recently shown that in fact *any* linear[3] code of constant distance δ that is list decodable from a $(\delta - \epsilon)$-fraction of errors with output list of constant dimension d has constant list sizes (depending on d, δ, and ϵ). This shows that, perhaps surprisingly, FRS codes themselves have constant list size (in fact the same list size of $L = (1/\epsilon)^{O(1/\epsilon)}$), without the need to pass to a subcode (list decoding can be performed *probabilistically* in time $\mathrm{poly}(L, n)$).

Reducing alphabet size. Similarly to the unique decoding setting, one can reduce the alphabet size to a constant (depending on ϵ) by considering suitable versions of "folded" AG codes [Gur09, GX12, GX14, GX15]. However, in this setting, the dimension of the output list was too large to apply the above subspace evasive machinery and obtain small list sizes. To overcome this, Guruswami and Xing [GX13] came-up with an alternative approach for constructing capacity-achieving list decodable codes that is based on restricting the evaluation points of "plain" (unfolded) versions of RS or AG codes to a subfield.[4]

Specifically, Guruswami and Xing first observed that while RS codes are generally *not* list decodable up to capacity with non-trivial list sizes [BKR10], for the special case of RS codes with evaluation points restricted to a subfield, it is possible to obtain slightly non-trivial list sizes, and furthermore, the lists satisfy a certain *periodic* structure. In more detail, consider the RS code $\mathsf{RS}_{q,m}(n, k)$, defined over a large extension field $\mathbb{F}_{q^m}$, with evaluation points coming from a small subfield $\mathbb{F}_q$, for $m = \Theta(1/\epsilon^2)$. Guruswami and Xing showed that in this setting, there exists an $\mathbb{F}_q$-linear subspace $\hat{V} \subseteq \mathbb{F}_{q^m}$ of constant dimension $O(1/\epsilon)$ so that any message $(f_0, f_1, \dots f_{k-1}) \in \mathbb{F}_{q^m}^k$ in the output list satisfies that once the first i coefficients $f_0, f_1, \dots, f_{i-1} \in \mathbb{F}_{q^m}$ are fixed, the next coefficient f_i belongs to an affine shift of $\hat{V}$.

Note that, indeed, the above structure does not a priori guarantee a small list size. In fact, the only bound on the list size that is implied by the above structure is $q^{O(k/\epsilon)} = q^{O(\epsilon mk)}$, which is only slightly smaller than the number of possible messages which is q^{km}. However, Guruswami and Xing noticed that, interestingly, the above periodic structure can lead to a list of constant dimension (which also leads in turn to constant list sizes using the machinery of [DL12] or [KRSW18] described above) when the message space is restricted to a *subspace design*, and once more, suggested to construct such objects explicitly. In a follow-up work [GK16], Guruswami and Kopparty explicitly constructed such objects, and combined with the approach of

[3]A code $C : \Sigma^k \to \Sigma^n$ is *linear* if $\Sigma = \mathbb{F}_q$ for some finite field $\mathbb{F}_q$, and the map $C : \mathbb{F}_q^k \to \mathbb{F}_q^n$ is linear.

[4]Guruswami and Xing first came-up with a similar approach in the folded setting [GX12], and only later observed in [GX13] that it also applies to unfolded versions. For simplicity, we only discuss the latter more basic approach.

Guruswami and Xing, this had the surprising consequence that a subcode of "plain" RS codes (with subfield evaluation points) is list decodable up to capacity, with constant list sizes (see Table 1 for exact parameters).

Guruswami and Xing further observed that a similar periodic structure occurs in the AG code setting. However, over constant-size fields, it is impossible to construct subspace designs that lead to constant list sizes.[5] Nevertheless, Guruswami and Xing showed that one can iteratively compose together subspace designs of exponentially increasing lengths to obtain extremely slowly growing list sizes (depending on $\log^* n$) over constant-size alphabets (see more discussion in Section 2 below). This led in turn to capacity-achieving list decodable codes with constant alphabet size $(1/\epsilon)^{O(1/\epsilon^2)}$, extremely slowly growing list size $\exp(\mathrm{poly}(1/\epsilon)) \cdot \exp\exp\exp(\log^* n)$, and efficient encoding and list decoding algorithms (running in time $\mathrm{poly}(1/\epsilon, n)$ and $\mathrm{poly}(L, n)$, respectively).

Finally, we mention that in [KRSW18], a different approach was given for obtaining *both* constant list and constant alphabet sizes, based on multi-level concatenation of FRS codes, and expander-based amplification. However, the resulting code is arguably more complicated and less natural and structured than the aforementioned algebraic constructions, and moreover, has a much higher complexity in terms of $1/\epsilon$. Specifically, the list size was *quadruply-exponential* in $\mathrm{poly}(1/\epsilon)$, which also dictated a similar running time for list decoding,[6], and the encoding time was also pretty large $\exp(\mathrm{poly}(1/\epsilon)) \cdot \mathrm{poly}(n)$ due to the need to brute-force search for the inner codes.

1.1 Our results

A main question left open by the above line of work is whether one can come up with constructions of capacity-achieving list decodable codes with *both* constant alphabet and constant list sizes, and admitting *fully polynomial-time* $\mathrm{poly}(1/\epsilon, n)$ encoding and list-decoding. Our main result (almost) answers this question in the affirmative.

Theorem 1.1. *For any $R \in (0,1)$ and $\epsilon > 0$, there is an infinite family of error-correcting codes of rate at least R over an alphabet of size $(1/\epsilon)^{O(1/\epsilon^2)}$ that can be encoded in time $\mathrm{poly}(1/\epsilon, n)$, and can be list decoded from a $(1-R-\epsilon)$-fraction of errors with list size at most $L = \exp(\mathrm{poly}(1/\epsilon))$ in time $\mathrm{poly}(L, n)$. Moreover, the codes, defined over an alphabet $\mathbb{F}_{q^m}$, are $\mathbb{F}_q$-linear, the output list is contained in an $\mathbb{F}_q$-linear subspace of dimension at most $\mathrm{poly}(1/\epsilon)$, and a basis for this subspace can be found in time $\mathrm{poly}(1/\epsilon, n)$.*

Note that our codes achieve list-decoding capacity with *both* constant alphabet and constant list sizes, and both encoding and list decoding can be performed in *fully polynomial-time* $\mathrm{poly}(1/\epsilon, n)$, except for pruning the subspace and outputting the final list which takes time $\exp(\mathrm{poly}(1/\epsilon)) \cdot \mathrm{poly}(n)$. Our codes are quite natural and structured, specifically, we use AG codes with evaluation points restricted to a subfield, and with the message space restricted to a (carefully chosen) $\mathbb{F}_q$-linear subspace. It is our hope that this relatively natural and simple structure will prove useful in future applications.

A barrier to improving the general running time of list-decoding to $\mathrm{poly}(1/\epsilon, n)$ is the exponential dependency of the list size on $1/\epsilon$ since, at the very least, such amount of time is required to output the whole list. However, currently the smallest known list size for explicit capacity-achieving list decodable codes is

[5] In [GX12], Guruswami and Xing suggested alternatively using *hierarchical subspace evasive sets* and showed that utilizing the above periodic structure, these could potentially lead to constant list sizes over constant-size alphabets. However, it is currently unknown how to explicitly construct such objects.

[6] The reason for the large list size is that the construction roughly uses four levels of encodings, two of these via FRS codes, and two other via random linear codes, and for both codes, the best-known list size is exponential in $1/\epsilon$. It may be possible to reduce the list size by replacing the random linear codes with other codes of smaller list size and succinct representation, e.g., the *pseudo-linear codes* of [GI01]. However, the list size would still be at least doubly-exponential in $1/\epsilon$.

$(1/\epsilon)^{O(1/\epsilon)}$, achieved by FRS codes [KRSW18]. We leave it as an interesting open problem to search for explicit capacity-achieving list decodable codes (even over large super-constant alphabet) with optimal list size $O(1/\epsilon)$, or even $\mathrm{poly}(1/\epsilon)$. We further mention that the alphabet size we obtain, on the other hand, is not much worse than the lower bound of $\exp(\Omega(1/\epsilon))$, and is generally the smallest known alphabet size for explicit capacity-achieving list decodable codes [GX12, GX13, GX14, GX15].

Finally, we note that using the machinery of [HRW20, KRR$^+$21] (specifically, taking a high-order tensor product of the codes given by Theorem 1.1, combined with an expander-based amplification), it is possible to bring down the dependency on n in the running time of both encoding and list-decoding to *nearly-linear*, say $n^{1.01}$. However, similarly to the multi-level construction of [KRSW18] mentioned above, the resulting codes become more complicated and less natural and structured, and also have a much higher complexity in terms of $1/\epsilon$. Obtaining a *truly-linear* dependency on n in the running time of either encoding or list-decoding for capacity-achieving list decodable codes seems to require, as in the unique decoding setting, completely different non-algebraic techniques.

Table 1 below summarizes the above discussion. In the next section, we shall give an overview of our techniques.

2 Techniques

The starting point for our construction is the aforementioned work of Guruswami of Xing [GX13]. As described above, in this work it was observed that the output list of RS or AG codes with subfield evaluation points satisfy a special *periodic* structure. Namely, there exists an $\mathbb{F}_q$-linear subspace $\hat{V} \subseteq \mathbb{F}_{q^m}$ of constant dimension $r = O(1/\epsilon)$ so that any message $(f_0, f_1, \ldots f_{k-1}) \in \mathbb{F}_{q^m}^k$ in the output list satisfies that given the first i coefficients $f_0, f_1, \ldots, f_{i-1} \in \mathbb{F}_{q^m}$, the next coefficient f_i belongs to an affine shift of $\hat{V}$. Moreover, it was shown that one can exploit this structure and reduce the output list size by restricting the message space to a *subspace design*.

An (r, s)*-subspace design over* $\mathbb{F}_{q^m}$ *of cardinality* k is a collection of k $\mathbb{F}_q$-linear subspaces $H_1, \ldots, H_k \subseteq \mathbb{F}_{q^m}$ so that $\sum_{i=1}^k \dim(\hat{V} \cap H_i) \leq s$ for any $\mathbb{F}_q$-linear subspace $\hat{V} \subseteq \mathbb{F}_{q^m}$ of dimension at most r. It follows by definition that, assuming the above periodic structure, when restricting each coefficient f_i to the subspace H_i, the resulting output list has dimension at most $\sum_{i=1}^k \dim(\hat{V} \cap H_i) \leq s$. It can be shown, using the probabilistic method, that there exists an (r, s)-subspace design $H_1, \ldots, H_k$ over $\mathbb{F}_{q^m}$ with $k = q^{\Omega(\epsilon m)}$ and $s = O(r/\epsilon)$, where each subspace H_i has co-dimension at most ϵm in $\mathbb{F}_{q^m}$. In [GK16], Guruswami and Kopparty gave an explicit construction of a subspace design with similar parameters.

Theorem 2.1 (Explicit subspace design, [GK16], Theorem 6)**.** *There exists an absolute constant $c > 1$, so that for every $\epsilon > 0$, positive integers k, m, r with $r < \frac{\epsilon m}{4}$, and a prime power q satisfying $q^m \geq \max\left\{k^{c \cdot r/\epsilon}, \left(\frac{2r}{\epsilon}\right)^{2r/\epsilon}\right\}$, there exists an (r, s)-subspace design $H_1, \ldots, H_k$ over $\mathbb{F}_{q^m}$ for $s = \frac{2r^2}{\epsilon}$, where each H_i has co-dimension at most ϵm in $\mathbb{F}_{q^m}$. Moreover, bases for $H_1, \ldots, H_k$ can be found in time* $\mathrm{poly}(q, k, m)$.

Thus, by restricting the message coefficients in RS codes with subfield evaluation points to the subspace design given by the above theorem, one can reduce the dimension of the output list to $O(1/\epsilon^3)$ (and by [KRSW18], this in fact implies that the list is of constant size). Note however that the above theorem could not be applied to AG codes, as it requires the number of subspaces k to be smaller than q^m, whereas for AG codes the number of message coordinates k (which grows to infinity) is much larger than q^m (which is constant in the AG setting).

Code	Alphabet size $\|\Sigma\|$	List size L	Notes
Random codes	$2^{O(1/\epsilon)}$	$O(1/\epsilon)$	Non-constructive
FRS codes [GR08, GW13]	$n^{O(1/\epsilon^2)}$	$n^{O(1/\epsilon)}$	
Previous codes [KRSW18]	$n^{O(1/\epsilon^2)}$	$\left(\frac{1}{\epsilon}\right)^{O(1/\epsilon)}$	Randomized list-decoding
Previous codes + subspace evasive set [DL12]	$n^{O(1/\epsilon^2)}$	$\left(\frac{1}{\epsilon}\right)^{O(1/\epsilon)}$	
Multi-level concatenation of previous codes + expander amplification [KRSW18]	$2^{\mathrm{poly}(1/\epsilon)}$	$2^{2^{2^{\mathrm{poly}(1/\epsilon)}}}$	Encoding time $2^{\mathrm{poly}(1/\epsilon)} \cdot \mathrm{poly}(n)$
RS codes with subsfield evaluation points + subspace design [GX13, GK16]	$n^{O(1/\epsilon^2)}$	$n^{O(1/\epsilon^3)}$	
Previous codes [KRSW18]	$n^{O(1/\epsilon^2)}$	$\left(\frac{1}{\epsilon}\right)^{O(1/\epsilon^4)}$	Randomized list-decoding
Previous codes + subspace evasive set [DL12]	$n^{O(1/\epsilon^2)}$	$\left(\frac{1}{\epsilon}\right)^{O(1/\epsilon^3)}$	
AG codes with subfield evaluation points + subspace design [GX13, GK16]	$\left(\frac{1}{\epsilon}\right)^{O(1/\epsilon^2)}$	$2^{\mathrm{poly}(1/\epsilon)} \cdot 2^{2^{2^{O(\log^* n)}}}$	
Tensor product of previous codes + expander amplification [HRW20, KRR+21]	$2^{\mathrm{poly}(1/\epsilon)}$	$2^{2^{2^{\mathrm{poly}(1/\epsilon)}}} \cdot 2^{2^{2^{2^{O(\log^* n)}}}}$	Encoding time $2^{\mathrm{poly}(1/\epsilon)} \cdot n^{1.01}$, list-decoding time $\mathrm{poly}(L) \cdot n^{1.01}$
This work: AG codes with subfield evaluation points + BTT evasive subspace	$\left(\frac{1}{\epsilon}\right)^{O(1/\epsilon^2)}$	$2^{\mathrm{poly}(1/\epsilon)}$	Basis for subspace containing list can be found in time $\mathrm{poly}(1/\epsilon, n)$

Table 1: Capacity-achieving list decodable codes $C : \Sigma^k \to \Sigma^n$ of rate R that are list decodable from a $(1-R-\epsilon)$-fraction of errors with list size L. All codes can be deterministically encoded in time $\mathrm{poly}(1/\epsilon, n)$ and deterministically list decoded in time $\mathrm{poly}(L, n)$ unless otherwise noted.

To overcome this, Guruswami and Xing suggested the following iterative construction. Suppose that the message space has the periodic structure described above, and that $k \gg q^m$. Then Guruswami and Xing suggested to first divide the k coordinates into $\frac{k}{k_1}$ blocks of k_1 coordinates each, where $k_1 \approx q^m$, and restrict each such block separately to an identical (r, s)-subspace design over $\mathbb{F}_{q^m}$ of cardinality k_1 that is guaranteed by the above Theorem 2.1. The main observation is that, when viewing each block of length k_1 as a single coordinate, the resulting subspace also has a periodic structure, however, with exponentially larger alphabet size q^{mk_1}.

Thus, one can once more divide the resulting $\frac{k}{k_1}$ coordinates into $\frac{k}{k_1 k_2}$ blocks of length k_2 each, where now $k_2 \approx q^{mk_1}$, and restrict to an identical subspace design on each block separately. Continuing this way, and noting that the alphabet size increases exponentially in each iteration, after $\approx \log^* k$ iterations, we arrive at alphabet size k, which is sufficiently large for restricting to a single subspace design. Since the dimension squares on each invocation of Theorem 2.1, the final dimension is doubly-exponential in $\log^* k$, and the resulting output list size is triply-exponential $\log^* k$.

Our main observation that allows us to obtain *both* constant alphabet and constant list sizes is that AG (or RS) codes with subfield evaluation points satisfy yet an even more refined structure, namely, the output list is contained in an affine shift of the image of a *block-triangular-Toeplitz* (BTT) *matrix*. We further observe that this structure can potentially lead to constant list sizes over a constant-size alphabet if the message space is restricted to an appropriate pseudo-random object that we call a BTT *evasive subspace*. In what follows we elaborate on these two ingredients.

2.1 Block-triangular-Toeplitz matrix

We start by formally defining the notion of a block-triangular-Toeplitz matrix (see Figure 1 below for an illustration).

Definition 2.2 (Block-triangular-Toeplitz (BTT) matrix)**.** *A (k, m, r)-block-triangular-Toeplitz (BTT) matrix over $\mathbb{F}_q$ is a $(km) \times (kr)$ matrix M over $\mathbb{F}_q$ so that $M = (M_{i,j})_{i,j \in [k]}$, as a $(k \times k)$-block matrix with $m \times r$ blocks $M_{i,j}$, satisfies the following conditions:*

1. *M is block-lower-triangular, i.e., $M_{i,j} = 0$ for $i, j \in [k]$ with $i < j$.*
2. *M is block-Toeplitz, i.e., $M_{i,j} = M_{i',j'}$ for $i, j, i', j' \in [k]$ with $i - j = i' - j'$.*
3. *M has maximal rank. By the two conditions above, this is equivalent to the statement that $M_{1,1}$ has rank $\min\{r, m\}$.*

*We say that M is (k, m, r)-*periodic *if only blocks on the main diagonal are required to be identical, i.e., the second condition above is weakened to $M_{i,i} = M_{i',i'}$ for all $i, i' \in [k]$.*

We say that $V \subseteq \mathbb{F}_q^{km}$ is a (k, m, r)-BTT *subspace* if $V = \mathrm{Image}(M)$ for some (k, m, r)-BTT matrix M (where M is viewed as a linear map from $\mathbb{F}_q^{kr}$ to $\mathbb{F}_q^{km}$, and $\mathrm{Image}(M)$ denotes its image). Similarly, we say that $V \subseteq \mathbb{F}_q^{km}$ is a (k, m, r)-*periodic subspace* if $V = \mathrm{Image}(M)$ for some (k, m, r)-periodic matrix M. Note that in this terminology, the periodic structure described above corresponds to the special case of a (k, m, r)-periodic subspace, where $\hat{V} = \mathrm{Image}(M_1)$. Our first main observation is that the output list of AG (or RS) codes with subfield evaluation points is in fact contained in an affine shift of a (k, m, r)-BTT subspace for $r = O(1/\epsilon)$ (under a suitable linear map).

$$\begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 \\ M_2 & M_1 & 0 & \cdots & 0 \\ M_3 & M_2 & M_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_k & M_{k-1} & M_{k-2} & \cdots & M_1 \end{pmatrix}$$

Figure 1: A (k, m, r)-BTT matrix, where each M_i is an $m \times r$ matrix and M_1 has maximal rank.

Theorem 2.3 (Output list contained in a BTT subspace)**.** *There exists an absolute constant $c > 1$ so that the following holds for any $R \in (0, 1)$, $\epsilon > 0$, $q \geq 1/\epsilon^c$ that is an even power of a prime, and $m \geq 1/\epsilon^2$. There is an infinite family of error-correcting codes $\{C_n\}_n$, where C_n satisfies the following properties:*

1. *$C_n : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^n$ is a linear code of rate at least R that can be encoded in time* $\mathrm{poly}(\log q, m, n)$.
2. *There exists an injective $\mathbb{F}_q$-linear map $\phi : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^{\hat{k}}$, where $\hat{k} \leq n$, so that C_n can be list decoded from a $(1 - R - \epsilon)$-fraction of errors, pinning down the images of the candidate messages under ϕ (viewed as length $\hat{k}m$ vectors over $\mathbb{F}_q$) to an affine shift of a $(\hat{k}, m, \epsilon m)$-*BTT *subspace V over $\mathbb{F}_q$. Moreover, the map ϕ, a basis for V, and the affine shift can be computed in time* $\mathrm{poly}(\log q, m, n)$.

We prove the above theorem in Section 6 using AG codes with subfield evaluation points. As a warm-up, we first prove, in Section 4, that this theorem holds in the more basic setting of RS codes with subfield evaluation points. In the RS setting, the linear-algebraic approach of [GX13] gives a functional equation of the form

$$A_0(X) + A_1(X)f(X) + A_2(X)f^{\sigma}(X) + \cdots + A_s(X)f^{\sigma^{s-1}}(X) = 0$$

that any low-degree polynomial f that has large agreement with a received word $\mathbf{y}$ must satisfy, where σ denotes the *Frobenius automorphism* mapping $f = \sum_{j=0}^{k-1} f_j X^j$ to $f = \sum_{j=0}^{k-1} f_j^q X^j$, and the coefficients of $A_0, \ldots, A_s$ depend on the received word $\mathbf{y}$.

We observe that the above functional equation quite naturally gives a $(k, m, (1 - \epsilon)m)$-BTT matrix, so that the solution set is contained in an affine shift of the *kernel* of this matrix.[7] We then show that the kernel of a (k, m, r)-BTT matrix is in fact a $(k, m, m - r)$-BTT subspace (i.e., the *image* of a $(k, m, m - r)$-BTT matrix), which gives the claimed $(k, m, \epsilon m)$-BTT subspace containing the list (in this setting, ϕ is just the identity map). We further show that a similar reasoning can be applied in the AG code setting.

2.2 BTT evasive subspace

We say that a subspace $W \subseteq \mathbb{F}_q^{km}$ is a (k, m, r, s)-BTT *evasive subspace* if $\dim(V \cap W) \leq s$ for every (k, m, r)-BTT subspace $V \subseteq \mathbb{F}_q^{km}$. Similarly, we say that a subspace $W \subseteq \mathbb{F}_q^{km}$ is a (k, m, r, s)-*periodic evasive subspace* if $\dim(V \cap W) \leq s$ for every (k, m, r)-periodic subspace $V \subseteq \mathbb{F}_q^{km}$. Note that any (r, s)-subspace design over $\mathbb{F}_{q^m}$ of cardinality k is a (k, m, r, s)-periodic evasive subspace (see Corollary 3.1). We first observe, using the probabilistic method, that there exists a (k, m, r, s)-BTT evasive subspace

[7] The fact that the solution set is contained in an affine shift of the kernel of a BTT matrix was also commented (but not exploited) in [GX20, Definition 3]. Here we provide a formal proof for this fact, show that the solution set can be equivalently defined as the image of a BTT matrix, and show that this property can be exploited to obtain improved list sizes.

$W \subseteq \mathbb{F}_q^{km}$ of co-dimension at most ϵkm and $s = O\left(r/\epsilon\right)$. Notably, the lemma holds for any field size q and block length m!

Lemma 2.4. *For every $\epsilon > 0$, positive integers k, m, r with $r < \frac{\epsilon m}{2}$, and a prime power q, there exists a (k, m, r, s)-BTT evasive subspace $W \subseteq \mathbb{F}_q^{km}$ of co-dimension at most ϵkm for $s = \frac{2r}{\epsilon}$.*

Moreover, we are able to explicitly construct BTT evasive subspaces with similar parameters over a field of considerably smaller size than the one required in Theorem 2.1.

Theorem 2.5 (Explicit BTT evasive subspace)**.** *There exists an absolute constant $c > 1$, so that for every $\epsilon > 0$, positive integers k, m, r with $r < \frac{\epsilon m}{24}$, and a prime power q satisfying that $q \geq m^c$, there exists a (k, m, r, s)-BTT evasive subspace $W \subseteq \mathbb{F}_q^{km}$ of co-dimension at most ϵkm for $s = \mathrm{poly}(r/\epsilon)$. Moreover, a basis for W can be found in time $\mathrm{poly}(q, k, m)$.*

We prove the above theorem in Section 3. To this end, we first observe that the iterative construction of [GX13], described above, implicitly gives the following *composition lemma* for *periodic* evasive subspaces. In what follows, for a subspace $W \subseteq \mathbb{F}_q^n$, and a positive integer k, let $W^k \subseteq \mathbb{F}_q^{kn}$ be the subspace containing all vectors $(w_1, \ldots, w_k) \in \mathbb{F}_q^{kn}$ where $w_i \in W$ for all $1 \leq i \leq k$. For a pair of subspaces $W \subseteq \mathbb{F}_q^n$ and $W' \subseteq \mathbb{F}_q^{kn}$, we let $W \circ W' := W^k \cap W'$.

Lemma 2.6 (Implicit in [GX13])**.** *Suppose that W is an "inner" (k, m, r, s)-periodic evasive subspace over $\mathbb{F}_q$, and W' is an "outer" (k', km, s, s')-periodic evasive subspace over $\mathbb{F}_q$. Then $W \circ W' = W^k \cap W'$ is a $(k'k, m, r, s')$-periodic evasive subspace over $\mathbb{F}_q$.*

Roughly speaking, the above lemma gives a way to combine together an "inner" periodic evasive subspace W with a short block length m (but a relatively small number of blocks k) with an "outer" periodic evasive subspace W' with a large number of blocks k' (but a long block length m'), to obtain a periodic evasive subspace $W \circ W'$ of both short block length m and large number of blocks $\approx k'$ (see Figure 2 below for an illustration). Applying this lemma iteratively for $\log^* k$ times, using the explicit subspace design given by Theorem 2.1 (which is in particular a periodic evasive subspace), gives the main result of [GX13] which reduces the list size of AG codes with subfield evaluation points to triply-exponential in $\log^* n$.

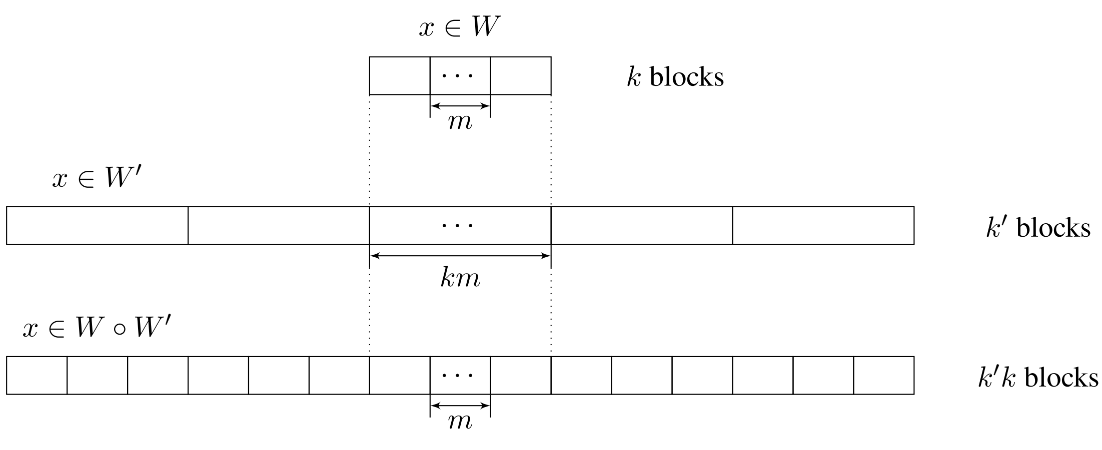

Figure 2: Illustration of the first two parameters in composition.

We further observe that essentially the same composition lemma holds when replacing the inner periodic evasive subspace with a BTT *evasive subspace*, in which case the resulting composed subspace is a BTT evasive subspace as well.

Lemma 2.7. *Suppose that W is an "inner" (k, m, r, s)-BTT evasive subspace over $\mathbb{F}_q$, and W' is an "outer" (k', km, s, s')-periodic evasive subspace over $\mathbb{F}_q$. Then $W \circ W' = W^{k'} \cap W'$ is a $(k'k, m, r, s')$-BTT evasive subspace over $\mathbb{F}_q$.*

To prove Theorem 2.5, we first apply the above composition lemma with the inner subspace being the non-explicit (k_1, m, r, s_1)-BTT evasive subspace, given by Lemma 2.4, for $k_1 \approx \log\log k$ (which can be found efficiently via brute-force search in this setting of parameters), and the outer subspace being the explicit $(k_2, k_1 m, s_1, s_2)$-periodic evasive subspace, given by Theorem 2.1, for $k_2 = \log k \approx \exp(k_1)$. Then we apply the above composition lemma once more with the inner subspace being the resulting $(k_2 k_1, m, r, s_2)$-BTT evasive subspace, and the outer subspace being yet another explicit $(k_3, k_1 k_2 m, s_2, s_3)$-periodic evasive subspace, given by Theorem 2.1, for $k_3 \approx k \approx \exp(k_2)$. As we apply the composition step only twice, this results in a (k, m, r, s_3)-BTT evasive subspace for $s_3 = \mathrm{poly}(r/\epsilon)$. A careful choice of parameters gives the explicit BTT evasive subspace claimed in Theorem 2.5.

Finally, we note that the above composition method is reminiscent of the classical technique of *code concatenation* [For66]. Roughly speaking, code concatenation is a technique for reducing the alphabet size of a code, where one starts with a long outer code over a large alphabet, and then reduces the alphabet size by encoding each large alphabet symbol with a short inner code over a smaller alphabet. Curiously, the parameters obtained by concatenation are very similar to those obtained by the above Composition Lemma 2.7, when viewing k as the codeword length and q^m as the alphabet size of the code.

In particular, a well-known method for constructing *asymptotically good* codes (i.e., codes with constant rate and distance) over small alphabets (e.g., the binary alphabet) is to first concatenate an inner asymptotically good code over a small alphabet of length $k_1 \approx \log\log k$ (which can be found via brute-force search) with an outer RS code of alphabet size $\approx \exp(k_1)$ and length $k_2 \approx \log k \approx \exp(k_1)$, and then concatenate the resulting code with another outer RS code of alphabet size $\approx k \approx \exp(k_2)$ and length $\approx k$. Our construction of BTT evasive subspaces uses the same two-level construction, with the explicit subspace design of Theorem 2.1 playing the role of the RS code over a large alphabet, and the non-explicit BTT evasive subspace of Lemma 2.4 playing the role of the non-explicit asymptotically good code over a small alphabet. However, despite the technical resemblance, we could not find any formal connection between code concatenation and the above composition method for evasive subspaces. We further note that a similar two-step composition approach was also used in other settings in theoretical computer science such as the original proof of the PCP theorem [ALM+98].

2.3 Proof of Main Theorem 1.1

Our main Theorem 1.1 follows as an immediate corollary of the above Theorems 2.3 and 2.5.

Proof of Theorem 1.1. Let $\epsilon' = \frac{\epsilon}{26}$ and $R' = R + 25\epsilon'$. Let $m = 1/(\epsilon')^2$, and let $q = \mathrm{poly}(1/\epsilon)$ be an even power of a prime so that $q \geq m^c$, where $c > 1$ is a sufficiently large constant for which both Theorems 2.3 and 2.5 hold. Let $\{C_n\}_n$ be the infinite family of codes, guaranteed by Theorem 2.3, with the following properties for each C_n:

1. $C_n : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^n$ is a linear code of rate at least R' that can be encoded in time $\mathrm{poly}(1/\epsilon, n)$.

2. There exists an injective linear map $\phi : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^{\hat{k}}$, where $\hat{k} \leq n$, so that C_n can be list decoded from a $(1 - R' - \epsilon')$-fraction of errors, pinning down the images of the candidate messages under ϕ (viewed as length $\hat{k}m$ vectors over $\mathbb{F}_q$) to an affine shift of a $(\hat{k}, m, \epsilon' m)$-$\mathrm{BTT}$ subspace V over $\mathbb{F}_q$. Moreover, the map ϕ, a basis for V, and the affine shift can be computed in time $\mathrm{poly}(1/\epsilon, n)$.

Fix a code C_n as above, and let $\epsilon'' = 25\epsilon'$. By Theorem 2.5, there exists a $(\hat{k}, m, \epsilon' m, s)$-BTT evasive subspace $W \subseteq \mathbb{F}_q^{\hat{k}m}$ of co-dimension at most $\epsilon''\hat{k}m$ for $s = \mathrm{poly}(1/\epsilon)$, and a basis for W can be found in time $\mathrm{poly}(1/\epsilon, n)$. Let C'_n be the code obtained from C_n by restricting the message space to $\phi^{-1}(W)$. We claim that C'_n satisfies Theorem 1.1.

Note first that C'_n is an $\mathbb{F}_q$-linear code of rate at least $R' - \epsilon''\hat{k}/n \geq R' - \epsilon'' = R$, and alphabet size $q^m = (1/\epsilon)^{O(1/\epsilon^2)}$, that can be encoded in time $\mathrm{poly}(1/\epsilon, n)$. Moreover, as $1 - R' - \epsilon' = 1 - R - \epsilon$, the code C_n can be list decoded from a $(1 - R - \epsilon)$-fraction of errors, pinning down the images of the candidate messages under ϕ (viewed as length $\hat{k}m$ vectors over $\mathbb{F}_q$) to an affine shift $\mathbf{u}$ of a $(\hat{k}, m, \epsilon' m)$-BTT subspace V over $\mathbb{F}_q$. This means that the candidate messages of the code C_n are contained in $\phi^{-1}(\mathbf{u} + V)$.

As C'_n is obtained from C_n by restricting the message space to $\phi^{-1}(W)$, the candidate messages of C'_n are contained in

$$\phi^{-1}(\mathbf{u} + V) \cap \phi^{-1}(W) = \phi^{-1}((\mathbf{u} + V) \cap W),$$

which is an affine shift of $\phi^{-1}(V \cap W)$ (or empty). We can find a basis B for $\phi^{-1}(V \cap W)$ and a vector $\mathbf{u}' \in \phi^{-1}((\mathbf{u} + V) \cap W)$ (if such exists) in time $\mathrm{poly}(1/\epsilon, n)$ given the received word. Then the list of candidate messages of C'_n is contained in the subspace spanned by B and $\mathbf{u}'$ over $\mathbb{F}_q$, whose dimension is bounded by $\dim(V \cap W) + 1 \leq s + 1 = \mathrm{poly}(1/\epsilon)$, and a basis for this subspace can be found in time $\mathrm{poly}(1/\epsilon, n)$. Consequently, the output list size is $\exp(\mathrm{poly}(1/\epsilon))$ and the entire list can be output in time $\exp(\mathrm{poly}(1/\epsilon)) \cdot \mathrm{poly}(n)$, as claimed. $\square$

Open problems. We end this section with a couple of intriguing open problems.

1. Is it possible to explicitly construct capacity-achieving list decodable codes with list size $\mathrm{poly}(1/\epsilon)$ (even over a large super-constant alphabet)? As mentioned above, the smallest known list size for explicit capacity-achieving list decodable codes is $(1/\epsilon)^{O(1/\epsilon)}$, achieved by FRS codes [KRSW18], while potentially the list size could be as small as $O(1/\epsilon)$, as is the case for random codes. Such a construction could also potentially lead to *fully polynomial-time* $\mathrm{poly}(1/\epsilon, n)$ list-decoding algorithms.

2. Is it possible to obtain capacity-achieving list decodable codes with *truly linear-time* encoding or list decoding algorithms? As in the unique decoding setting, this seems to require completely different techniques, e.g., graph-based constructions [MRR+20, RWZ20].

3. A question that is still widely open is to explicitly construct capacity-achieving list decodable codes over small *fixed-size* alphabets, e.g., the *binary* alphabet. Over a q-ary alphabet, the list-decoding capacity is known to be $h_q^{-1}(1 - R)$, where $h_q(x) = x\log_q(q-1) + x\log_q(1/x) + (1-x)\log_q(1/(1-x))$ is the q-ary entropy function. Once more, this question seems to require completely different techniques such as graph-based constructions [Ta-17, GQST20].

4. Can our methods be used to construct other pseudo-random objects? In particular, an intriguing question is whether these techniques could be used to construct *lossless dimension expanders* over constant-size fields, whose state-of-the-art constructions [GRX18] are based on the list-decoding machinery of [GX13].

Organization. In Section 3 we present our explicit construction of BTT evasive subspaces (Theorem 2.5). In Section 4 we first show, as a warm-up, that the output list of RS codes with subfield evaluation points is contained in an affine shift of a BTT subspace. Then in Section 6, after providing the required AG code preliminaries in Section 5, we show how to extend the analysis to AG codes with subfield evaluation points (Theorem 2.3).

3 Explicit BTT evasive subspace

In this section, we prove Theorem 2.5, which is restated below.

Theorem 2.5 (Explicit BTT evasive subspace)**.** *There exists an absolute constant $c > 1$, so that for every $\epsilon > 0$, positive integers k, m, r with $r < \frac{\epsilon m}{24}$, and a prime power q satisfying that $q \geq m^c$, there exists a (k, m, r, s)-BTT evasive subspace $W \subseteq \mathbb{F}_q^{km}$ of co-dimension at most ϵkm for $s = \mathrm{poly}(r/\epsilon)$. Moreover, a basis for W can be found in time $\mathrm{poly}(q, k, m)$.*

The first ingredient in our proof is Lemma 2.4, restated below, which shows the existence of a (non-explicit) (k, m, r, s)-BTT evasive subspace $W \subseteq \mathbb{F}_q^{km}$ of co-dimension at most ϵkm and $s = O(r/\epsilon)$. Notably, the lemma holds for any field size q and block length m.

Lemma 2.4. *For every $\epsilon > 0$, positive integers k, m, r with $r < \frac{\epsilon m}{2}$, and a prime power q, there exists a (k, m, r, s)-BTT evasive subspace $W \subseteq \mathbb{F}_q^{km}$ of co-dimension at most ϵkm for $s = \frac{2r}{\epsilon}$.*

Proof. Let $W \subseteq \mathbb{F}_q^{km}$ be a random linear subspace of co-dimension ϵkm. Fix a (k, m, r)-BTT subspace $V \subseteq \mathbb{F}_q^{km}$. We first bound the probability that $\dim(V \cap W) \geq s$. Fix a subspace $V^* \subseteq V$ of dimension s. Since W is a random subspace of co-dimension ϵkm, the probability that V^* is contained in W is at most $\prod_{i=0}^{s-1} \frac{q^{(1-\epsilon)km} - q^i}{q^{km} - q^i} \leq q^{-\epsilon kms}$. As the number of s-dimensional subspaces $V^* \subseteq V$ is at most q^{krs}, by a union bound, we have that W contains some s-dimensional subspace $V^* \subseteq V$ with probability at most $q^{(r-\epsilon m)ks}$. So $\dim(V \cap W) \geq s$ with probability at most $q^{(r-\epsilon m)ks}$.

Next, we observe that the number of (k, m, r)-BTT subspaces is at most q^{rkm}, as each such subspace is determined by the first r columns of a (k, m, r)-BTT matrix. Consequently, by a union bound, we get that $\dim(V \cap W) \geq s$ for some (k, m, r)-BTT subspace V, with probability at most $q^{rkm+(r-\epsilon m)ks}$. This latter probability is smaller than 1 since

$$rkm + (r - \epsilon m)ks = rkm + (r - \epsilon m) \cdot \frac{2kr}{\epsilon} = rk\left(\frac{2r}{\epsilon} - m\right) < 0,$$

where the first equality is by our choice of $s = 2r/\epsilon$, and the last inequality is by our choice of $r < \frac{\epsilon m}{2}$. We conclude that there exists a $(k, m, r, \frac{2r}{\epsilon})$-$\mathrm{BTT}$ evasive subspace W of co-dimension at most ϵkm. $\square$

Remark 1. We further note that to find a BTT evasive subspace as above, one can enumerate over all subspaces $W \subseteq \mathbb{F}_q^{km}$ of co-dimension at most ϵkm, and over all (k, m, r)-BTT subspaces V, and compute the dimension of their intersection, which takes time $q^{O((km)^2)}$.

Our second ingredient is Theorem 2.1 from [GK16], restated below, which gives an *explicit* construction of an (r, s)-subspace design over $\mathbb{F}_{q^m}$ of cardinality k, where each subspace has co-dimension at most ϵm and $s = O\left(\frac{r^2}{\epsilon}\right)$, as long as q^m is sufficiently larger than k.

Theorem 2.1 (Explicit subspace design, [GK16], Theorem 6)**.** *There exists an absolute constant $c > 1$, so that for every $\epsilon > 0$, positive integers k, m, r with $r < \frac{\epsilon m}{4}$, and a prime power q satisfying $q^m \geq \max\left\{k^{c \cdot r/\epsilon}, \left(\frac{2r}{\epsilon}\right)^{2r/\epsilon}\right\}$, there exists an (r, s)-subspace design $H_1, \ldots, H_k$ over $\mathbb{F}_{q^m}$ for $s = \frac{2r^2}{\epsilon}$, where each H_i has co-dimension at most ϵm in $\mathbb{F}_{q^m}$. Moreover, bases for $H_1, \ldots, H_k$ can be found in time $\mathrm{poly}(q, k, m)$.*

For completeness, we sketch the proof of the above theorem in Appendix A. Note that the above theorem in particular gives an explicit periodic evasive subspace with the same parameters.

Corollary 3.1 (Explicit periodic evasive subspace)**.** *There exists an absolute constant $c > 1$, so that for every $\epsilon > 0$, positive integers k, m, r with $r < \frac{\epsilon m}{4}$, and a prime power q satisfying $q^m \geq \max\left\{k^{c \cdot r/\epsilon}, \left(\frac{2r}{\epsilon}\right)^{2r/\epsilon}\right\}$, there exists a (k, m, r, s)-periodic evasive subspace $W \subseteq \mathbb{F}_q^{km}$ of co-dimension at most ϵkm for $s = \frac{2r^2}{\epsilon}$. Moreover, a basis for W can be found in time $\mathrm{poly}(q, k, m)$.*

Proof. Let $H_1, H_2, \ldots, H_k$ be the (r, s)-subspace design over $\mathbb{F}_{q^m}$ guaranteed by Theorem 2.1 for the same choice of parameters, and let $W = H_1 \times H_2 \times \cdots \times H_k$. Then by Theorem 2.1, we clearly have that a basis for W is a subspace of $\mathbb{F}_q^{km}$ of co-dimension at most ϵkm, and that W can be found in time $\mathrm{poly}(q, k, m)$. It remains to show that W is a (k, m, r, s)-periodic evasive subspace. Let M be a (k, m, r)-periodic matrix, and let $V = \mathrm{Image}(M)$, we would like to show that $\dim(V \cap W) \leq s$.

By definition, M is a block-lower-triangular matrix with k copies of an $m \times r$ matrix $\hat{M}$ on the main diagonal, and $\hat{M}$ has full column rank r. Let $\hat{V} = \mathrm{Image}(\hat{M})$, which is a subspace of $\mathbb{F}_q^m$ of dimension r. For $i \in [k]$, choose an $m \times m$ matrix R_i such that $H_i = \ker(R_i)$, and let $R \in \mathbb{F}_q^{km \times km}$ be a $(k \times k)$-block diagonal matrix with blocks $R_1, R_2, \ldots, R_k$ on the main diagonal. Note that $W = \ker(R)$, and furthermore, $RM \in \mathbb{F}_q^{km \times kr}$ is a $(k \times k)$-block-lower-triangular matrix with blocks $R_1\hat{M}, R_2\hat{M}, \ldots, R_k\hat{M}$ on the main diagonal.

So we have

$$\begin{aligned}
\dim(V \cap W) &= \dim(V \cap \ker(R)) \\
&= \dim(\ker(RM)) \leq \sum_{i=1}^{k} \dim(\ker(R_i\hat{M})) \\
&= \sum_{i=1}^{k} \dim(\hat{V} \cap \ker(R_i)) = \sum_{i=1}^{k} \dim(\hat{V} \cap H_i) \leq s,
\end{aligned}$$

where the last inequality follows since $H_1, \ldots, H_k$ is an (r, s)-subspace design. $\square$

Our last ingredient is Lemma 2.7, restated below, which gives a composition lemma for BTT evasive subspaces.

Lemma 2.7. *Suppose that W is an "inner" (k, m, r, s)-BTT evasive subspace over $\mathbb{F}_q$, and W' is an "outer" (k', km, s, s')-periodic evasive subspace over $\mathbb{F}_q$. Then $W \circ W' = W^{k'} \cap W'$ is a $(k'k, m, r, s')$-BTT evasive subspace over $\mathbb{F}_q$.*

Proof. Let V be a $(k'k, m, r)$-BTT subspace. Our goal is to show that $\dim(V \cap (W^{k'} \cap W')) \leq s'$. Since W' is a (k', km, s, s')-periodic evasive subspace, it suffices to show that $V' := V \cap W^{k'}$ is contained in a (k', km, s)-periodic subspace U, and consequently

$$\dim(V \cap (W^{k'} \cap W')) = \dim((V \cap W^{k'}) \cap W') \leq \dim(U \cap W') \leq s'.$$

Since V is a $(k'k, m, r)$-BTT subspace, there exists a $(k'k, m, r)$-BTT matrix M whose image equals V. As a $k' \times k'$ block matrix, M has k' copies of a $(km) \times (kr)$ block $\hat{M}$ on its main diagonal. Next observe that $\hat{M}$ itself is a (k, m, r)-BTT matrix, and so if we let $\hat{V} := \mathrm{Image}(\hat{M})$, then $\hat{V}$ is a (k, m, r)-BTT subspace. Recalling our assumption that W is a (k, m, r, s)-BTT evasive subspace, this implies in turn that $\dim(\hat{V} \cap W) \leq s$. Let $H \subseteq \mathbb{F}_q^{km}$ be a subspace of dimension s containing $\hat{V} \cap W$, and let $\{b^{(1)}, \ldots, b^{(s)}\} \subseteq \mathbb{F}_q^{km}$ be a basis for H.

Next, we introduce a bit of notation. We write a vector $x \in \mathbb{F}_q^{k'km}$ as $x = (x_1, x_2, \ldots, x_{k'})$ where $x_i \in \mathbb{F}_q^{km}$, and for $i = 1, \ldots, k'$, we let $\pi_i(x) = x_i$. For a subspace $X \subseteq \mathbb{F}_q^{k'km}$, and $i = 0, 1, \ldots, k'$, we let

$$X_i = \{(x_1, x_2, \ldots, x_{k'}) \in X \mid x_1 = x_2 = \cdots = x_i = 0\}.$$

In particular, we have $X_0 = X$ and $X_k = \{0\}$.

Claim 3.2. *For all $i = 1, \ldots, k'$, there exist vectors $b^{(i,1)}, \ldots, b^{(i,s)} \in \mathbb{F}_q^{k'km}$ satisfying the following conditions:*

1. *For all $j = 1, \ldots, s$, it holds that $(b^{(i,j)})_1 = \cdots = (b^{(i,j)})_{i-1} = 0$ and $(b^{(i,j)})_i = b^{(j)}$.*
2. $(V \cap W^{k'})_{i-1} \subseteq (V \cap W^{k'})_i + \operatorname{span}\{b^{(i,1)}, \ldots, b^{(i,s)}\}$.

Proof. Fix $i \in [k']$, and let $H' = \pi_i((V \cap W^{k'})_{i-1})$. Note that

$$H' \subseteq \pi_i(V_{i-1}) \cap \pi_i((W^{k'})_{i-1}) = \hat{V} \cap W \subseteq H.$$

Let $t = \dim H'$. Fix a basis $\{v^{(1)}, \ldots, v^{(t)}\}$ for H' and extend it to a basis $\{v^{(1)}, \ldots, v^{(s)}\}$ for H. For $j = 1, \ldots, t$, choose $u^{(j)} \in (V \cap W^{k'})_{i-1}$ such that $(u^{(j)})_i = v^{(j)}$, which is possible since $v^{(j)} \in H' = \pi_i((V \cap W^{k'})_{i-1})$. For $j = t+1, \ldots, s$, choose $u^{(j)} \in \mathbb{F}_q^{k'km}$ with $(u^{(j)})_1 = \cdots = (u^{(j)})_{i-1} = 0$ such that $(u^{(j)})_i = v^{(j)}$. Then we have

$$(V \cap W^{k'})_{i-1} = (V \cap W^{k'})_i + \operatorname{span}\{u^{(1)}, \ldots, u^{(t)}\} \subseteq (V \cap W^{k'})_i + \operatorname{span}\{u^{(1)}, \ldots, u^{(s)}\}. \quad (1)$$

As $\{b^{(1)}, \ldots, b^{(s)}\}$ and $\{v^{(1)}, \ldots, v^{(s)}\}$ are both bases of H, there exists a unique invertible $s \times s$ matrix $A = (a_{j,\ell})_{j,\ell \in [s]}$ over $\mathbb{F}_q$ such that $b^{(j)} = \sum_{\ell=1}^{s} a_{j,\ell} v^{(\ell)}$ for $j \in [s]$. For $j \in [s]$, let $b^{(i,j)} = \sum_{\ell=1}^{s} a_{j,\ell} u^{(\ell)}$, and note that $(b^{(i,j)})_1 = \cdots = (b^{(i,j)})_{i-1} = 0$ and

$$(b^{(i,j)})_i = \sum_{\ell=1}^{s} a_{j,\ell} (u^{(\ell)})_i = \sum_{\ell=1}^{s} a_{j,\ell} v^{(\ell)} = b^{(j)}.$$

So the first condition of the claim is satisfied. As A is invertible, we have $\operatorname{span}\{b^{(i,1)}, \ldots, b^{(i,s)}\} = \operatorname{span}\{u^{(1)}, \ldots, u^{(s)}\}$. Combining this with (1) proves the second condition. $\square$

Now recall that our goal is to exhibit a (k', km, s)-periodic matrix $\tilde{M}$ so that $V \cap W^{k'} \subseteq \operatorname{Image}(\tilde{M})$. We construct $\tilde{M}$ as follows. For $i = 1, \ldots, k'$, let M_i be a $(k'km) \times s$ matrix whose columns are $b^{(i,1)}, \ldots, b^{(i,s)}$. Let

$$\tilde{M} = \begin{pmatrix} M_1 & M_2 & \cdots & M_{k'} \end{pmatrix}.$$

By the first condition of Claim 3.2, we have that $\tilde{M}$ is a (k', km, s)-periodic matrix. By the second condition of Claim 3.2, we further have that $(V \cap W^{k'})_{i-1} \subseteq (V \cap W^{k'})_i + \operatorname{Image}(M_i)$ for all $i = 1, \ldots k'$, and so $V \cap W^{k'} = (V \cap W^{k'})_0 \subseteq \operatorname{Image}(\tilde{M})$, as claimed. This completes the proof of the lemma. $\square$

Next, we prove Theorem 2.5 based on the ingredients above.

Proof of Theorem 2.5. Our goal is to construct a (k, m, r, s)-BTT evasive subspace W of co-dimension at most ϵkm for $s = \operatorname{poly}(r/\epsilon)$. We shall construct W by applying two composition steps. In the first step, we shall compose an inner BTT evasive subspace W_1, given by Lemma 2.4, which can be found via brute-force search, with an outer explicit periodic evasive subspace W_2, given by Corollary 3.1, to obtain a BTT evasive subspace $W_1 \circ W_2$. In the second step, we shall compose the resulting BTT evasive subspace $W_1 \circ W_2$ with yet another outer explicit periodic evasive subspace W_3, given by Corollary 3.1, to obtain our final BTT evasive subspace $W := (W_1 \circ W_2) \circ W_3$. One technical issue is that the desired number of blocks k may not be a multiple of the number of blocks of the inner subspace. This is solved by first constructing a BTT evasive subspace W' in a slightly larger ambient space $\mathbb{F}_q^{k'm} \supseteq \mathbb{F}_q^{km}$ and then letting $W = W' \cap \mathbb{F}_q^{km}$ (where $\mathbb{F}_q^{km}$ is identified with a subspace of $\mathbb{F}_q^{k'm}$ via the map $(x_1, \ldots, x_{km}) \mapsto (0, \ldots, 0, x_1, \ldots, x_{km})$).

In the following, assume $c > 1$ is a large enough constant. Let $\epsilon' = \epsilon/6$. By assumption, we have $r < \epsilon m/24 = \epsilon' m/4$ and $q \geq m^c$.

BTT evasive subspace W_1: Let W_1 be a (k_1, m, r, s_1)-BTT evasive subspace of co-dimension at most $\epsilon' k_1 m$ for $k_1 = c^2 m^3 \cdot \lceil \frac{\log\log k}{\log q} \rceil$ and $s_1 = \frac{2r^2}{\epsilon'} \geq \frac{2r}{\epsilon'}$. Note that such a subspace exists by Lemma 2.4. We further claim that a basis for W_1 can be found in time $\mathrm{poly}(q, k, m)$. To see this, first note that if $m \log q \leq (c^2 \log\log k + c^2)^{c+1}$, then by Remark 1, a basis for W_1 can be found in time

$$q^{O((k_1 \cdot m)^2)} = 2^{O(k_1^2 m^2 \log q)} \leq \exp(\mathrm{poly}(\log\log k)) \leq \mathrm{poly}(k). \tag{2}$$

On the other hand, if $m \log q > (c^2 \log\log k + c^2)^{c+1}$, then either $m > c^2 \log\log k + c^2$ or $q > \log q > (c^2 \log\log k + c^2)^c$. In either case, we have $q \geq (c^2 \log\log k + c^2)^c$ since $q \geq m^c$. This implies

$$q \geq q^{1/4} m^{(3/4)c} > \left(c^2 m^3 \cdot \left\lceil \frac{\log\log k}{\log q} \right\rceil \right)^{c/4} = k_1^{c/4}.$$

Therefore,

$$q^m \geq \max\{k_1^{cm/4}, m^m\} \geq \max\left\{ k_1^{c \cdot r/\epsilon'}, \left(\frac{2r}{\epsilon'}\right)^{2r/\epsilon'} \right\} \tag{3}$$

where we use the facts $r < \epsilon' m/4$ and $q \geq m^c \geq m$. Consequently, by Corollary 3.1, there exists a $(k_1, m, r, \frac{2r^2}{\epsilon'})$-periodic evasive subspace W_1 of co-dimension at most $\epsilon' k_1 m$, which is in particular a BTT evasive subspace with the same parameters. Moreover, a basis for W_1 can be found in time $\mathrm{poly}(q, k_1, m) = \mathrm{poly}(q, k, m)$.

Periodic evasive subspace W_2: Let W_2 be a $(k_2, k_1 m, s_1, s_2)$-periodic evasive subspace of co-dimension at most $\epsilon' k_2 k_1 m$ for $k_2 = \lceil \log k \rceil$ and $s_2 = \frac{2s_1^2}{\epsilon'} = \frac{8r^4}{(\epsilon')^3}$. Note that such a subspace exists by Corollary 3.1 as

$$s_1 = \frac{2r^2}{\epsilon'} < \frac{c^2 \epsilon' m^2}{4} \leq \frac{\epsilon' k_1 m}{4},$$

$$q^{k_1 m} \geq \lceil \log k \rceil^{c^2 m^2} > \lceil \log k \rceil^{2c(r/\epsilon')^2} = k_2^{c \cdot s_1/\epsilon'}, \tag{4}$$

and

$$q^{k_1 m} \geq \left(\frac{m^2}{4}\right)^{m^2/4} > \left(\frac{4r^2}{(\epsilon')^2}\right)^{4r^2/(\epsilon')^2} = \left(\frac{2s_1}{\epsilon'}\right)^{2s_1/\epsilon'}$$

where the inequalities hold by the choice of $k_1 = c^2 m^3 \cdot \lceil \frac{\log\log k}{\log q} \rceil$ and the assumptions $r < \frac{\epsilon' m}{4}$ and $q \geq m^c$. Moreover, a basis for W_2 can be found in time $\mathrm{poly}(q, k_2, k_1 m) = \mathrm{poly}(q, k, m)$.

BTT evasive subspace $W_1 \circ W_2$**:** By Lemma 2.7, we have that $W_1 \circ W_2 = W_1^{k_2} \cap W_2$ is a (k_1k_2, m, r, s_2)-BTT evasive subspace for $s_2 = \frac{8r^4}{(\epsilon')^3}$. Note furthermore that $W_1 \circ W_2$ has co-dimension at most $2\epsilon' k_1 k_2 m$, and a basis for $W_1 \circ W_2$ can be found in time $\mathrm{poly}(q, k, m)$.

Periodic evasive subspace W_3**:** Let W_2 be a (k_3, k_1k_2m, s_2, s_3)-periodic evasive subspace of co-dimension at most $\epsilon' k_1 k_2 k_3 m$ for $k_3 = \lceil \frac{k}{k_1 k_2} \rceil$ and $s_3 = \frac{2s_2^2}{\epsilon'} = \frac{128 r^8}{(\epsilon')^7}$. Note that such a subspace exists by Corollary 3.1 as

$$s_2 = \frac{8r^4}{(\epsilon')^3} < \frac{c^2 \epsilon' m^4}{4} \le \frac{\epsilon' k_1 k_2 m}{4},$$

$$q^{k_1 k_2 m} \ge k^{c^2 m^4} > k^{8c(r/\epsilon')^4} \ge k_3^{c \cdot s_2/\epsilon'},$$

and

$$q^{k_1 k_2 m} \ge \left(\frac{m^4}{16}\right)^{m^4/16} > \left(\frac{16r^4}{(\epsilon')^4}\right)^{16r^4/(\epsilon')^4} = \left(\frac{2s_2}{\epsilon'}\right)^{2s_2/\epsilon'}$$

where the inequalities hold once more by the choice of $k_1 = c^2 m^3 \cdot \lceil \frac{\log \log k}{\log q} \rceil$ and $k_2 = \lceil \log k \rceil$ together with the assumptions $r < \epsilon' m/4$ and $q \ge m^c$. Moreover, a basis for W_3 can be found in time $\mathrm{poly}(q, k_3, k_1 k_2 m) = \mathrm{poly}(q, k, m)$.

BTT evasive subspace $W' = (W_1 \circ W_2) \circ W_3$**:** By Lemma 2.7, we have that $W' := (W_1 \circ W_2) \circ W_3$ is a $(k_1 k_2 k_3, m, r, s_3)$-BTT evasive subspace for $s_3 = \frac{128 r^8}{\epsilon^7} = \mathrm{poly}(r/\epsilon)$. Note furthermore that W' has co-dimension at most $3\epsilon' k_1 k_2 k_3 m$, and a basis for W' can be found in time $\mathrm{poly}(q, k, m)$.

BTT evasive subspace W**:** If k is a multiple of $k_1 k_2$, then $k_1 k_2 k_3 = k$ and we may choose $W = W'$ as the desired BTT evasive subspace. Next, we explain how to extend it to arbitrary k.

1. First assume $k \ge k_1 k_2$ so that $k' := k_1 k_2 k_3 = k_1 k_2 \lceil \frac{k}{k_1 k_2} \rceil$ satisfies $k' \le 2k$. Then $W' \subseteq \mathbb{F}_q^{k'm}$ is a (k', m, r, s_3)-BTT evasive subspace of co-dimension at most $3\epsilon' k' m \le 6\epsilon' k m = \epsilon k m$. Identify $\mathbb{F}_q^{km}$ with a subspace of $\mathbb{F}_q^{k'm}$ via the map $(x_1, \ldots, x_{km}) \mapsto (0, \ldots, 0, x_1, \ldots, x_{km})$. We let $W := W' \cap \mathbb{F}_q^{km}$, whose co-dimension in $\mathbb{F}_q^{km}$ is at most $\epsilon k m$ since the co-dimension of W' in $\mathbb{F}_q^{k'm}$ is at most $\epsilon k m$.

   Consider any (k, m, r)-BTT subspace $V \subseteq \mathbb{F}_q^{km}$. Note that there exists a (k', m, r)-BTT subspace $V' \subseteq \mathbb{F}_q^{k'm}$ such that $V = V' \cap \mathbb{F}_q^{km}$. As W' is a (k', m, r, s_3)-BTT evasive subspace, we have $\dim(V' \cap W') \le s_3$, which implies $\dim(V \cap W) \le s_3$. So $W \subseteq \mathbb{F}_q^{km}$ is a (k, m, r, s)-BTT evasive subspace of co-dimension at most $\epsilon k m$ for $s = s_3 = \mathrm{poly}(r/\epsilon)$.

2. Now assume $k_1 \le k < k_1 k_2$. Let $k_2' := \lceil \frac{k}{k_1} \rceil \le k_2$ so that $k_2' k_1 \le 2k$. By replacing k_2 with k_2' in the construction of W_2, we may construct a $(k_2', k_1 m, s_1, s_2)$-periodic evasive subspace W_2' of co-dimension at most $\epsilon' k_2' k_1 m$. This is because replacing k_2 by $k_2' \le k_2$ preserves (4). Composing W_2' with W_1 gives a $(k_1 k_2', m, r, s_2)$-BTT evasive subspace $W_1 \circ W_2' \subseteq \mathbb{F}_q^{k_1 k_2' m}$ of co-dimension at most $2\epsilon' k_2' k_1 m \le 4\epsilon' k m \le \epsilon k m$. Similarly to the previous case, restricting to the subspace $\mathbb{F}_q^{km}$ yields the desired (k, m, r, s)-BTT evasive subspace W of co-dimension at most $\epsilon k m$ for $s = s_2 = \mathrm{poly}(r/\epsilon)$.

3. Finally, assume $k < k_1$. By replacing k_1 with k in the construction of W_1, we may construct the desired (k, m, r, s)-BTT evasive subspace W of co-dimension at most $\epsilon' k m \le \epsilon k m$ for $s = s_1 = \mathrm{poly}(r/\epsilon)$. This is because replacing k_1 by $k < k_1$ preserves (2) and (3).

□

4 Reed–Solomon codes with subfield evaluation points

We first show, as a warm-up, that RS codes with evaluation points over a subfield are list decodable up to capacity with the output list contained in an affine shift of a BTT subspace. Later, in Section 6, we shall show how the analysis can be extended to AG codes over constant-size alphabets, thus proving Theorem 2.3. We start with the formal definition of RS codes with subfield evaluation points.

Definition 4.1 (RS codes with subfield evaluation points)**.** *Let $n, k, m \in \mathbb{N}^+$ be such that $k \leq n$, and let $q \geq n$ be a prime power. The* Reed–Solomon code $\mathsf{RS}_{q,m}(n,k)$ over $\mathbb{F}_{q^m}$ with evaluation points in $\mathbb{F}_q$ *maps a polynomial $f \in \mathbb{F}_{q^m}[X]$ of degree at most $k-1$ (viewed as a length k vector of coefficients over $\mathbb{F}_{q^m}$) to the codeword $C_f := (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \in (\mathbb{F}_{q^m})^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are n distinct elements in $\mathbb{F}_q$.*

Note that $\mathsf{RS}_{q,m}(n,k)$ is a linear code over the alphabet $\mathbb{F}_{q^m}$ with codeword length n, rate k/n, and minimum distance $n-k+1$. In this section, we show that this code is also list decodable up to its minimum distance with the output list being contained in an affine shift of a BTT subspace.

Theorem 4.2. *Let $\epsilon > 0$, let $n, k, m \in \mathbb{N}^+$ be such that $k \leq n$ and $m \geq 1/\epsilon^2$, and let $q \geq n$ be a prime power. Then $\mathsf{RS}_{q,m}(n,k)$ can be list decoded from up to $(1-\epsilon)(n-k)$ errors, pinning down the candidate messages (viewed as length km vectors of coefficients over $\mathbb{F}_q$) to an affine shift of a $(k, m, \epsilon m)$-BTT subspace V over $\mathbb{F}_q$. Moreover, a basis for V and the affine shift can be found in time* $\mathrm{poly}(\log q, m, n)$.

The above theorem is a consequence of the following lemma.

Lemma 4.3. *Let $n, k, m \in \mathbb{N}^+$ be such that $k \leq n$, and let $q \geq n$ be a prime power. Let $s \in [m]$ and $t, d \in \mathbb{N}^+$ be parameters, satisfying that*

$$(s+1)(d+1) + k - 1 > n \tag{5}$$

and

$$t > d + k - 1. \tag{6}$$

Then $\mathsf{RS}_{q,m}(n,k)$ can be list decoded from agreement at least t, pinning down the candidate messages (viewed as length km vectors of coefficients over $\mathbb{F}_q$) to an affine shift of a $(k, m, s-1)$-BTT subspace V over $\mathbb{F}_q$. Moreover, a basis for V and the affine shift can be found in time $\mathrm{poly}(\log q, m, n)$.

Before we prove the above lemma, we show how it implies Theorem 4.2.

Proof of Theorem 4.2. Let $s = \frac{1}{\epsilon} + 1$, let $d = \frac{n-k+2}{s+1} - 1$ so that (5) is satisfied, and let $t = d + k$ so that (6) is satisfied. Then with this setting of parameters, $\mathsf{RS}_{q,m}(n,k)$ can be list decoded from agreement t, or equivalently, from up to

$$n - t = n - d - k = n - k + 1 - \frac{n-k+2}{s+1} \geq n - k - \frac{n-k}{s-1} = (1-\epsilon)(n-k).$$

errors. Moreover, by choice of $m \geq 1/\epsilon^2$, we have that V is a $(k, m, s-1)$-BTT subspace for $s - 1 = \frac{1}{\epsilon} \leq \epsilon m$. □

The rest of this section is devoted to the proof of Lemma 4.3. To prove this lemma, we follow the linear-algebraic approach of [GX13]. Suppose that $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in (\mathbb{F}_{q^m})^n$ is a received word. Our goal is to show that all polynomials $f \in \mathbb{F}_{q^m}[X]_{<k}$ that have large agreement with $\mathbf{y}$ are contained in an affine shift of a BTT subspace. To this end, following [GX13], we first show in Section 4.1 the existence of a nonzero polynomial Q (depending on the received word $\mathbf{y}$) that gives a functional equation that any polynomial f that has large agreement with $\mathbf{y}$ must satisfy. Then we show in Section 4.2 that this functional equation induces a special structure on the solution set, specifically, the solution set is contained in an affine shift of the kernel of a BTT matrix. Finally, in Section 4.3 we show that the kernel of a BTT matrix is a BTT subspace, which implies that the solution set is contained in an affine shift of a BTT subspace. We further show that the polynomial Q, a basis for the BTT subspace V, and the affine shift could be found efficiently.

4.1 The polynomial Q

In what follows, let $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ be the *Frobenius automorphism* $a \mapsto a^q$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It extends to an automorphism of $\mathbb{F}_{q^m}[X]$ over $\mathbb{F}_q$ by acting on the coefficients, which we also denote by σ by a slight abuse of notation. For $f \in \mathbb{F}_{q^m}[X]$, denote by f^σ the element $\sigma(f)$.

Suppose that $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in (\mathbb{F}_{q^m})^n$ is a received word. We let Q be a nonzero multivariate polynomial in $(\mathbb{F}_{q^m}[X])[Y_1, Y_2, \ldots, Y_s]$ of the form

$$Q = A_0 + A_1 Y_1 + A_2 Y_2 + \cdots + A_s Y_s,$$

where $A_0, A_1, \ldots, A_s \in \mathbb{F}_{q^m}[X]$, $\deg(A_0) \leq d + k - 1$, and $\deg(A_i) \leq d$ for $i = 1, 2, \ldots, s$. We also require the polynomials A_i to satisfy the constraint

$$A_0(\alpha_i) + A_1(\alpha_i) y_i + A_2(\alpha_i) y_i^{\sigma} + \cdots + A_s(\alpha_i) y_i^{\sigma^{s-1}} = 0 \tag{7}$$

for all $i = 1, \ldots, n$, where $\alpha_1, \ldots, \alpha_n$ are the evaluation points.

We first claim that such a nonzero polynomial Q exists and can be computed efficiently. To see this, think of the coefficients of the polynomials A_i as unknowns. This gives $d + k + s(d+1) = (s+1)(d+1) + k - 1$ unknowns in total, while (7) gives n homogeneous linear constraints over $\mathbb{F}_{q^m}$. By (5), the number of unknowns is greater than the number of linear constraints which guarantees the existence of a nonzero solution Q. Moreover, we can find Q in time $\mathrm{poly}(\log q, m, n)$ by solving the system of linear equations represented by (7).

Next, we show that Q gives a functional equation that any f that has sufficiently large agreement with the received word $\mathbf{y}$ needs to satisfy.

Claim 4.4. *Let $f \in \mathbb{F}_{q^m}[X]_{<k}$. Suppose that $\mathbf{y}$ agrees with the codeword $C_f = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n))$ in at least t coordinates. Then f satisfies the functional equation*

$$Q(f, f^\sigma, \ldots, f^{\sigma^{s-1}}) = A_0 + A_1 f + A_2 f^\sigma + \cdots + A_s f^{\sigma^{s-1}} = 0. \tag{8}$$

Proof. Define

$$Q^* = A_0 + A_1 f + A_2 f^\sigma + \cdots + A_s f^{\sigma^{s-1}} \in \mathbb{F}_{q^m}[X].$$

We want to prove that $Q^* = 0$. As $\deg(f) \leq k - 1$, $\deg(A_0) \leq d + k - 1$, and $\deg(A_i) \leq d$ for $i = 1, 2, \ldots, s$, we know that $\deg(Q^*) \leq d + k - 1$.

Suppose that $\mathbf{y}$ agrees with C_f in the i-th symbol for some $i \in [n]$, i.e., $y_i = f(\alpha_i)$. By (7), we have

$$\begin{aligned}
0 &= A_0(\alpha_i) + A_1(\alpha_i)y_i + A_2(\alpha_i)y_i^{\sigma} + \cdots + A_s(\alpha_i)y_i^{\sigma^{s-1}} \\
&= A_0(\alpha_i) + A_1(\alpha_i)f(\alpha_i) + A_2(\alpha_i)(f(\alpha_i))^{\sigma} + \cdots + A_s(\alpha_i)(f(\alpha_i))^{\sigma^{s-1}} \\
&= A_0(\alpha_i) + A_1(\alpha_i)f(\alpha_i) + A_2(\alpha_i)f^{\sigma}(\alpha_i) + \cdots + A_s(\alpha_i)f^{\sigma^{s-1}}(\alpha_i) \\
&= (A_0 + A_1 f + A_2 f^{\sigma} + \cdots + A_s f^{\sigma^{s-1}})(\alpha_i) \\
&= Q^*(\alpha_i).
\end{aligned}$$

The third equality uses the fact that $(f(\alpha_i))^{\sigma} = f^{\sigma}(\alpha_i^{\sigma}) = f^{\sigma}(\alpha_i)$, which holds since $\alpha_i \in \mathbb{F}_q$ is fixed by σ.

As $\mathbf{y}$ and C_f agree in at least t symbols, the above argument shows that Q^* has at least t zeros. On the other hand, the degree of Q^* is at most $d + k - 1$, which is less than t by (6). This implies $Q^* = 0$. $\square$

4.2 The BTT subspace V

Next, we show that the functional equation (8), given by Claim 4.4 above, implies that the list of candidate messages is contained in an affine shift of the kernel of a BTT subspace. We start by expanding the functional equation (8) in terms of the coefficients of the polynomial f and $A_0, A_1, \ldots, A_s$.

As $f \in \mathbb{F}_{q^m}[X]_{<k}$, we may write

$$f = \sum_{j=0}^{k-1} f_j X^j$$

where the coefficients f_i are in $\mathbb{F}_{q^m}$. Also write

$$A_\ell = \sum_{i=0}^{d+k-1} a_{\ell,i} X^i, \quad \ell = 0, 1, \ldots, s,$$

where the coefficients $a_{\ell,i}$ are in $\mathbb{F}_{q^m}$ and $a_{\ell,i} = 0$ for $\ell \in [s]$ and $i > d$. Choose the largest integer $u \geq 0$ such that X^u divides A_ℓ for $\ell = 0, 1, \ldots, s$. By replacing Q with Q/X^u, we may assume that $u = 0$. So $a_{\ell,0} \neq 0$ for some $\ell \in \{0, 1, \ldots, s\}$. By (8), we actually have $a_{\ell,0} \neq 0$ for some $\ell \in [s]$.

With the notations above, (8) becomes

$$\begin{aligned}
0 &= \sum_{i=0}^{d+k-1} a_{0,i} X^i + \sum_{\ell=1}^{s} \left(\sum_{i=0}^{d} a_{\ell,i} X^i \right) \left(\sum_{j=0}^{k-1} f_j^{\sigma^{\ell-1}} X^j \right) \\
&= \sum_{i=0}^{d+k-1} \left(a_{0,i} + \sum_{\ell=1}^{s} \sum_{j=0}^{i} a_{\ell,i-j} f_j^{\sigma^{\ell-1}} \right) X^i,
\end{aligned}$$

where we let $f_i = 0$ for $i \geq k$. So we obtain the equations

$$\sum_{j=0}^{i} \sum_{\ell=1}^{s} a_{\ell,i-j} f_j^{\sigma^{\ell-1}} = -a_{0,i}, \qquad i = 0, 1, \ldots, k-1. \tag{9}$$

Next, we show that the solution set of all $f = (f_0, f_1, \ldots, f_{k-1})$ satisfying (9) is contained in an affine shift of the kernel of a BTT matrix. In what follows, fix an arbitrary $\mathbb{F}_q$-linear bijection $\phi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$. For an element $a \in \mathbb{F}_{q^m}$, let $\bar{a} := \phi(a) \in \mathbb{F}_q^m$, and for a vector $\mathbf{f} = (f_0, f_1, \ldots, f_{k-1}) \in (\mathbb{F}_{q^m})^k$, let $\bar{\mathbf{f}} := (\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{k-1}) \in \mathbb{F}_q^{mk}$.

Claim 4.5. *Let S be the set of all vectors $f = (f_0, f_1, \ldots, f_{k-1}) \in (\mathbb{F}_{q^m})^k$ satisfying that*

$$\sum_{j=0}^{i} \sum_{\ell=1}^{s} a_{\ell,i-j} f_j^{\sigma^{\ell-1}} = 0, \qquad i = 0, 1, \ldots, k-1, \tag{10}$$

where $a_{\ell,i-j} \in \mathbb{F}_{q^m}$, and $a_{\ell,0} \neq 0$ for some $\ell \in [s]$. Let $\bar{S} := \{\bar{f} \mid f \in S\} \subseteq \mathbb{F}_q^{mk}$. Then $\bar{S} \subseteq \ker(M)$ for a (k, r, m)-BTT matrix M over $\mathbb{F}_q$ with $m - s + 1 \leq r \leq m$. Moreover, M can be constructed in time $\mathrm{poly}(\log q, m, n)$.

Proof. First note that both the multiplication map $m_b : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, given by $a \mapsto b \cdot a$ for $a, b \in \mathbb{F}_{q^m}$, and the Frobenius automorphism $\sigma : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, given by $a \mapsto a^q$ for $a \in \mathbb{F}_{q^m}$, are $\mathbb{F}_q$-linear operations over $\mathbb{F}_{q^m}$. Consequently, for all $i = 0, 1, \ldots, k-1$, there exists an $m \times m$ matrix M_i over $\mathbb{F}_q$ so that $\sum_{\ell=1}^{s} a_{\ell,i} \cdot b^{\sigma^{\ell-1}} = M_i \cdot \bar{b}$ for every $b \in \mathbb{F}_{q^m}$. In this notation, we can rewrite (10) as $M \cdot \bar{f} = 0$, where

$$M = \begin{pmatrix} M_0 & 0 & 0 & \cdots & 0 \\ M_1 & M_0 & 0 & \cdots & 0 \\ M_2 & M_1 & M_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_{k-1} & M_{k-2} & M_{k-3} & \cdots & M_0 \end{pmatrix}.$$

Then we have that M is a block lower-triangular Toeplitz matrix with blocks of size $m \times m$. To obtain a BTT matrix, we need to further ensure that all matrices M_0 have full rank. For this, we let $r := \mathrm{rank}(M_0)$, and choose a subset B of r linearly independent rows of M_0. Then in the matrix M, we only keep the rows whose projection on the block M_0 belongs to B. This clearly gives a (k, r, m)-BTT matrix M so that $\bar{S} \subseteq \ker(M)$. Moreover, M can clearly be constructed in time $\mathrm{poly}(\log q, m, n)$. To conclude the proof of the claim, it remains to show that $r = \mathrm{rank}(M_0) \geq m - s + 1$.

To see that $\mathrm{rank}(M_0) \geq m - s + 1$, we show that $\dim(\ker(M_0)) \leq s - 1$. Recall that M_0 represents the $\mathbb{F}_q$-linear map $b \mapsto \sum_{\ell=1}^{s} a_{\ell,0} \cdot b^{\sigma^{\ell-1}}$ for $b \in \mathbb{F}_{q^m}$. Recalling our assumption that $a_{\ell,0} \neq 0$ for some $\ell \in [s]$, we know that $B(x) := \sum_{\ell=1}^{s} a_{\ell,0} \cdot x^{\sigma^{\ell-1}}$ is a nonzero polynomial of degree at most q^{s-1} over $\mathbb{F}_{q^m}$, and consequently, it has at most q^{s-1} zeros in $\mathbb{F}_{q^m}$. Since the map $B(x)$ is $\mathbb{F}_q$-linear, we conclude that the kernel is an $\mathbb{F}_q$-linear subspace of dimension at most $s - 1$, and so $\dim(\ker(M_0)) \leq s - 1$. □

By (9) and Claim 4.5 above, we have that all polynomials $f = (f_0, f_1, \ldots, f_{k-1})$ that agree with $\mathbf{y}$ on at least t points are contained in an affine shift of the kernel of a (k, r, m)-BTT matrix over $\mathbb{F}_q$ for $r \geq m - s + 1$. In the next section, we prove that the kernel of a (k, r, m)-BTT matrix is a $(k, m, m - r)$-BTT subspace. Finally, noting that in our setting $m - r \leq s - 1$, and that a basis for the kernel of M, as well as the desired affine shift (which is any valid solution to (9)), can be found in time $\mathrm{poly}(\log q, m, n)$, concludes the proof of Lemma 4.3.

4.3 The kernel of a BTT matrix is a BTT subspace

In this section, we prove the following lemma.

Lemma 4.6. *Suppose that M is a (k, r, m)-BTT matrix over $\mathbb{F}_q$, where $r \leq m$. Then $\ker(M)$ is a $(k, m, m - r)$-BTT subspace over $\mathbb{F}_q$.*

To prove the above lemma, let $V := \ker(M)$, where

$$M = \begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 \\ M_2 & M_1 & 0 & \cdots & 0 \\ M_3 & M_2 & M_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_k & M_{k-1} & M_{k-2} & \cdots & M_1 \end{pmatrix}$$

is a (k, r, m)-BTT matrix. Our goal is to show that V is a $(k, m, m-r)$-BTT subspace, and for this we need to exhibit a $(k, m, m-r)$-BTT matrix $\tilde{M}$ so that $V = \mathrm{Image}(\tilde{M})$.

We start by introducing some notation. We write a vector $v \in \mathbb{F}_q^{km}$ as $v = (v_1, v_2, \ldots, v_k)$ where $v_i \in \mathbb{F}_q^m$. For $i = 0, 1, \ldots, k$, we let

$$V_i = \{(v_1, v_2, \ldots, v_k) \in V \mid v_1 = v_2 = \cdots = v_i = 0\}.$$

In particular, we have $V_0 = V$ and $V_k = \{0\}$. Finally, define $\sigma : \mathbb{F}_q^{km} \to \mathbb{F}_q^{km}$ by

$$\sigma(v_1, v_2, \ldots, v_k) = (0, v_1, v_2, \ldots, v_{k-1}).$$

Claim 4.7. *For all $i = 1, \ldots, k$, $\sigma(V_{i-1}) \subseteq V_i \subseteq V_{i-1}$.*

Proof. The right-hand containment clearly holds by the definition of V_i. To see that the left-hand containment holds, let $v = (v_1, \ldots, v_k) \in V_{i-1}$, and let $u = \sigma(v) = (0, v_1, \ldots, v_{k-1})$. Our goal is to show that $u \in V_i$. First note that since $v \in V_{i-1}$, we have that $v_1 = \cdots = v_{i-1} = 0$, and so $u = (u_1, \ldots, u_k)$ satisfies that $u_1 = \cdots = u_i = 0$. Thus to show that $u \in V_i$, it remains to show that $u \in V$, or equivalently that $M \cdot u = 0$.

To this end, note that by the structure of M,

$$M \cdot u = \begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 \\ M_2 & M_1 & 0 & \cdots & 0 \\ M_3 & M_2 & M_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_k & M_{k-1} & M_{k-2} & \cdots & M_1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ v_1 \\ \vdots \\ v_{k-1} \end{pmatrix} = \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ M_2 & M_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ M_{k-1} & M_{k-2} & \cdots & M_1 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_{k-1} \end{pmatrix} = 0,$$

where the last equality follows since $v \in V$, and so

$$M \cdot v = \begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 \\ M_2 & M_1 & 0 & \cdots & 0 \\ M_3 & M_2 & M_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_k & M_{k-1} & M_{k-2} & \cdots & M_1 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = 0.$$

$\square$

We also note the following claim which follows by counting the number of linearly-independent constraints defining V_i.

Claim 4.8. *For all $i = 0, 1, \ldots, k$, $\dim(V_i) = (k-i)(m-r)$. In particular, $\dim(V_{i-1}) = \dim(V_i) + (m-r)$ for all $i = 1, \ldots, k$.*

The above two claims imply the following.

Claim 4.9. *The following holds for all* $i = 1, \ldots, k-1$. *Suppose that* $b^{(1)}, \ldots, b^{(m-r)}$ *are* $m-r$ *linearly independent vectors in* $\mathbb{F}_q^{km}$ *so that*

$$V_{i-1} = V_i + \mathrm{span}\{b^{(1)}, \ldots, b^{(m-r)}\}. \tag{11}$$

Then

$$V_i = V_{i+1} + \mathrm{span}\left\{\sigma(b^{(1)}), \ldots, \sigma(b^{(m-r)})\right\}. \tag{12}$$

Proof. First note that by our assumption (11), we have that $b^{(1)}, \ldots, b^{(m-r)}$ are contained in V_{i-1}. By Claim 4.7, this implies in turn that $\sigma(b^{(1)}), \ldots, \sigma(b^{(m-r)}) \in V_i$ and $V_{i+1} \subseteq V_i$, and consequently we have that the right-hand side of (12) is contained in the left-hand side.

To see the containment in the other direction, recall that by Claim 4.8, $\dim(V_i) - \dim(V_{i+1}) = m-r$, and so it suffices to show that there is no non-trivial linear combination of $\sigma(b^{(1)}), \ldots, \sigma(b^{(m-r)})$ that belongs to V_{i+1}. Suppose in contradiction that there exists a non-trivial linear combination $a := \alpha_1 \cdot \sigma(b^{(1)}) + \cdots + \alpha_{m-r} \cdot \sigma(b^{(m-r)}) \in V_{i+1}$. By the definition of V_{i+1}, this implies in turn that $a_{i+1} = 0$. But in this case, the non-trivial linear combination $a' := \alpha_1 \cdot b^{(1)} + \cdots + \alpha_{m-r} \cdot b^{(m-r)}$ satisfies that $a'_i = 0$. Consequently, we have that $a' \in V_i$, contradicting our assumption (11). $\square$

Now we prove Lemma 4.6 using the above claim.

Proof of Lemma 4.6. Recall that our goal is to exhibit a $(k, m, m-r)$-BTT matrix $\tilde{M}$ so that $V = \mathrm{Image}(\tilde{M})$. We construct $\tilde{M}$ as follows. Since $\dim(V_0) = \dim(V_1) + (m-r)$, there exist $m-r$ linearly independent vectors $b^{(1)}, \ldots, b^{(m-r)} \in \mathbb{F}_q^{km}$ so that $V_0 = V_1 + \mathrm{span}\{b^{(1)}, \ldots, b^{(m-r)}\}$. For $i = 1, \ldots, k$, let M_i be a $(km) \times (m-r)$ matrix whose columns are $\sigma^{(i-1)}(b^{(1)}), \ldots, \sigma^{(i-1)}(b^{(m-r)})$. Let

$$\tilde{M} = \begin{pmatrix} M_1 & M_2 & \cdots & M_k \end{pmatrix}.$$

Then we clearly have that $\tilde{M}$ is a $(k, m, m-r)$-BTT matrix. Moreover, by Claim 4.9 we further have that $V_{i-1} = V_i + \mathrm{Image}(M_i)$ for all $i = 1, \ldots k$, and so $V = V_0 = \mathrm{Image}(\tilde{M})$. This concludes the proof of Lemma 4.6. $\square$

5 Preliminaries on function fields and algebraic-geometric codes

We first give preliminaries and notations about function fields and algebraic-geometric codes. The reader may refer to, e.g., [Sti09] for detailed background.

Function fields. Let $\mathbb{F}_q$ be a finite field. An extension field F of $\mathbb{F}_q$ is called a *function field in one variable* or simply a *function field* over $\mathbb{F}_q$ if F is a finite extension of $\mathbb{F}_q(x)$ for some element $x \in F$ that is transcendental over $\mathbb{F}_q$. The *field of constants* of F is the algebraic closure of $\mathbb{F}_q$ in F.

In the rest of this section, let F be a function field over $\mathbb{F}_q$ such that its field of constants is $\mathbb{F}_q$, i.e, the algebraic closure of $\mathbb{F}_q$ in F is $\mathbb{F}_q$ itself.

Discrete valuations and places. A (normalized) *discrete valuation* of F is a map $v : F \to \mathbb{Z} \cup \{+\infty\}$ with the following properties:

- $v(a) = +\infty$ iff $a = 0$.
- $v(ab) = v(a) + v(b)$ for $a, b \in F$.
- $v(a + b) \geq \min\{v(a), v(b)\}$ for $a, b \in F$.
- $v(F^\times) = \mathbb{Z}$.

For a discrete valuation v of F, we associate a pair $P = (\mathcal{O}_v, \mathfrak{m}_v)$ where $\mathcal{O}_v$ is the ring $\{a \in F : v(a) \geq 0\}$ and $\mathfrak{m}_v$ is the ideal $\{a \in \mathcal{O}_v : v(a) > 0\}$ of $\mathcal{O}_v$. Call P a *place* of F.[8] Denote by $\mathbb{P}(F)$ the set of all places of F, i.e.,

$$\mathbb{P}(F) := \{(\mathcal{O}_v, \mathfrak{m}_v) : v \text{ is a discrete valuation of } F\}.$$

We may recover the discrete valuation v from a place $P = (\mathcal{O}, \mathfrak{m})$ as follows. Let $v(0) = +\infty$. For $0 \neq a \in \mathcal{O}$, $v(a)$ is the largest $k \in \mathbb{N}$ such that $a \in \mathfrak{m}^k$, where we let $\mathfrak{m}^0 = \mathcal{O}$. For $a \in F^\times \setminus \mathcal{O}$, let $v(a) = -v(a^{-1})$. This gives a one-to-one correspondence between the set $\mathbb{P}(F)$ of all places of F and the set of all discrete valuations of F. For a place $P \in \mathbb{P}(F)$, denote by v_P the discrete valuation corresponding to P.

Intuitively, $v_P(f)$ indicates the order of zeros or poles of a function $f \in F$ at the place P: If $v_P(f) \geq 0$, then $v_P(f)$ is the order of zeros of $f \in F$ at P. Otherwise $-v_P(f)$ is the order of poles of f at P.

It can be shown that for a place $P = (\mathcal{O}, \mathfrak{m})$ of F, the quotient ring $\kappa_P := \mathcal{O}/\mathfrak{m}$ is a finite field extension of $\mathbb{F}_q$, called the *residue class field* or *residue field* of P. If $[\kappa_P : \mathbb{F}_q] = 1$, we say the place P is $\mathbb{F}_q$-*rational* or simply *rational*. In this case, we identify $\mathbb{F}_q$ with κ_P via the field isomorphism $\mathbb{F}_q \to \kappa_P$ sending $a \in \mathbb{F}_q$ to $a + \mathfrak{m}$.

For $f \in \mathcal{O}$ and a rational place P of F, define

$$f(P) := f + \mathfrak{m} \in \kappa_P$$

which we view as an element of $\mathbb{F}_q$ by identifying $\mathbb{F}_q$ with κ_P as above.

Local power series and Laurent series expansion. Let $P = (\mathcal{O}, \mathfrak{m})$ be a rational place of F. An element $u \in \mathcal{O}$ is called a *uniformizing parameter* or *uniformizer* of P if $v_P(u) = 1$, or equivalently, u generates the ideal $\mathfrak{m}$.

Fix $u \in \mathcal{O}$ to be a uniformizer of P. We may write any $f \in \mathcal{O}$ as a *power series* in u over $\mathbb{F}_q$

$$f = c_0 + c_1 u + c_2 u^2 + \cdots$$

where the coefficients $c_i \in \mathbb{F}_q$ may be found as follows: Let $f_0 = f$. For $i = 0, 1, 2, \ldots$, let $c_i = f_i(P)$ and let $f_{i+1} = (f_i - c_i)/u \in \mathcal{O}$.

A *Laurent series* is a generalization of a power series, where we allow finitely many terms of negative degree. Generalizing the above representation by power series, we may write any element of F as a Laurent series in u over $\mathbb{F}_q$. Namely, for $f \in F^\times$, let $e = v_P(f)$ and $f^* = f/u^e \in \mathcal{O}$. Suppose $f^* = c_0 + c_1 u + c_2 u^2 + \cdots$. Then

$$f = u^e f^* = c_0 u^e + c_1 u^{e+1} + c_2 u^{e+2} + \cdots .$$

[8]It is common in the literature to define a place to be just the ideal $\mathfrak{m}_v$ associated with a discrete valuation v instead of $(\mathcal{O}_v, \mathfrak{m}_v)$ (see, e.g., [Sti09]). This is equivalent to our definition since $\mathcal{O}_v$ is determined by $\mathfrak{m}_v$ via $\mathcal{O}_v = \{a \in F^\times : a^{-1} \notin \mathfrak{m}_v\} \cup \{0\}$.

Thus, for a rational place $P = (\mathcal{O}, \mathfrak{m})$ and a uniformizer u of P, we have a local expansion of every element of $\mathcal{O}$ or F as a power series or a Laurent series in u over $\mathbb{F}_q$, respectively.

Divisors. A *divisor* of F is a formal sum $\sum_P n_P P$ of finitely many places $P \in \mathbb{P}(F)$, where $n_P \in \mathbb{Z}$. The set of all divisors of F forms an abelian group $\mathrm{Div}(F)$, called the *divisor group* of F.

The *degree* of a divisor $D = \sum_P n_P P$ is $\deg(D) := \sum_P n_P[\kappa_P : \mathbb{F}_q]$. The *support* of D, denoted by $\mathrm{Supp}(D)$, is the set of places P for which $n_P \neq 0$. If $n_P \geq 0$ for all $P \in \mathrm{Supp}(D)$, we write $D \geq 0$ and call D an *effective divisor*. Note that $D \geq 0$ implies $\deg(D) \geq 0$. Let $\mathrm{Div}_0(F) := \{D \in \mathrm{Div}(F) : \deg(D) = 0\}$, which is a subgroup of $\mathrm{Div}(F)$.

Let $f \in F^\times$. It can be shown that $v_P(f) = 0$ holds for all but finitely many places $P \in \mathbb{P}(F)$. So $\mathrm{div}(f) := \sum_{P\in\mathbb{P}(F)} v_P(f)P$ is a well-defined divisor. Divisors of the form $\mathrm{div}(f)$ are called *principal divisors* of F. The degree of a principal divisor is always zero, i.e., $\mathrm{div}(f) \in \mathrm{Div}_0(F)$ for $f \in F^\times$.

Riemann–Roch spaces. For a divisor D of F, the *Riemann–Roch space* associated with D is

$$L(D) := \{f \in F^\times : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

which is a finite-dimensional vector space over $\mathbb{F}_q$. Let $\ell(D) := \dim_{\mathbb{F}_q} L(D)$.

By definition, for $D = \sum_P n_P P$, the condition $\mathrm{div}(f) + D \geq 0$ is equivalent to $v_P(f) \geq -n_P$ for $P \in \mathbb{P}(F)$. So $L(D)$ is the space of functions in F whose prescribed zeros and allowed poles are specified by D: At a place P, if $n_P < 0$, then any $f \in L(D)$ must have a zero of order at least $-n_P$ at P. On the other hand, if $n_P \geq 0$, then $f \in L(D)$ is allowed to have a pole of order at most n_P at P.

Note that if $L(D)$ contains a nonzero element f, then $\mathrm{div}(f) + D \geq 0$, which implies

$$\deg(D) = \deg(\mathrm{div}(f)) + \deg(D) = \deg(\mathrm{div}(f) + D) \geq 0.$$

So for any divisor D with $\deg(D) < 0$, we have $L(D) = \{0\}$ and $\ell(D) = 0$.

The Riemann–Roch theorem. The *Riemann–Roch theorem* states that

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1$$

holds for any divisor D of F, where K is a certain divisor of F called a *canonical divisor*, and g is a nonnegative integer depending only on F called the *genus* of F.

In fact, we only need the following corollary of the Riemann–Roch theorem.

Theorem 5.1 (Riemann's inequality)**.** $\ell(D) \geq \deg(D) - g + 1$.

Algebraic-geometric codes. Let D be a divisor of F and let $S = \{P_1, P_2, \ldots, P_n\}$ be a set of n distinct rational places of F such that $\mathrm{Supp}(D) \cap S = \emptyset$. Define the *algebraic-geometric (*AG*) code*

$$C(S, D) := \{(f(P_1), f(P_2), \ldots, f(P_n)) : f \in L(D)\} \subseteq \mathbb{F}_q^n, \tag{13}$$

which is an $\mathbb{F}_q$-linear code of block length n.

Let $D_S = \sum_{P\in S} P \in \mathrm{Div}(F)$. We have the following theorem.

Theorem 5.2 ([Sti09, Theorem 2.2.2])**.** *The dimension of $C(S, D)$ is $\ell(D) - \ell(D - D_S)$, which equals $\ell(D)$ if $\deg(D) < \deg(D_S) = n$. The minimum distance of $C(S, D)$ is at least $n - \deg(D)$.*

5.1 Constant field extensions of function fields

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a finite field extension of degree $m \in \mathbb{N}^+$. Denote by $F^{(m)}$ the compositum $F\mathbb{F}_{q^m}$ of F and $\mathbb{F}_{q^m}$. Then $F^{(m)}$ is a function field over $\mathbb{F}_{q^m}$. Recall that we assume the field of constants of F is $\mathbb{F}_q$. This implies that the field of constants of $F^{(m)}$ is $\mathbb{F}_{q^m}$ [Sti09, Proposition 3.6.1].

Places and divisors of $F^{(m)}$. Let $P = (\mathcal{O}, \mathfrak{m})$ be a *rational* place of F and v_P the corresponding discrete valuation of F. It can be shown that there exists a *unique* discrete valuation v'_P of $F^{(m)}$ that extends v_P. We denote the corresponding place of $F^{(m)}$ by $P^{(m)} = (\mathcal{O}^{(m)}, \mathfrak{m}^{(m)})$, which is an $\mathbb{F}_{q^m}$-rational place. As v'_P extends v_P, we have $\mathcal{O} \subseteq \mathcal{O}^{(m)}$ and $\mathfrak{m} \subseteq \mathfrak{m}^{(m)}$. So $f(P^{(m)}) = f(P)$ for any $f \in \mathcal{O} \subseteq \mathcal{O}^{(m)}$. And a uniformizer $u \in \mathfrak{m}$ of P is also a uniformizer of $P^{(m)}$.

Let $D = \sum_P n_P P$ be a divisor of F such that every $P \in \mathrm{Supp}(D)$ is rational. Then we define

$$D^{(m)} := \sum_{P \in \mathrm{Supp}(D)} n_P P^{(m)},$$

which is a divisor of $F^{(m)}$. The Riemann-Roch space $L(D^{(m)})$ and its dimension $\ell(D^{(m)})$ are defined as before, except that the base field is changed to $\mathbb{F}_{q^m}$. That is,

$$L(D^{(m)}) = \{f \in (F^{(m)})^\times : \mathrm{div}(f) + D^{(m)} \geq 0\} \cup \{0\}$$

and $\ell(D^{(m)}) = \dim_{\mathbb{F}_{q^m}} L(D^{(m)})$.

The following lemma is a special case of [Sti09, Theorem 3.6.3 (d)].

Lemma 5.3. *Let D be as above. If $f_1, \ldots, f_k \in F$ form a basis of $L(D)$ over $\mathbb{F}_q$, then they form a basis of $L(D^{(m)})$ over $\mathbb{F}_{q^m}$. In particular, $\ell(D^{(m)}) = \ell(D)$.*

Remark 2. We only need the definition of $D^{(m)}$ for the special case that every $P \in \mathrm{Supp}(D)$ is rational, but it can also be defined for a general divisor D. See [Sti09, Definition 3.1.8] for the general definition, where it is called the *conorm* of D and denoted by $\mathrm{Con}_{F^{(m)}/F}(D)$.

We also note that $P^{(m)}$ and $D^{(m)}$ above are simply denoted by P and D respectively in [GX13] by a slight abuse of notation.

The Frobenius automorphism. Let σ be the Frobenius automorphism $a \mapsto a^q$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. As $\mathbb{F}_q$ is the field of constants of F, we have $F \cap \mathbb{F}_{q^m} = \mathbb{F}_q$. This implies that $\mathrm{Gal}(F^{(m)}/F)$ is isomorphic to $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ via the restriction map $\tau \mapsto \tau|_{\mathbb{F}_{q^m}}$ (see [Lan02, Theorem 1.12]). So $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ uniquely extends to an automorphism of $F^{(m)}$ that fixes F, which we also call σ by an abuse of notation.

As σ is an automorphism of $F^{(m)}$, it permutes the places of $F^{(m)}$. Let P be any rational place of F. As σ fixes F, it also fixes P. So σ also fixes $P^{(m)}$.

5.2 The Garcia–Stichtenoth tower

We need the following tower of function fields introduced by Garcia and Stichtenoth in [GS96].

Definition 5.4 (Garcia–Stichtenoth tower [GS96])**.** *Let $r > 1$ be a prime power and $q = r^2$. For $i = 1, 2, \ldots,$ let $K_i = \mathbb{F}_q(x_1, x_2, \ldots, x_i)$, where x_1 is transcendental over $\mathbb{F}_q$ and x_i satisfies the following recursive equation for $i > 1$.*

$$x_i^r + x_i = \frac{x_{i-1}^r}{x_{i-1}^{r-1} + 1}.$$

The Garcia–Stichtenoth tower *over* $\mathbb{F}_q$ *is the infinite tower of function fields* $K_1 \subseteq K_2 \subseteq \cdots$.

For each $e \in \mathbb{N}^+$, we have $[K_e : K_1] = r^{e-1}$ and the field of constants of K_e is $\mathbb{F}_q$.

Rational places. Let $e \in \mathbb{N}^+$. The field K_e has at least $r^e(r-1)+1$ rational places. One of them is the place P_∞ "at the infinity," which is totally ramified over K_1 and is the unique pole of x_1, i.e., $v_{P_\infty}(x_1) = -[K_e : K_1] = -r^{e-1}$. More generally, we have $v_{P_\infty}(x_i) = -r^{e-i}$ for $i \in [e]$. In particular, $v_{P_\infty}(x_e) = -1$ and hence x_e^{-1} is a uniformizer of P_∞.

In addition, define S_e to be the set of all tuples $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_e) \in \mathbb{F}_q^e$ such that $\alpha_1^r + \alpha_1 \neq 0$ and $\alpha_i^r + \alpha_i = \frac{\alpha_{i-1}^r}{\alpha_{i-1}^{r-1}+1}$ for $i = 2, 3, \ldots, e$. For each $\alpha \in S_e$, there exists a corresponding rational place P_α of K_e. It is the unique rational place P satisfying $v_P(x_i) \geq 0$ and $x_i(P) = \alpha_i$ for $i = 1, 2, \ldots, e$.

There are precisely $r^e(r-1)$ elements in S_e, corresponding to $r^e(r-1)$ rational places P_α of K_e.

Genus. For $e \in \mathbb{N}^+$, the genus $g(K_e)$ of K_e is given by

$$g(K_e) = \begin{cases} (r^{e/2}-1)^2 & e \text{ is even,} \\ (r^{(e-1)/2}-1)(r^{(e+1)/2}-1) & e \text{ is odd.} \end{cases}$$

In particular, we have $g(K_e) \leq r^e$.

Explicitness. To construct AG codes using the Garcia–Stichtenoth tower, we need to construct bases for Riemann–Roch spaces of K_e. An efficient algorithm of computing such bases was given in [SAK+01] for one-point divisors kP_∞.

Theorem 5.5 ([SAK+01])**.** *For $k \in \mathbb{N}$ and $e \in \mathbb{N}^+$, a basis B of the Riemann–Roch space $L(kP_\infty)$ of K_e over $\mathbb{F}_q = \mathbb{F}_{r^2}$ can be found in time* $\mathrm{poly}(k, r^e)$*. Moreover, given $\alpha \in S_e$ and $f \in L(kP_\infty)$ (represented in the basis B), the evaluation $f(P_\alpha)$ can also be found in time* $\mathrm{poly}(k, r^e)$.

In addition, it was shown in [GX12] that the Laurent series expansion of $f \in L(kP_\infty)$ at the place P_∞ in the uniformizer x_e^{-1} can be computed efficiently.

Lemma 5.6 ([GX12])**.** *Given $f \in L(kP_\infty)$ and $N \in \mathbb{N}^+$, the first N coefficients $c_0, c_1, \ldots, c_{N-1} \in \mathbb{F}_q$ of the Laurent series expansion*

$$f = c_0 T^{-k} + c_1 T^{-k+1} + c_2 T^{-k+2} + \cdots$$

at the place P_∞ in the uniformizer $T = x_e^{-1}$ can be found in time $\mathrm{poly}(k, r^e, N)$.

6 Algebraic-geometric codes with subfield evaluation points

In this section, we present the proof of Theorem 2.3, which is restated below.

Theorem 2.3 (Output list contained in a BTT subspace)**.** *There exists an absolute constant $c > 1$ so that the following holds for any $R \in (0,1)$, $\epsilon > 0$, $q \geq 1/\epsilon^c$ that is an even power of a prime, and $m \geq 1/\epsilon^2$. There is an infinite family of error-correcting codes $\{C_n\}_n$, where C_n satisfies the following properties:*

1. *$C_n : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^n$ is a linear code of rate at least R that can be encoded in time* $\mathrm{poly}(\log q, m, n)$.

2. *There exists an injective $\mathbb{F}_q$-linear map $\phi : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^{\hat{k}}$, where $\hat{k} \le n$, so that C_n can be list decoded from a $(1 - R - \epsilon)$-fraction of errors, pinning down the images of the candidate messages under ϕ (viewed as length $\hat{k}m$ vectors over $\mathbb{F}_q$) to an affine shift of a $(\hat{k}, m, \epsilon m)$-BTT subspace V over $\mathbb{F}_q$. Moreover, the map ϕ, a basis for V, and the affine shift can be computed in time $\mathrm{poly}(\log q, m, n)$.*

It is based on AG codes with subfield evaluation points and closely follows [GX13]. Specifically, we use the Garcia–Stichtenoth tower of function fields discussed in Subsection 5.2. We note that this framework is generic and can be adapted to work for other families of function fields as well. For more details, see Remark 3 at the end of this section.

Our construction is given below as Definition 6.1. It uses the constant field extension $K_e^{(m)}$ of K_e, where K_e is the eth field in the Garcia–Stichtenoth tower over $\mathbb{F}_q = \mathbb{F}_{r^2}$. Recall that K_e has a rational place P_∞ and $r^e(r-1)$ rational places P_α for $\alpha \in S_e$. And for each rational place P of K_e, there is a corresponding $\mathbb{F}_{q^m}$-rational place $P^{(m)}$ of $K_e^{(m)}$.

Definition 6.1 (AG codes with subfield evaluation points from the Garcia–Stichtenoth tower)**.** *Let $r > 1$ be a prime power and $q = r^2$. Let $n, k, m, e \in \mathbb{N}^+$ be such that $k \le n$ and $n \le r^e(r-1)$. Let $\alpha_1, \dots, \alpha_n \in S_e \subseteq \mathbb{F}_q^e$ be distinct and let $P_i = P_{\alpha_i}^{(m)}$ for $i \in [n]$. The code* $\mathsf{GS}_{q,m,e}(n,k)$ over $\mathbb{F}_{q^m}$ with evaluation points $P_1, \dots, P_n$ *maps $f \in L((k-1)P_\infty^{(m)}) \subseteq K_e^{(m)}$ to the codeword $C_f := (f(P_1), f(P_2), \dots, f(P_n)) \in (\mathbb{F}_{q^m})^n$.*

Explicitness. By Theorem 5.5, a basis B of $L((k-1)P_\infty)$ over $\mathbb{F}_q$ can be computed in time $\mathrm{poly}(k, r^e) = \mathrm{poly}(r^e)$. Suppose $B = \{\beta_1, \beta_2, \dots, \beta_b\}$, where $b = \ell((k-1)P_\infty)$. By Lemma 5.3, B is also a basis of $L((k-1)P_\infty^{(m)})$ over $\mathbb{F}_{q^m}$. So we may write $f \in L((k-1)P_\infty^{(m)})$ uniquely as a linear combination of β_i over $\mathbb{F}_{q^m}$:

$$f = \sum_{i=1}^{b} c_i \beta_i, \quad \text{where } c_i \in \mathbb{F}_{q^m}. \tag{14}$$

We represent f by the coefficients $c_1, \dots, c_b$ in the basis B. Note

$$f(P^{(m)}) = \left(\sum_{i=1}^{b} c_i \beta_i\right)(P^{(m)}) = \sum_{i=1}^{b} c_i \beta_i(P)$$

for any rational place P of K_e. So by Theorem 5.5, the encoding map $\mathsf{Enc} : L((k-1)P_\infty^{(m)}) \to (\mathbb{F}_{q^m})^n$ sending f to $C_f = (f(P_1), f(P_2), \dots, f(P_n))$ can be computed in time $\mathrm{poly}(k, r^e, n, m \log q) = \mathrm{poly}(r^e, m)$.

Rate and minimum distance. Denote by g the genus of K_e. The following theorem bounds the rate and the minimum distance of the code $\mathsf{GS}_{q,m,e}(n,k)$.

Theorem 6.2. $\mathsf{GS}_{q,m,e}(n,k)$ *is a linear code over the alphabet $\mathbb{F}_{q^m}$ with block length n. Its rate is at least $(k-g)/n$ and its minimum distance is at least $n-k+1$.*

Proof. Let $S = \{P_1, \dots, P_n\}$ and $D = (k-1)P_\infty^{(m)}$. Then $\mathsf{GS}_{q,m,e}(n,k)$ is simply the linear code $C(S,D)$ defined in (13) with the base field replaced by $\mathbb{F}_{q^m}$. By Theorem 5.2, its dimension is $\ell((k-1)P_\infty^{(m)})$ and its minimum distance is at least $n - \deg((k-1)P_\infty^{(m)}) = n-k+1$. By Lemma 5.3 and Riemann's inequality (Theorem 5.1), we have $\ell((k-1)P_\infty^{(m)}) = \ell((k-1)P_\infty) \ge k-g$. So the rate of $\mathsf{GS}_{q,m,e}(n,k)$ is at least $(k-g)/n$. $\square$

The embedding ϕ. To list-decode the code $\mathsf{GS}_{q,m,e}(n,k)$, we need an embedding (i.e., injective linear map)

$$\phi : L((k-1)P_\infty^{(m)}) \to \mathbb{F}_{q^m}^k.$$

It is defined to be the $\mathbb{F}_{q^m}$-linear map that outputs the first k coefficients of the Laurent series expansion at the place $P_\infty^{(m)}$ in the uniformizer $T := x_e^{-1}$. That is, if the Laurent series expansion of $f \in L((k-1)P_\infty^{(m)})$ at $P_\infty^{(m)}$ in T is

$$f = f_0 T^{-(k-1)} + f_1 T^{-(k-1)+1} + f_2 T^{-(k-1)+2} + \cdots,$$

with the coefficients $f_i \in \mathbb{F}_{q^m}$, then $\phi(f) = (f_0, f_1, \ldots, f_{k-1})$.

The kernel of ϕ is $L(-P_\infty^{(m)}) = \{0\}$. So ϕ is indeed an embedding. Representing a function $f \in L((k-1)P_\infty^{(m)})$ in the form (14), we can compute $\phi(f)$ from f in time $\mathrm{poly}(r^e, m)$ by Lemma 5.6.

List decoding. Next, we show that for properly chosen parameters, the code $\mathsf{GS}_{q,m,e}(n,k)$ is list decodable up to the relative distance $1-R-\epsilon$ and that the image of the output list under the embedding ϕ is contained in an affine shift of a low-dimensional BTT subspace.

Theorem 6.3. *Let $\epsilon > 0$ and $R \in (0, 1-\epsilon)$. Let $e \in \mathbb{N}^+$ be a growing parameter. Let $r \geq 4/\epsilon + 1$ be a prime power and $q = r^2$. Choose $n, m, k \in \mathbb{N}^+$ such that $m \geq 4/\epsilon^2$, $4r^e/\epsilon \leq n \leq (r-1)r^e$ and $k = \lceil Rn + r^e \rceil \leq n$. Then $\mathsf{GS}_{q,m,e}(n,k)$ has rate at least R. And it can be list decoded from up to a $(1-R-\epsilon)$-fraction of errors with a list of candidate messages whose images under ϕ (viewed as length km vectors over $\mathbb{F}_q$) are contained in an affine shift of a $(k, m, \epsilon m)$-BTT subspace V over $\mathbb{F}_q$. Moreover, a basis for V and the affine shift can be found in time $\mathrm{poly}(n, m)$ given the received word.*

The above theorem is a consequence of the following lemma.

Lemma 6.4. *Let $n, k, m, e, r, q \in \mathbb{N}^+$ and $\mathsf{GS}_{q,m,e}(n,k)$ be as in Definition 6.1. Let $s \in [m]$ and $t, d \in \mathbb{N}^+$ be parameters, satisfying that*

$$(s+1)(d-g+1) + k - 1 > n \tag{15}$$

and

$$t > d + k - 1 \tag{16}$$

where g is the genus of K_e. Then $\mathsf{GS}_{q,m,e}(n,k)$ can be list decoded from agreement at least t with a list of candidate messages whose images under ϕ (viewed as length km vectors over $\mathbb{F}_q$) are contained in an affine shift of a $(k, m, s-1)$-BTT subspace V over $\mathbb{F}_q$. Moreover, a basis for V and the affine shift can be found in time $\mathrm{poly}(r^e, m)$.

Before we prove the above lemma, we show how it implies Theorem 6.3.

Proof of Theorem 6.3. We know $g \leq r^e$. So the rate of $\mathsf{GS}_{q,m,e}(n,k)$ is at least $(k-g)/n \geq (k-r^e)/n \geq R$ by Theorem 6.2.

Let $\epsilon' = \epsilon/4$. By assumption, we have $r^e/n \leq \epsilon'$. Let $s = \frac{1}{\epsilon'} + 1$, let $d = \frac{n-k+2}{s+1} + g - 1$ so that (15) is satisfied, and let $t = d + k$ so that (16) is satisfied. Then with this setting of parameters, we know from

Lemma 6.4 that $\mathsf{GS}_{q,m,e}(n,k)$ can be list decoded from agreement t, or equivalently, from up to

$$\begin{aligned} n-t = n-d-k = n-k+1-g-\frac{n-k+2}{s+1} &\geq \left(1-\frac{1}{s+1}\right)(n-k+1)-g-\frac{1}{s+1} \\ &\geq (1-\epsilon')(n-Rn-r^e)-r^e-\epsilon' \\ &\geq (1-R-4\epsilon')n \\ &= (1-R-\epsilon)n \end{aligned}$$

errors. Moreover, as $m \geq 4/\epsilon^2 = 1/(\epsilon\cdot\epsilon')$, we have that V is a $(k,m,s-1)$-BTT subspace for $s-1=\frac{1}{\epsilon'} \leq \epsilon m$. And a basis for V as well as the affine shift can be found in time $\mathrm{poly}(r^e,m)=\mathrm{poly}(n,m)$ by Lemma 6.4. $\square$

Theorem 2.3 follows easily from Theorem 6.3.

Proof of Theorem 2.3. Fix a prime power $r=O(1/\epsilon)$ such that $r \geq 4/\epsilon+1$. Let $q=r^2$ and $m=\lceil 4/\epsilon^2\rceil$. Choose the family of codes to be

$$\{\mathsf{GS}_{q,m,e}(n,k) : e\in\mathbb{N}^+, 4r^e/\epsilon \leq n \leq (r-1)r^e, k=\lceil Rn+r^e\rceil\}.$$

Then Theorem 2.3 follows from Theorem 6.3. $\square$

So it remains to prove Lemma 6.4. We prove this lemma in the next two subsections.

6.1 The polynomial Q

In what follows, let σ be the Frobenius automorphism $a\mapsto a^q$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It uniquely extends to an automorphism of $K_e^{(m)}$ that fixes K_e, which we also call σ by an abuse of notation. The automorphism σ fixes $P^{(m)}$ for any rational place P of K_e. For $f\in K_e^{(m)}$, denote by f^σ the element $\sigma(f)$.

Suppose that $\mathbf{y}=(y_1,y_2,\ldots,y_n)\in(\mathbb{F}_{q^m})^n$ is a received word. We let Q be a nonzero multivariate polynomial in $K_e^{(m)}[Y_1,Y_2,\ldots,Y_s]$ of the form

$$Q = A_0 + A_1Y_1 + A_2Y_2 + \cdots + A_sY_s$$

where $A_0,A_1,\ldots,A_s\in K_e^{(m)}$, $A_0\in L((d+k-1)P_\infty^{(m)})$, and $A_i\in L(dP_\infty^{(m)})$ for $i=1,2,\ldots,s$. We also require the coefficients A_i to satisfy the constraint

$$A_0(P_i)+A_1(P_i)y_i+A_2(P_i)y_i^{\sigma}+\cdots+A_s(P_i)y_i^{\sigma^{s-1}}=0 \tag{17}$$

for all $i=1,\ldots,n$, where $P_1,\ldots,P_n$ are the evaluation points.

We first claim that such a nonzero polynomial Q exists and can be computed efficiently. To see this, write A_0 as a vector over $\mathbb{F}_{q^m}$ with $\ell((d+k-1)P_\infty^{(m)})$ coordinates, and write A_i as a vector over $\mathbb{F}_{q^m}$ with $\ell(dP_\infty^{(m)})$ coordinates for $i=1,\ldots,n$. Think of the coordinates of these vectors as unknowns. This gives

$$\begin{aligned} \ell((d+k-1)P_\infty^{(m)})+s\cdot\ell(dP_\infty^{(m)}) &\geq (d+k-1)-g+1+s(d-g+1) \\ &= (s+1)(d-g+1)+(k-1) \end{aligned}$$

unknowns in total, where the first inequality above follows from Riemann's inequality (Theorem 5.1). On the other hand, (17) gives n homogeneous linear constraints in these unknowns over $\mathbb{F}_{q^m}$. By (15), the number of unknowns is greater than the number of linear constraints which guarantees the existence of a nonzero solution Q. Moreover, we can find Q in time $\mathrm{poly}(r^e, m)$ by constructing and then solving the system of linear equations represented by (17). (Note d is polynomial in r^e since $d < t$ by (16) and the agreement t is bounded by $n \le (r-1)r^e$.)

Next, we show that Q gives a functional equation that any f that has sufficiently large agreement with the received word $\mathbf{y}$ needs to satisfy.

Claim 6.5. *Let $f \in L((k-1)P_\infty^{(m)})$. Suppose $\mathbf{y}$ agrees with the codeword $C_f = (f(P_1), f(P_2), \ldots, f(P_n))$ in at least t coordinates. Then f satisfies the functional equation*

$$Q(f, f^\sigma, \ldots, f^{\sigma^{s-1}}) = A_0 + A_1 f + A_2 f^\sigma + \cdots + A_s f^{\sigma^{s-1}} = 0. \tag{18}$$

Proof. Define

$$Q^* = A_0 + A_1 f + A_2 f^\sigma + \cdots + A_s f^{\sigma^{s-1}} \in K_e^{(m)}.$$

We want to prove that $Q^* = 0$. As $f \in L((k-1)P_\infty^{(m)})$, $A_0 \in L((d+k-1)P_\infty^{(m)})$, $A_i \in L(dP_\infty^{(m)})$ for $i = 1, 2, \ldots, s$, and σ fixes $P_\infty^{(m)}$, we know $Q^* \in L((d+k-1)P_\infty^{(m)})$.

Suppose that $\mathbf{y}$ agrees with C_f in the i-th symbol for some $i \in [n]$, i.e., $y_i = f(P_i)$. By (17), we have

$$\begin{aligned}
0 &= A_0(P_i) + A_1(P_i)y_i + A_2(P_i)y_i^\sigma + \cdots + A_s(P_i)y_i^{\sigma^{s-1}} \\
&= A_0(P_i) + A_1(P_i)f(P_i) + A_2(P_i)(f(P_i))^\sigma + \cdots + A_s(P_i)(f(P_i))^{\sigma^{s-1}} \\
&= A_0(P_i) + A_1(P_i)f(P_i) + A_2(P_i)f^\sigma(P_i) + \cdots + A_s(P_i)f^{\sigma^{s-1}}(P_i) \\
&= (A_0 + A_1 f + A_2 f^\sigma + \cdots + A_s f^{\sigma^{s-1}})(P_i) \\
&= Q^*(P_i).
\end{aligned}$$

The third equality uses the fact that $(f(P_i))^\sigma = f^\sigma(P_i)$, which holds since $P_i = P_{\alpha_i}^{(m)}$ is fixed by σ.

As $\mathbf{y}$ and C_f agree in at least t symbols, the above argument shows that there exist $i_1, \ldots, i_t \in [n]$ such that Q^* vanishes at $P_{i_1}, \ldots, P_{i_t}$. Let $D = \sum_{j=1}^t P_{i_j}$. Then $Q^* \in L((d+k-1)P_\infty^{(m)} - D)$. On the other hand, the degree of the divisor $(d+k-1)P_\infty^{(m)} - D$ is $d+k-1-t$, which is less than zero by (16). So $L((d+k-1)P_\infty^{(m)} - D) = \{0\}$. This implies $Q^* = 0$. □

6.2 The BTT subspace V

Next, we show that the functional equation (18), given by Claim 6.5 above, implies that the image of the list of candidate messages under the embedding ϕ is contained in an affine shift of a low-dimensional BTT subspace. We start by expanding the functional equation (18) in terms of the coefficients of the polynomials f and $A_0, A_1, \ldots, A_s$.

Suppose that $f \in L((k-1)P_\infty^{(m)})$ agrees with $\mathbf{y}$ in at least t coordinates. Consider the Laurent series expansion of f at $P_\infty^{(m)}$ in the uniformizer $T = x_e^{-1}$:

$$f = \sum_{i=0}^{\infty} f_i T^{-(k-1)+i}$$

where the coefficients f_i are in $\mathbb{F}_{q^m}$. As $T \in K_e$ is fixed by σ, we have $f^{\sigma^j} = \sum_{i=0}^\infty f_i^{\sigma^j} T^{-(k-1)+i}$ for any integer j. By definition, $\phi(f) = (f_0, f_1, \ldots, f_{k-1})$.

Similarly, expand $A_0 \in L((d+k-1)P_\infty^{(m)})$ and $A_1, \ldots, A_s \in L(dP_\infty^{(m)})$ as Laurent series at $P_\infty^{(m)}$ in the uniformizer T:

$$A_0 = \sum_{i=0}^{\infty} a_{0,i} T^{-(d+k-1)+i} \quad \text{and} \quad A_\ell = \sum_{i=0}^{\infty} a_{\ell,i} T^{-d+i}, \quad \ell = 1, \ldots, s \tag{19}$$

where the coefficients $a_{\ell,i}$ are in $\mathbb{F}_{q^m}$ for $\ell = 0, 1, \ldots, s$ and $i \in \mathbb{N}$. Choose the largest integer $u \geq 0$ such that there exists $\ell_0 \in \{0, 1, \ldots, s\}$ satisfying $a_{\ell_0,u} \neq 0$. By (18), we may assume $\ell_0 \in [s]$. (Otherwise, we have $a_{0,u} \neq 0$ and $a_{1,u} = \cdots = a_{s,u} = 0$. Then the LHS of (18), which we denote by Q^*, satisfies $v_{P_\infty^{(m)}}(Q^*) = -(d-k+1) + u < +\infty$, contradicting (18).) Then we have $0 \neq A_{\ell_0} \in L((d-u)P_\infty^{(m)})$, which implies $u \leq d$.

Let $\hat{a}_{\ell,i} = a_{\ell,i+u}$ for $\ell = 0, 1, \ldots, s$ and $i \in \mathbb{N}$. So $\hat{a}_{\ell_0,0} = a_{\ell_0,u} \neq 0$. We may rewrite (19) as

$$A_0 = \sum_{i=0}^{\infty} \hat{a}_{0,i} T^{-(d+k-1)+u+i} \quad \text{and} \quad A_\ell = \sum_{i=0}^{\infty} \hat{a}_{\ell,i} T^{-d+u+i}, \quad \ell = 1, \ldots, s.$$

With the notations above, (18) becomes

$$\begin{aligned} 0 &= \sum_{i=0}^{\infty} \hat{a}_{0,i} T^{-(d+k-1)+u+i} + \sum_{\ell=1}^{s} \left(\sum_{i=0}^{\infty} \hat{a}_{\ell,i} T^{-d+u+i} \right) \left(\sum_{i=0}^{\infty} f_i^{\sigma^{\ell-1}} T^{-(k-1)+i} \right) \\ &= \sum_{i=0}^{\infty} \left(\hat{a}_{0,i} + \sum_{\ell=1}^{s} \sum_{j=0}^{i} \hat{a}_{\ell,i-j} f_j^{\sigma^{\ell-1}} \right) T^{-(d+k-1)+u+i}. \end{aligned}$$

So we obtain the equations

$$\sum_{j=0}^{i} \sum_{\ell=1}^{s} \hat{a}_{\ell,i-j} f_j^{\sigma^{\ell-1}} = -\hat{a}_{0,i}, \qquad i = 0, 1, \ldots, k-1 \tag{20}$$

where $\hat{a}_{\ell,0} \neq 0$ for some $\ell \in [s]$.

By Claim 4.5, the solution set of all $\phi(f) = (f_0, f_1, \ldots, f_{k-1})$ satisfying (20) is contained in an affine shift of the kernel of a (k, r, m)-BTT matrix M over $\mathbb{F}_q$ for some $r \geq m - s + 1$, and M can be constructed in time $\mathrm{poly}(\log q, m, n)$ given the coefficients $\hat{a}_{\ell,i}$. By Lemma 4.6, the kernel of M is a $(k, m, m-r)$-BTT subspace. It is a subspace of a $(k, m, s-1)$-BTT subspace since $m - r \leq s - 1$.

To compute $\hat{a}_{\ell,i}$ for $\ell = 0, 1, \ldots, s$ and $i = 0, 1, \ldots, k-1$, we first find Q in time $\mathrm{poly}(r^e, m)$, which determines $A_0, A_1, \ldots, A_s$. Then we compute the coefficients $\hat{a}_{\ell,i} = a_{\ell,i+u}$ of the Laurent series of $A_0, A_1, \ldots, A_s$ in time $\mathrm{poly}(r^e, m)$.

Finally, noting that a basis for the kernel of M, as well as the desired affine shift (which is any valid solution to (20)), can be found in time $\mathrm{poly}(r^e, m)$, concludes the proof of Lemma 6.4.

Remarks. We conclude this section with some remarks:

Remark 3. For ease of presentation, we only present the construction from the Garcia–Stichtenoth tower, but this framework is generic and also works for other families of function fields, e.g., the Hermitian tower considered in [She93, GX12]. Besides bounds for the genus and the number of evaluation points, we need the function fields to be explicit in the sense that there should be efficient algorithms for the following subroutines: computing a basis of the Riemann–Roch space $L(D)$ used in the code, evaluating a function $f \in L(D)$ at any evaluation point, and computing the Laurent series expansion of $f \in L(D)$ at a fixed rational place P in a uniformizer that is fixed by the Frobenius automorphism.

In particular, if we replace K_e by the rational function field $\mathbb{F}_q(X)$, choose the divisor D to be $(k-1)P_\infty$ where P_∞ denotes the unique pole of X, and choose the rational place P for Laurent series expansions to be the unique zero of X, then we recover the Reed–Solomon codes with subfield evaluation points that have been discussed in Section 4.

Remark 4. We have defined two $\mathbb{F}_{q^m}$-linear maps, the encoding map $\mathsf{Enc} : L((k-1)P_\infty^{(m)}) \to \mathbb{F}_{q^m}^n$ and the embedding $\phi : L((k-1)P_\infty^{(m)}) \to \mathbb{F}_{q^m}^k$ that outputs the first k coefficients of the Laurent series expansion at $P_\infty^{(m)}$ in x_e^{-1}. See Figure 3. Both of these two maps are efficiently computable.

$$
\begin{tikzcd}
L((k-1)P_\infty^{(m)}) \arrow[r, "\mathsf{Enc}"] \arrow[dr, "\phi"'] & \mathbb{F}_{q^m}^n \\
& \mathbb{F}_{q^m}^k
\end{tikzcd}
$$

Figure 3: The linear maps Enc and ϕ.

As explained in the proof of Theorem 1.1, the final code is defined to be $\mathsf{Enc}(\phi^{-1}(W))$ for some BTT evasive subspace $W \subseteq \mathbb{F}_{q^m}^k$. That is, we restrict the message space to $\phi^{-1}(W)$.

We note that [GX13] used a different idea: In [GX13], the map ϕ was defined on the Riemann-Roch space $L(k'P_\infty^{(m)})$ with $k' = k-1+2g \geq k-1$. This choice of larger k' guarantees that the map $\phi : L(k'P_\infty^{(m)}) \to \mathbb{F}_{q^m}^k$ is surjective (instead of being injective). Then [GX13] chose a subspace $V \subseteq L(k'P_\infty^{(m)})$ such that the restriction of ϕ to V is an isomorphism between V and $\mathbb{F}_{q^m}^k$. In this way, $\mathbb{F}_{q^m}^k$ may be identified with the message space V. This space V was further replaced by an evasive subspace in [GX13] to reduce the list size.

This way of restricting the message space in [GX13] may be used to replace ours. Nevertheless, we feel that our method is somewhat simpler. In particular, we only need Riemann's inequality $\ell(D) \geq \deg(D)-g+1$ in the analysis, while [GX13] uses the fact that $\ell(D) = \deg(D) - g + 1$ when $\deg(D) \geq 2g-1$, which is derived from the full Riemann–Roch theorem.

Acknowledgement. We thank Venkatesan Guruswami for bringing our attention to [GX20].

References

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and intractability of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998.

[BFNW93] László Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Computational Complexity*, 3(4):307–318, 1993.

[BKR10] Eli Ben-Sasson, Swastik Kopparty, and Jaikumar Radhakrishnan. Subspace polynomials and limits to list decoding of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 56(1):113–120, 2010.

[BW87] E. R. Berlekamp and L. Welch. Error correction of algebraic block codes. US Patent Number 4,633,470, 1987.

[CPS99] Jin-Yi Cai, Aduri Pavan, and D. Sivakumar. On the hardness of permanent. In *Proceedings of the 16th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, volume 1563 of *Lecture Notes in Computer Science*, pages 90–99. Springer, 1999.

[DKSS13] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. *SIAM Journal on Computing*, 42(6):2305–2328, 2013.

[DL12] Zeev Dvir and Shachar Lovett. Subspace evasive sets. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC)*, pages 351–358. ACM Press, 2012.

[For66] David Forney. *Concatenated Codes*. M.I.T. Press, Cambridge, MA, USA, 1966.

[GI01] Venkatesan Guruswami and Piotr Indyk. Expander-based constructions of efficiently decodable codes. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 658–667. IEEE Computer Society, 2001.

[GK16] Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016.

[GL89] Oded Goldreich and Leonid A Levin. A hard-core predicate for all one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC)*, pages 25–32. ACM, 1989.

[GQST20] Fernando Granha Jeronimo, Dylan Quintana, Shashank Srivastava, and Madhur Tulsiani. Unique decoding of explicit ϵ-balanced codes near the gilbert-varshamov bound. In *Proceedings of the 61st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 2020.

[GR08] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008.

[GRS00] Oded Goldreich, Dana Ron, and Madhu Sudan. Chinese remaindering with errors. *IEEE Transactions on Information Theory*, 46(4):1330–1338, 2000.

[GRX18] Venkatesan Guruswami, Nicolas Resch, and Chaoping Xing. Lossless dimension expanders via linearized polynomials and subspace designs. In *Proceedings of the 33rd Computational Complexity Conference (CCC)*, volume 102 of *LIPIcs*, pages 4:1–4:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

[GS96] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[GS99] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[Gur09] Venkatesan Guruswami. Artin automorphisms, cyclotomic function fields, and folded list-decodable codes. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC)*, pages 23–32. ACM Press, 2009.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. *Journal of the ACM*, 56(4):20:1–20:34, 2009.

[GW13] Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013.

[GX12] Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC)*, pages 339–350. ACM, 2012.

[GX13] Venkatesan Guruswami and Chaoping Xing. List decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin subcodes up to the Singleton bound. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC)*, pages 843–852. ACM Press, 2013.

[GX14] Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding of folded algebraic-geometric codes over constant-sized alphabets. In *Proceedings of the 25th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1858–1866. SIAM, 2014.

[GX15] Venkatesan Guruswami and Chaoping Xing. Optimal rate algebraic list decoding using narrow ray class fields. *Journal of Combinatorial Theory, Series A*, 129:160–183, 2015.

[GX20] Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 27:172, 2020.

[HRW20] Brett Hemenway, Noga Ron-Zewi, and Mary Wootters. Local list recovery of high-rate tensor codes and applications. *SIAM Journal on Computing*, 49(4):157–195, 2020.

[JLJ+89] Jørn Justesen, Knud J. Larsen, Helge Elbrønd Jensen, Allan Havemose, and Tom Høholdt. Construction and decoding of a class of algebraic geometry codes. *IEEE Transactions on Information Theory*, 35(4):811–821, 1989.

[KM93] Eyal Kushilevitz and Yishay Mansour. Learning decision trees using the Fourier spectrum. *SIAM Journal on Computing*, 22(6):1331–1348, 1993.

[KRR+21] Swastik Kopparty, Nicolas Resch, Noga Ron-Zewi, Shubhangi Saraf, and Shashwat Silas. On list recovery of high-rate tensor codes. *IEEE Transactions on Information Theory*, 67(1):296–316, 2021.

[KRSW18] Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters. Improved list decoding of folded Reed-Solomon and multiplicity codes. In *Proceedings of the 59th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 212–223. IEEE Computer Society, 2018.

[Lan02] Serge Lang. *Algebra*. Springer, 2002.

[MRR+20] Jonathan Mosheiff, Nicolas Resch, Noga Ron-Zewi, Shashwat Silas, and Mary Wootters. LDPC codes achieve list-decoding capacity. In *Proceedings of the 61st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 2020.

[Pet60] W. Wesley Peterson. Encoding and error-correction procedures for the Bose-Chaudhuri codes. *IRE Transactions on Information Theory*, 6(4):459–470, 1960.

[RS60] Irving S. Reed and Gustave Solomon. Polynomial codes over certain finite fields. *SIAM Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[RWZ20] Noga Ron-Zewi, Mary Wootters, and Gilles Zémor. Linear-time erasure list-decoding of expander codes. In *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2020.

[SAK+01] Kenneth W Shum, Ilia Aleshnikov, P Vijay Kumar, Henning Stichtenoth, and Vinay Deolalikar. A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound. *IEEE Transactions on Information Theory*, 47(6):2225–2241, 2001.

[She93] B. Z. Shen. A Justesen construction of binary concatenated codes that asymptotically meet the Zyablov bound for low rate. *IEEE Transactions on Information Theory*, 39(1):239–242, 1993.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[STV01] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR lemma. *Journal of Computer and System Sciences*, 62(2):236–266, 2001.

[Sud97] Madhu Sudan. Decoding of Reed Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997.

[Ta-17] Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In *Proceedings of the 49th Annual ACM Symposium on Theory of Computing (STOC)*, pages 238–251. ACM Press, 2017.

[Tre03] Luca Trevisan. List-decoding using the XOR lemma. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 126–135. IEEE Computer Society, 2003.

[TU12] Amnon Ta-Shma and Christopher Umans. Better condensers and new extractors from Parvaresh-Vardy codes. In *Proceedings of the 27th Computational Complexity Conference (CCC)*, pages 309–315. IEEE Computer Society, 2012.

[TZ04] Amnon Ta-Shma and David Zuckerman. Extractor codes. *IEEE Transactions on Information Theory*, 50(12):3015–3025, 2004.

A The Guruswami–Kopparty explicit subspace design

In this section, for completeness, we review the proof of Theorem 2.1, restated below, that gives an explicit construction of a subspace design.

Theorem 2.1 (Explicit subspace design, [GK16], Theorem 6)**.** *There exists an absolute constant $c > 1$, so that for every $\epsilon > 0$, positive integers k, m, r with $r < \frac{\epsilon m}{4}$, and a prime power q satisfying $q^m \geq \max\left\{k^{c \cdot r/\epsilon}, \left(\frac{2r}{\epsilon}\right)^{2r/\epsilon}\right\}$, there exists an (r, s)-subspace design $H_1, \ldots, H_k$ over $\mathbb{F}_{q^m}$ for $s = \frac{2r^2}{\epsilon}$, where each H_i has co-dimension at most ϵm in $\mathbb{F}_{q^m}$. Moreover, bases for $H_1, \ldots, H_k$ can be found in time* $\mathrm{poly}(q, k, m)$.

First, we recall the definition of a subspace design.

Definition A.1 (subspace design)**.** *An* (r, s)-subspace design over $\mathbb{F}_{q^m}$ of cardinality k *is a collection of k $\mathbb{F}_q$-linear subspaces $H_1, H_2, \ldots, H_k \subseteq \mathbb{F}_{q^m}$ so that $\sum_{i=1}^{k} \dim(\hat{V} \cap H_i) \leq s$ for any $\mathbb{F}_q$-linear subspace $\hat{V} \subseteq \mathbb{F}_{q^m}$ of dimension at most r.*

Next, we sketch the construction of subspace designs in [GK16]. Let $r, t, m, q, d \in \mathbb{N}^+$ be such that q is a prime power and $r \leq t \leq m < q$. Let γ be a generator of the multiplicative group $\mathbb{F}_q^\times$. For $\alpha \in \mathbb{F}_{q^d}$, define

$$S_\alpha = \{\alpha^{q^j} \gamma^i : 0 \leq j < d, 0 \leq i < t\}.$$

Lemma A.2. *There exists a set $\mathcal{F} \subseteq \mathbb{F}_{q^d}$ of cardinality at least $\frac{q^d - 1}{4dt}$ that satisfies the following conditions:*

1. *$\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$ for $\alpha \in \mathcal{F}$.*
2. *$S_\alpha \cap S_\beta = \emptyset$ for distinct $\alpha, \beta \in \mathcal{F}$.*
3. *$|S_\alpha| = dt$ for $\alpha \in \mathcal{F}$.*

Moreover, $\mathcal{F}$ can be computed in time polynomial in q^d.

Let $V = \{f(X) \in \mathbb{F}_q[X] : \deg(f) < m\} \cong \mathbb{F}_{q^m}$. For $\alpha \in \mathbb{F}_{q^d}$, define

$$H_\alpha := \{P(X) \in V : P(\alpha \cdot \gamma^i) = 0 \text{ for } j = 0, 1, \ldots, t-1\}$$

which is a subspace of V. As shown in [GK16], Theorem 2.1 follows as a consequence of the following theorem.

Theorem A.3 ([GK16])**.** *Let $\mathcal{F}$ be as in Lemma A.2. Then the collection $(H_\alpha)_{\alpha \in \mathcal{F}}$ is an (r, s)-subspace design in $V \cong \mathbb{F}_{q^m}$ for $s = \frac{(m-1)r}{d(t-r+1)}$, such that every subspace H_α has co-dimension at most dt.*

Note that Theorem A.3 requires the field size q to be greater than m while Theorem 2.1 does not, so the latter does not directly follow from the former. The idea in [GK16] is first using Theorem A.3 to construct a subspace design in $\mathbb{F}_Q^{m'}$ over an extension field $\mathbb{F}_Q$, where $m' = m/[\mathbb{F}_Q : \mathbb{F}_q]$ and $Q > m'$. (Assume m is a multiple of $[\mathbb{F}_Q : \mathbb{F}_q]$ for simplicity.) Then [GK16] showed that, by identifying $\mathbb{F}_Q^{m'}$ with $\mathbb{F}_q^m$, this also yields a subspace design in $\mathbb{F}_q^m$ with somewhat worse parameters, thereby proving Theorem 2.1. We refer the reader to [GK16] for details.

A.1 Proof of Lemma A.2

In [GK16], the set $\mathcal{F} \subseteq \mathbb{F}_{q^d}$ is chosen in the following way: For simplicity, assume d is a prime. For $\alpha, \beta \in \mathbb{F}_{q^d}^\times$, write $\alpha \sim \beta$ if $\beta = \alpha^{q^i} \cdot \delta$ for some $0 \le i < d$ and $\delta \in \mathbb{F}_q^\times$. Then $\sim$ is an equivalence relation on $\mathbb{F}_{q^d}^\times$. For each equivalence class $O \subseteq \mathbb{F}_{q^d}^\times$, choose a representative $\alpha_0 \in O$. For $\alpha \in O$, add α to $\mathcal{F}$ if and only if $\alpha = \alpha_0 \gamma^{it}$ for some integer i satisfying $0 \le i < \lfloor (q-1)/t \rfloor$.

However, we note that this construction of $\mathcal{F}$ does not always satisfy the conditions in Lemma A.2 when $d > 1$. For example, suppose d is a prime and $q-1$ is divisible by d, so that $\mathbb{F}_q^\times$ contains all the dth roots of unity. In this case, $\mathbb{F}_{q^d}$ is a *Kummer extension* $\mathbb{F}_q(\alpha)$ over $\mathbb{F}_q$ where $\alpha^d = u$ for some $u \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^d$. Then we have that α^{q-1} is a d-th root of unity as $(\alpha^{q-1})^d = (\alpha^d)^{q-1} = u^{q-1} = 1$. By assumption that $\mathbb{F}_q^\times$ contains all dth roots of unity, this implies in turn that $\alpha^{q-1} \in \mathbb{F}_q^\times$.

Let $\alpha_0 = \alpha^{q^i} \cdot \delta$ be the representative that we chose for the equivalence class of α, where $0 < i < d$ and $\delta \in \mathbb{F}_q^\times$. Then we claim that $\alpha_0^{q-1} \in \mathbb{F}_q^\times$ as $\alpha_0^{q-1} = (\alpha^{q-1})^{q^i} \cdot \delta^{q-1} = \alpha^{q-1} \in \mathbb{F}_q^\times$. Consequently, we have that $\alpha_0^q = \alpha_0 \gamma^{it+j}$ for some integers i and j with $0 \le i < \lceil (q-1)/t \rceil$ and $0 \le j < t$. If $0 < i < \lfloor (q-1)/t \rfloor$, then α_0 and $\alpha_0 \gamma^{it}$ are distinct and both added to $\mathcal{F}$. This violates the second condition in Lemma A.2 since we have $\alpha_0^q \in S_{\alpha_0}$ and $\alpha_0^q = \alpha_0 \gamma^{it+j} \in S_{\alpha_0 \gamma^{it}}$, which implies $S_{\alpha_0} \cap S_{\alpha_0 \gamma^{it}} \neq \emptyset$. Similarly, if $i = 0$, then the third condition $|S_\alpha| = dt$ does not hold.

One way of fixing this problem is ignoring those elements $\alpha \in \mathbb{F}_{q^d}^\times$ satisfying $\alpha^{q^i - 1} \in \mathbb{F}_q^\times$ for some $0 < i < d$. The next lemma gives an upper bound for the number of those elements.

Lemma A.4. *Let $B = \{\alpha \in \mathbb{F}_{q^d}^\times : \alpha^{q^i-1} \in \mathbb{F}_q^\times$ for some $0 < i < d\}$. Then $|B| \le (q^d-1)/2$.*[9]

Proof. If $d = 1$, then $|B| = 0 \le (q^d - 1)/2$. So assume $d \ge 2$. Consider $\alpha \in B$. We have $\alpha^{q^i-1} = \delta$ for some $0 < i < d$ and $\delta \in \mathbb{F}_q^\times$. Note $\alpha^{q^{d-i}-1} = (1/\delta)^{q^{d-i}} = 1/\delta$. So by replacing (i, δ) with $(d-i, 1/\delta)$ if necessary, we may assume $i \le d/2$.

For any $\alpha' \in \mathbb{F}_{q^d}^\times$ satisfying $(\alpha')^{q^i-1} = \delta$, we have $(\alpha'/\alpha)^{q^i} = \alpha'/\alpha$ and hence $\alpha'/\alpha \in \mathbb{F}_{q^i}^\times$. So the number of $\alpha' \in \mathbb{F}_{q^d}^\times$ satisfying $(\alpha')^{q^i-1} = \delta$ is at most $q^i - 1$. Therefore, for fixed $\delta \in \mathbb{F}_q^\times$, the number of $\alpha \in \mathbb{F}_{q^d}^\times$ for which there exists an integer $0 < i \le d/2$ satisfying $\alpha^{q^i-1} = \delta$ is bounded by

$$N := \sum_{i=1}^{\lfloor d/2 \rfloor} (q^i - 1) = (q^{\lfloor d/2 \rfloor + 1} - q)/(q-1) - \lfloor d/2 \rfloor.$$

There are $q-1$ choices of $\delta \in \mathbb{F}_q^\times$. So we have

$$|B| \le (q-1)N = q^{\lfloor d/2 \rfloor + 1} - q - \lfloor d/2 \rfloor (q-1).$$

When $d \ge 3$, we have $q^{\lfloor d/2 \rfloor + 1} \le q^{d-1} \le q^d/2$ and hence $|B| \le (q^d-1)/2$, as desired.

Now assume $d = 2$. We need a more careful analysis in this case. Note that if $\delta \in \mathbb{F}_q^\times$ can be written as α^{q-1} then $\delta^{q+1} = \alpha^{(q-1)(q+1)} = \alpha^{q^2-1} = 1$, i.e., δ is a $(q+1)$th root of unity. The number of such $\delta \in \mathbb{F}_q^\times$ equals $\gcd(q+1, q-1) = \gcd(q+1, 2)$. So we have

$$|B| \le \gcd(q+1, 2)N = \gcd(q+1, 2) \cdot (q-1). \tag{21}$$

It is easy to see that the RHS of (21) is at most $(q^2-1)/2$. So $|B| \le (q^2-1)/2 = (q^d-1)/2$. $\square$

[9] This bound is attained when $q = 3$ and $d = 2$ but not tight in general. We have made no attempt to optimize the bound.

We now give a complete proof of Lemma A.2.

Proof of Lemma A.2. Let B be as in Lemma A.4. For $\alpha, \beta \in \mathbb{F}_{q^d}^\times$, write $\alpha \sim \beta$ if $\beta \in \alpha^{q^i}\mathbb{F}_q^\times$ for some $0 \le i < d$. Then $\sim$ is an equivalence relation on $\mathbb{F}_{q^d}^\times$. Note that if $\alpha \sim \beta$ and $\alpha \in B$, then $\beta \in B$. So $\mathbb{F}_{q^d}^\times \setminus B$ is a disjoint union of equivalence classes under the relation $\sim$. Moreover, the definition of B implies that for every $\alpha \in \mathbb{F}_{q^d}^\times \setminus B$, the equivalence class $O_\alpha = \{\alpha^{q^j}\gamma^i : 0 \le j < d, 0 \le i < q-1\}$ of α has cardinality exactly $d(q-1)$. So the number of equivalence classes contained in $\mathbb{F}_{q^d}^\times \setminus B$ is $\frac{q^d-1-|B|}{d(q-1)} \ge \frac{q^d-1}{2d(q-1)}$, where we use the bound $|B| \le (q^d-1)/2$ given by Lemma A.4.

Construct $\mathcal{F}$ as follows: For each equivalence class $O \subseteq \mathbb{F}_{q^d}^\times \setminus B$, fix a representative $\alpha_0 \in O$, and add $\alpha_0\gamma^{it}$ to $\mathcal{F}$ for $i = 0, 1, \dots, \lfloor (q-1)/t \rfloor - 1$. We have

$$|\mathcal{F}| \ge \frac{q^d-1}{2d(q-1)} \cdot \left\lfloor \frac{q-1}{t} \right\rfloor \ge \frac{q^d-1}{2d(q-1)} \cdot \frac{q-1}{2t} = \frac{q^d-1}{4dt}.$$

Clearly, $\mathcal{F}$ can be computed in time polynomial in $|\mathbb{F}_{q^d}| = q^d$.

We have $S_\alpha \cap S_\beta = \emptyset$ for distinct $\alpha, \beta \in \mathcal{F}$ and $|S_\alpha| = dt$ for $\alpha \in \mathcal{F}$. This follows from the fact that every equivalence class $O = \{\alpha_0^{q^j}\gamma^i : 0 \le j < d, 0 \le i < q-1\} \subseteq \mathbb{F}_{q^d}^\times \setminus B$ has cardinality exactly $d(q-1)$, i.e., the $d(q-1)$ elements $\alpha_0^{q^j}\gamma^i$ are distinct.

Finally, we also have $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$ for $\alpha \in \mathcal{F}$. This follows from the fact that $\alpha^{q^i-1} \ne 1$ for $\alpha \in \mathbb{F}_{q^d}^\times \setminus B$ and $0 < i < d$, which holds by the definition of B. $\square$

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il