List decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin subcodes up to the Singleton bound[*]

Venkatesan Guruswami [†]
Carnegie Mellon University, Pittsburgh
guruswami@cmu.edu

Chaoping Xing [‡]
Nanyang Technological University, Singapore
xingcp@ntu.edu.sg

ABSTRACT

We consider Reed-Solomon (RS) codes whose evaluation points belong to a subfield, and give a linear-algebraic list decoding algorithm that can correct a fraction of errors approaching the code distance, while pinning down the candidate messages to a well-structured affine space of dimension a constant factor smaller than the code dimension. By pre-coding the message polynomials into a subspace-evasive set, we get a Monte Carlo construction of a subcode of Reed-Solomon codes that can be list decoded from a fraction $(1 - R - \varepsilon)$ of errors in polynomial time (for any fixed $\varepsilon > 0$) with a list size of $O(1/\varepsilon)$. Our methods extend to algebraic-geometric (AG) codes, leading to a similar claim over constant-sized alphabets. This matches parameters of recent results based on folded variants of RS and AG codes.

Further, the underlying algebraic idea also extends nicely to Gabidulin's construction of rank-metric codes based on linearized polynomials. This gives the ***first*** construction of positive rate rank-metric codes list decodable beyond half the distance, and in fact gives codes of rate R list decodable up to the optimal $(1 - R - \varepsilon)$ fraction of rank errors.

We introduce a new notion called *subspace designs* as another way to pre-code messages and prune the subspace of candidate solutions. Using these, we also get a *deterministic* construction of a polynomial time list decodable subcode of RS codes. By using a cascade of several subspace designs, we extend our approach to AG codes, which gives the ***first deterministic*** construction of an algebraic code family of rate R with efficient list decoding from $1 - R - \varepsilon$ fraction of errors over an *alphabet of constant size* (that depends only on ε). The list size bound is almost a constant (governed by $\log^*$ (block length)), and the code can be constructed in quasi-polynomial time.

Categories and Subject Descriptors

E.4 [**Data**]: Coding and Information Theory

Keywords

List error-correction; Algebraic codes; Subspace designs; Pseudorandomness; Rank-metric codes

1. INTRODUCTION

Reed-Solomon (RS) codes are a classical and widely used family of algebraic error-correcting codes. An $[n, k]$ RS code over a field $\mathbb{F}$ encodes polynomials $f \in \mathbb{F}[X]$ of degree $< k$ by their evaluations at a sequence $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $n \leqslant |\mathbb{F}|$ distinct field elements. The rate R of this code equals k/n, and any two distinct codewords differ on more than $(1 - R)n$ positions. Thus, a codeword can be unambiguously identified when up to a fraction $(1 - R)/2$ of its symbols are corrupted. Polynomial time algorithms dating back to 1960 are known to correct a fraction $(1-R)/2$ of errors and recover the correct codeword [22]. We stress that in this work we focus on *worst-case symbol errors*, and the error fraction counts the proportion of symbols of the received word which differ from the corresponding codeword symbol.

When the error fraction ρ exceeds $(1-R)/2$, unique recovery of the correct codeword may not be possible, but one can hope to *list decode* a small set of codewords that includes all codewords within distance ρn from the noisy input string. In fact, such a list decoding task can be accomplished in polynomial time for Reed-Solomon codes for ρ as large as $1 - \sqrt{R}$ [24, 13]. This remains the best known bound on list decodable error-fraction for RS codes. The $1 - \sqrt{R}$ bound is best possible (in the sense that a larger noise level might necessitate super-polynomial list size) in some more general settings like list recovery [11], but for list decoding itself the only known limit is the trivial bound of $1 - R$.

Recently, variants of RS codes, such as folded Reed-Solomon codes and derivative codes [12, 14, 18], have been used to decode up to a fraction of errors approaching $1 - R$. The $1 - R$ bound is the Singleton bound on relative distance of codes, and information-theoretically optimal for error-correction as one cannot hope to correct an error fraction larger than the proportion of redundant symbols in the codeword.

In this work, we show that certain *subcodes* of RS codes where the evaluation points $\alpha_1, \ldots, \alpha_n$ belong to a *subfield*

[*] Full version available at http://eccc.hpi-web.de/report/2012/146/

[†] Research supported in part by a Packard Fellowship and NSF CCF 0963975.

[‡] Research supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03 and Singapore A*STAR SERC under Research Grant 1121720011.

STOC'13, June 1–4, 2013, Palo Alto, California, USA.
Copyright 2013 ACM 978-1-4503-2029-0/13/06 ...$10.00.

of $\mathbb{F}$ can also be decoded up to the $1-R$ radius. In fact, we show that these RS codes *themselves* can be list decoded up to radius $(1-R-\varepsilon)$, pinning down the candidate messages to a subspace of dimension εk (or, to be accurate, a subspace over the subfield $\mathbb{K}$ of $\mathbb{F}$ of dimension $\varepsilon k[\mathbb{F}:\mathbb{K}]$). The *list size*, i.e., bound on number of codewords that might be output, is $\approx |\mathbb{F}|^{\varepsilon k}$; though exponential, note that it is non-trivially smaller than the total number $|\mathbb{F}|^k$ of possible messages.

To bring down the list size and decoding complexity, we use a subcode of the RS code that only encodes polynomials whose coefficients are restricted to belong to a carefully chosen subset that is (a) large (so we don't lose much in rate) and (b) *subspace-evasive.* Specifically, we ensure that this subset has a small intersection with every subspace of the sort output by the list decoder, and further allows for polynomial time computation of this intersection. (Note that testing all $\mathbb{F}^{\varepsilon k}$ candidates in the subspace for membership in the subspace-evasive subset would take too long.)

An explicit construction of a large subspace-evasive set in $\mathbb{F}^k$ that intersects every d-dimensional subspace in $d^{O(d)}$ points was given by Dvir and Lovett [4]. The intersection size was improved to $2^{O(d)}$ at the expense of worse construction complexity [1]. In our applications, the subspaces we need to evade have $\Omega(k)$ dimension, so we cannot afford an intersection size that is exponential in the dimension. We instead exploit the structural properties of the subspaces we encounter in list decoding to construct subsets with much smaller intersection. We do this in two ways: (i) using hierarchically subspace-evasive (h.s.e) sets as in our previous work [15][1]; this in fact achieves $O_\varepsilon(1)$ intersection size, but we only know a randomized construction, and (ii) using *subspace designs*, a notion apparently new to this work, which we can construct deterministically, and which ensures that the intersection is itself a subspace of (nearly) $O_\varepsilon(1)$ size. Further details on our techniques, both algebraic and pseudorandomness related, are discussed in Section 2.

1.1 Our results for RS & AG codes

Below is a statement of our result on list decoding RS codes (the details can be found in Section 7.1).

Theorem 1.1 (List decoding RS (sub)-codes). *Let $\varepsilon > 0$, and k, n be integers with $1 \leqslant k < n$. Let $\mathbb{F}_q$ be a field of characteristic 2, with $n \leqslant q \leqslant \mathrm{poly}(n)$. Let $m = \Theta(1/\varepsilon^2)$. Consider the $[n,k]$ Reed-Solomon code over alphabet $\mathbb{F}_{q^m}$ of rate $R = k/n$ whose evaluation points lie in the subfield $\mathbb{F}_q$. This code can be list decoded in polynomial time up to $(1-\varepsilon)(n-k)$ errors pinning down the candidate messages to an subspace over $\mathbb{F}_q$ of dimension at most εmk.*

Further, there are subcodes of this RS code, of rate $(1-\varepsilon)R$, list-decodable in polynomial time (for fixed $\varepsilon > 0$) from fraction $(1-R-\varepsilon)$ of errors using list size ℓ, with

(i) $\ell = O(1/(R\varepsilon))$. (This subcode is non-linear and admits a Monte Carlo construction in $(n/\varepsilon)^{O(1)}$ time.)

(ii) $\ell = n^{O(1/\varepsilon^2)}$, with the list contained in a subspace of dimension $O(1/\varepsilon^2)$ over $\mathbb{F}_q$. (This subcode is $\mathbb{F}_q$-linear and can be constructed in $n^{\mathrm{poly}(1/\varepsilon)}$ time.)

As a comparison, folded RS and derivative codes offer a list size guarantee similar to the deterministic construction (ii) above (in fact, the bound on dimension is better and equals $O(1/\varepsilon)$) [14]. Those codes also admit a randomized subcode construction (using appropriate subspace-evasive sets) that brings down the list size to $O_\varepsilon(1)$, similar to (i) above [14], and an explicit construction to reduce the list size to $\exp(\tilde{O}(1/\varepsilon))$ [4]. These and other previous results for list decoding from $1-R-\varepsilon$ error fraction are listed in Figure 1. The main point of Theorem 1.1 above is not the parameters, but that we can construct subcodes of Reed-Solomon codes themselves that can be list decoded up to the optimal error fraction with polynomial complexity. Perhaps more importantly, the methods extend to (i) Algebraic-geometric codes, leading to explicit codes offering new trade-offs (the last row of Figure 1), and (ii) Gabildulin codes for the rank metric, giving the first algorithm to list decode beyond half the distance with positive rate, as discussed in Section 1.2.

AG subcodes. In our work [15], we extended the linear-algebraic list decoding algorithm to folded algebraic-geometric (AG) codes, and showed that (pseudorandom) subcodes of certain folded AG codes achieve similar parameters to part (i) of Theorem 1.1 and in addition have an alphabet size $\exp(\tilde{O}(1/\varepsilon^2))$ (the alphabet size using RS codes in Theorem 1.1 is $n^{O(1/\varepsilon^2)}$). Here, we extend our approach for RS codes with evaluation points in a subfield to algebraic-geometric codes based on constant extensions. Using pseudorandomly constructed subcodes of such AG codes, in this work we match these parameters obtained in [15]. Perhaps more significantly, we also give a deterministic subcode construction (in quasi-polynomial time) with near-constant list size. This gives the ***first deterministic construction*** of an *algebraic* code family with optimal rate list decoding (i.e., list decoding $1-R-\varepsilon$ fraction of errors with rate R) over an *alphabet of constant size* (that depends only on ε). Previously, such codes were known only via code concatenation with inner codes found by brute-force combined with expander-based symbol redistribution [12]. Additionally, the list size in our construction is bounded by a very slowly growing function of the block length. The one minus point is that the construction time is quasi-polynomial in the block length. Below is a more formal statement that we can prove for AG list decoding (the details appear in Section 7.2).

Theorem 1.2 (List decoding AG (sub)-codes). *For arbitrary $R, \varepsilon \in (0,1)$, pick a prime power $q = \Theta(1/\varepsilon^2)$ and integer $m = \Theta(1/\varepsilon^2)$. Then, we can construct a family of algebraic-geometric codes over $\mathbb{F}_{q^m}$ of rate R that can be list decoded from a fraction $(1-R)(1-\varepsilon)$ of errors, pinning down the candidate messages to an subspace over $\mathbb{F}_q$ of dimension at most εmk (where k is the dimension of the code).*

Further, there are subcodes of this AG code, of rate at least $(1-\varepsilon)R$ with the following guarantees for list decoding from fraction $(1-R-\varepsilon)$ of errors:

(i) Constant list size $O(1/(R\varepsilon))$, polynomial decoding complexity $\mathrm{poly}(N, \exp(1/\varepsilon^2))$. This subcode is non-linear and admits a Monte Carlo construction in $(N/\varepsilon)^{O(1)}$ time where N is the block length.

(ii) An $(N/\varepsilon)^{O(1)}$ time decoder that finds a subspace of dimension $\exp(O(\log^* N)^2)$ over $\mathbb{F}_q$ containing the list. This subcode is $\mathbb{F}_q$-linear and can be constructed deterministically in $N^{O(\log_q^3 N)}$ time.

A point worth noting about our deterministic constructions (part (ii) of Theorems 1.1 and 1.2) is that the subcode

[1] Actually, we use a combination of h.s.e sets with the Dvir-Lovett construction; see Section 2 for details.

Code	Construction	Alphabe size	List size	Decoding time	Reference
Folded RS/derivative	Deterministic	$n^{O(1/\varepsilon^2)}$	$n^{O(1/\varepsilon)}$	$n^{O(1/\varepsilon)}$	[12, 14], [18]
Folded RS subcode	Monte Carlo	$n^{O(1/\varepsilon^2)}$	$O(1/\varepsilon)$	$n^{O(1/\varepsilon)}$	[14]
Folded RS subcode	Deterministic	$n^{O(1/\varepsilon^2)}$	$(1/\varepsilon)^{O(1/\varepsilon)}$	$n^{O(1)}2^{1/\varepsilon^{O(1)}}$	[4]
Folded cyclotomic	Las Vegas	$(\log n)^{O(1/\varepsilon^2)}$	$n^{O(1/\varepsilon^2)}$	$n^{O(1/\varepsilon^2)}$	[8]
Folded AG subcode	Monte Carlo	$\exp(\tilde{O}(1/\varepsilon^2))$	$O(1/\varepsilon)$	$n^{O(1)}2^{1/\varepsilon^{O(1)}}$	[15]
RS subcode	Monte Carlo	$n^{O(1/\varepsilon^2)}$	$O(1/\varepsilon)$	$n^{O(1)}2^{1/\varepsilon^{O(1)}}$	Thm. 1.1
RS subcode	Deterministic	$n^{O(1/\varepsilon^2)}$	$n^{O(1/\varepsilon^2)}$	$n^{O(1/\varepsilon^2)}$	Thm 1.1
AG subcode	Monte Carlo	$\exp(\tilde{O}(1/\varepsilon^2))$	$O(1/\varepsilon)$	$n^{O(1)}2^{1/\varepsilon^{O(1)}}$	Thm. 1.2
AG subcode	Deterministic†	$\exp(\tilde{O}(1/\varepsilon^2))$	$\ell = 2^{2^{(\log^* n)^2}}$	$n^{O(1)}(1/\varepsilon)^{O(\ell)}$	Thm. 1.2

Figure 1: Parameters of various constructions of codes that enable list decoding $(1-R-\varepsilon)$ fraction of errors, with rate R. The last four lines are from this work. The † refers to quasi-polynomial construction time (though this can be improved to polynomial time using explicit subspace designs constructed subsequently in [9]). The rows with first column in boldface are not dominated by other constructions. The last row gives the first deterministic construction of algebraic codes for efficient optimal rate list decoding over constant-sized alphabets. $\log^* n$ denotes the number of iterated logarithms to the base 2 needed to reach a number below 1.

is *linear* over the subfield $\mathbb{F}_q$ of the alphabet $\mathbb{F}_{q^m}$. Further, the list decoder will prune the $\approx \varepsilon mk$-dimensional to a near-constant dimensional subspace by imposing additional $\mathbb{F}_q$-*linear* constraints on the message.

To summarize, our basic construction is based on Reed-Solomon codes themselves, and not any folded version or other variant. The underlying approach can be extended to AG codes, and yields codes matching previous parameters for randomized constructions, and a deterministic construction with improved parameters. Figure 1 compares parameters of different constructions for optimal rate list decoding.

As mentioned earlier, a further advantage of our approach is that it extends to give similar guarantees for *Gabidulin codes* [5], which are the rank-metric analog of Reed-Solomon codes, based on linearized polynomials. In fact, we originally discovered the new algorithm in the context of rank-metric codes, and later realized it also applied for RS and AG codes. We describe rank-metric codes and the prior and our results for list decoding them next.

Subsequent work on subspace designs. Following the submission of this work, the first author and Kopparty have constructed subspace designs which are in fact inspired by folded RS and derivative codes [9]. Their construction provides explicit algebraic descriptions of the subspaces leading to a highly efficient deterministic construction. Plugging these in, we can construct the deterministic subcodes of RS codes in Part (ii) of Theorem 1.1 in n^c time with a fixed exponent c, and the subcode of AG codes in Part (ii) of Theorem 1.2 in poly(N) time (though the bound on the dimension of the candidate space of solutions worsens slightly to doubly exponential in $\log^* N$).

1.2 Rank-metric codes

A rank-metric code $\mathcal{C}$ is a collection of matrices of certain dimension over a finite field (say, $\mathcal{C} \subseteq \mathbb{M}_{n\times t}(\mathbb{F}_h)$, with $n \leqslant t$, where $\mathbb{M}_{n\times t}(\mathbb{F}_h)$ denotes the set of $n \times t$ matrices with entries in $\mathbb{F}_h$). The rate of $\mathcal{C}$ is defined to be $\log_h |\mathcal{C}|/(nt)$. The notion of distance $d(A, B)$ between matrices A, B is the rank distance $\text{rank}(A - B)$, and the (rank) distance d of $\mathcal{C}$ equals $\min_{A\neq B\in\mathcal{C}} \text{rank}(A - B)$. Gabidulin gave a construction of rank-metric codes which are the analog of RS codes in the world of linearized polynomials [5]. The messages of Gabidulin codes are h-linearized polynomials over $\mathbb{F}_{h^t}$ of h-degree less than k, and such a polynomial f is encoded into $(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n))^T \in \mathbb{M}_{n\times t}(\mathbb{F}_h)$, where $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{h^t}$ are linearly independent over $\mathbb{F}_h$, and we think of $f(\alpha_j)$ as a column vector in $\mathbb{F}_h^t$ under a fixed $\mathbb{F}_h$-basis of $\mathbb{F}_{h^t}$. The rate of this code is k/n, and its rank distance is $n - k + 1$, which is optimal and meets the Singleton bound for rank-metric codes.

Prior and recent work. The rank metric was first considered in the context of coding theory by Delsarte (who used the terminology of bilinear forms) [3]. In addition to being a natural concept of inherent interest, rank-metric codes are motivated by several applications such as linear network coding, magnetic tape recording, memory chip arrays, pacetime coding in wireless communications, public key cryptosystems, etc. The Gabidulin codes play a preeminent role in the subject, and the problem of unique decoding them up to $(n - k)/2$ rank errors (this means recovering a codeword matrix M given $M + E$ where the error matrix E has rank at most $(n - k)/2$) has received a lot of attention. In fact, starting with Gabidulin's original paper [5], it has been solved *several* times, by adapting the different approaches for unique decoding Reed-Solomon codes to the linearized setting.

Despite this interest and many results paralleling RS codes, an algorithm for *list* decoding Gabidulin codes beyond half the distance has remained elusive. In this context, it is worth mentioning that no analog of the Johnson bound (which implies a small list size up to radius $1 - \sqrt{R}$ for RS codes) is known for rank-metric codes. Therefore, we currently do not even know if list decoding Gabidulin codes up to radius $1 - \sqrt{R}$, or for that matter any error fraction exceeding $(1 - R)/2$, is *combinatorially* feasible (in that the number of close-by codewords is guaranteed to be small). By adapting a construction from [2], Wachter-Zeh has shown that for Gabidulin codes, correcting more than a fraction $1 - \sqrt{R}$ of rank errors is not possible with a polynomial sized list [25].

Recently, a folded variant of Gabidulin codes (paralleling the folded RS codes of [12]) was considered in [10] (and independently in [20]), and a linear-algebraic list decoding algorithm along the lines of [14] was given for these codes. The results of [10] are stated for the model of "subspace codes" and deal with the analog of Gabidulin codes in this setting defined by [26, 17]. But subspace codes are closely related to rank-metric codes (see [23]), and the results of [10] can be readily translated to rank-metric codes. In particular, the authors of [10] give a code construction that can correct a fraction $(1-\varepsilon)$ of rank errors for any $\varepsilon > 0$, but the rate is polynomially small. The loss in rate occurs because in order to keep the list size small, the h-linearized message polynomials must be restricted to have coefficients in the base field $\mathbb{F}_h$ instead of $\mathbb{F}_{h^t}$, and this makes the rate a factor t smaller. The same drawback applies to [20].

List decoding of subspace codes that are in some sense the linearized analog of Parvaresh-Vardy codes [21] was studied in [19], but their algorithm could only correct "insertions" (and not removal of basis elements from the subspace), and so does not immediately apply to the rank-metric setting.

Our results. In this work, we consider Gabidulin codes where the n evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n$ belong to a subfield $\mathbb{F}_{h^n}$ of the field $\mathbb{F}_{h^t}$ over which the message polynomials are defined (so we require $n|t$). The evaluation points thus form an $\mathbb{F}_h$-basis of $\mathbb{F}_{h^n}$. We give a list decoding algorithm for these Gabidulin codes, and combine them with suitable hierarchical subspace-evasive sets, to prove the following statement paralleling Theorem 1.1.

THEOREM 1.3. *Let $\mathbb{F}_h$ be a finite field of characteristic 2, $\varepsilon > 0$, and k, n, t be integers with $1 \leqslant k < n < O(\varepsilon^2 t)$ and $n|t$. Consider the Gabidulin code $\mathcal{G} \subseteq \mathbb{M}_{n\times t}(\mathbb{F}_h)$ consisting of evaluations of h-linearized polynomials in $\mathbb{F}_{h^t}[X]$ of h-degree at most $k-1$ at an $\mathbb{F}_h$-basis of $\mathbb{F}_{h^n}$. The code $\mathcal{G}$ can be list decoded in polynomial time up to $(1-\varepsilon)(n-k)$ rank errors pinning down the candidate messages to an $\mathbb{F}_h$-subspace of dimension at most εtk.*

Further, there is a Monte Carlo construction of a subcode of this Gabidulin code, of rate $R = (1-\varepsilon)k/n$, which can be list decoded from $(1-\varepsilon)(n-k)$ errors in $\mathrm{poly}(n, \log h, \exp(1/\varepsilon^2))$ *time, outputting a list of size at most $O(1/(R\varepsilon))$.*

Thus we are able to give a Monte Carlo construction of a rank-metric code of rate R that is efficiently list decodable up to a fraction $(1-R-\varepsilon)$ of rank errors. Note that we list decode up to the best possible radius, approaching the Singleton bound. Further, to our knowledge, this is the first construction of rank-metric codes with rate bounded away from zero that can be list decoded beyond the half-the-distance bound. We can also obtain a result for ***subspace codes*** studied by Koetter and Kschischang [17] using similar methods, yielding list decodable codes with trade-offs almost matching existential bounds.

Due to space restrictions, we do not discuss the technical aspects of our result for Gabidulin or subspace codes further in this extended abstract; the details may be found in the full version. All skipped proofs also appear in the full version.

2. OUR TECHNIQUES

We now discuss at a high level some of the new ingredients in this work.

Algebraic ideas. We begin by describing how restricting evaluation points to a subfield enables correcting more errors, which is the algebraic starting point of our work. The idea behind list decoding results for folded RS (or derivative) codes in [12, 14] is that the encoding of a message polynomial $f \in \mathbb{F}_Q[X]$ includes the values of f and closely related polynomials at the evaluation points. Given a string not too far from the encoding of f, one can use this property together with the "interpolation method" to find an algebraic condition that f (and its closely related polynomials) must satisfy, eg. $A_0(X) + A_1(X)f(X) + A_2(X)f'(X) + \cdots + A_s(X)f^{(s-1)}(X) = 0$ in the case of derivative codes [14] (here $f^{(i)}$ denotes the i'th formal derivative of f, and the $A_0, A_1, \ldots, A_s$ are low-degree polynomials found by the decoder). The solutions $f(X)$ to this equation form an affine space, which can be efficiently found (and later pruned for list size reduction when we pre-code messages into a subspace-evasive set).

For Reed-Solomon codes as in Theorem 1.1, the encoding only includes the values of f at $\alpha_1, \alpha_2, \ldots, \alpha_n$. But since $\alpha_i \in \mathbb{F}_q$, we have $f(\alpha_i)^q = f^\sigma(\alpha_i)$ where f^σ is the polynomial obtained by the action of the Frobenius automorphism that maps $y \mapsto y^q$ on f (formally, $f^\sigma(X) = \sum_{j=0}^{k-1} f_j^q X^j$ if $f(X) = \sum_{j=1}^{k-1} f_j X^j$). Thus the decoder can "manufacture" the values of f^σ (and similarly $f^{\sigma^2}, f^{\sigma^3}$, etc.) at the α_i. Applying the above approach then enables finding a relation $A_0(X) + A_1(X)f(X) + A_2(X)f^\sigma(X) + \cdots + A_s(X)f^{\sigma^{s-1}}(X) = 0$, which is again an $\mathbb{F}_q$-linear condition on f that can be used to solve for f.

To extend this idea to algebraic-geometric codes, we work with constant extensions $\mathbb{F}_{q^m} \cdot F$ of algebraic function fields $F/\mathbb{F}_q$. The messages belong to a Riemann-Roch space over $\mathbb{F}_{q^m}$, but they are encoded via their evaluations at $\mathbb{F}_q$-rational points. Similarly to [15], for decoding we recover the message function f in terms of the coefficients of its local expansion at some rational point P. (The Reed-Solomon setting is a special case when $F = \mathbb{F}_q(X)$, and P is 0, i.e., the zero of X.) To get the best trade-offs, we use AG codes based on a tower of function fields due to Garcia and Stichtenoth [6, 7] which achieve the optimal trade-off between the number of $\mathbb{F}_q$-rational points and the genus. For this case, we recover messages in terms of their local expansion around the point at infinity P_∞ which is also used to define the Riemann-Roch space of messages.

Subspace designs and subspace-evasive sets. In the case of folded RS codes, the solutions to the equation $A_0(X) + A_1(X)f(X) + A_2(X)f(\gamma X) + \cdots + A_s(X)f(\gamma^{s-1}X) = 0$ are restricted to an s-dimensional space over $\mathbb{F}_Q$ with $Q = q^m$, if $f \in \mathbb{F}_Q[X]$ [14], and a similar statement holds for derivative codes. For the Reed-Solomon codes with evaluation points in $\mathbb{F}_q$ considered in this work, *each* coefficient f_j, $j = 0, 1, \ldots, k-1$, of $f = f_0 + f_1 X + \cdots + f_{k-1}X^{k-1} \in \mathbb{F}_{q^m}[X]$ will be restricted to an s-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$. This would lead to a list size bound of $(q^s)^k$, which is exponentially large. Thus, to get polynomial complexity, we need to prune this space by intersecting it with a large subspace-evasive subset of $\mathbb{F}_q^{mk}$ (where we treat the coefficient vector $(f_0, f_1, \ldots, f_{k-1})$ as an element of $\mathbb{F}_q^{mk}$ by fixing some $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$). Despite the large dimension, the solution subspace has a nice "periodic" structure; namely, once $f_0, f_1, \ldots, f_{i-1}$ are fixed, the i'th "block" f_i belongs to an s-dimensional subspace of $\mathbb{F}_q^m$. Exploiting this, we can use hierarchically subspace-evasive (h.s.e) sets of the kind constructed in [15] to randomly construct a subcode achieving list size as small as $O(1/\varepsilon)$. (We actually observe and use a simplification of this construction, by defining the set based on values of random polynomials instead of their zero sets, following [14, Sec. 4.1].)

Naively computing the intersection of the solution space with the h.s.e set will involve trying all possibilities in $\mathbb{F}_q^m$ to compute the allowed extensions f_i to each partial solution $f_0, \dots, f_{i-1}$. The resulting q^m time complexity will be a large polynomial (like n^{1/ε^2}) in the Reed-Solomon case, and worse still, super-polynomial in the case of Gabidulin codes for rank-metric. To circumvent this problem, we compose the h.s.e set with an "inner" subspace-evasive subset $\mathcal{I} \subset \mathbb{F}_q^m$ in each of the k blocks. (That is, we insist f_i belongs to $\mathcal{I}$, in addition to $(f_0, \dots, f_{k-1})$ belonging to the h.s.e set.)

For the subset $\mathcal{I}$, we use the subspace-evasive variety constructed by Dvir and Lovett [4] (with a different choice of degree parameters to accommodate any field size). The intersection of an s-dimensional subspace with this variety can be found in time polynomial in the intersection size. This allows us to find the allowed extensions f_i to $f_0, \dots, f_{i-1}$ efficiently without searching over all q^m possibilities, and leads to the claimed runtime bounds for decoding the (randomized) subcodes of RS and Gabidulin codes in Theorems 1.1 and 1.3.

The h.s.e sets are constructed randomly and lead to Monte Carlo constructions of the associated subcodes. We next turn to our *deterministic* subcode constructions (parts (ii) of Theorems 1.1 and 1.2). The starting point for this is an observation we make that the periodic property of the subspace of candidate solutions is even nicer than what was used in [15]. Specifically, there is a subspace $W \subset \mathbb{F}_q^m$ such that once $f_0, f_1, \dots, f_{i-1}$ are fixed, f_i belongs to a coset of W (the point is that this W is the *same* for every block i). Our idea then is to restrict f_i to belong to a subspace H_i where $H_1, H_2, \dots, H_k$ are a collection of subspaces in $\mathbb{F}_q^m$ such that for any s-dimensional subspace $W \subset \mathbb{F}_q^m$, only a small number of them have non-trivial intersection with W. More precisely, we require that $\sum_{i=1}^k \dim(W \cap H_i)$ is small. We call such a collection as a *subspace design* in $\mathbb{F}_q^m$. We feel that the concept of subspace designs is interesting in its own right, and view the introduction of this notion in Section 5 as a key contribution in this work.

There are known explicit constructions of "spreads" which are a collection of $\approx q^{m/2}$ subspaces of $\mathbb{F}_q^m$ which pairwise intersect only at 0 [16]. These would ensure that $\sum_{i=1}^k \dim(W \cap H_i) \leqslant \dim(W) \leqslant s$. But the subspaces in such spreads necessarily have dimension at most $m/2$, so restricting $f_i \in H_i$ for such subspaces would incur a factor two loss in rate. We instead resort to random choices of the subspaces. We prove that $q^{\Omega(\varepsilon m)}$ random subspaces of dimension $(1-\varepsilon)m$ have small total intersection with every s-dimensional W. Furthermore, we are also able to derandomize this construction using conditional expectations to also get a deterministic construction. This leads to the subcodes of Reed-Solomon codes promised in Theorem 1.1, part (ii).

For explicit subcodes of algebraic-geometric codes (Section 7.2), we need additional ideas. The dimension k in the case of AG codes is much larger than the alphabet size q^m (that's the whole point of generalizing to AG codes). So we cannot have a subspace design in $\mathbb{F}_q^m$ with k subspaces. We therefore use several "layers" of subspace designs in a cascaded fashion – the first one in $\mathbb{F}_q^m$, the next one in $\mathbb{F}_q^{m_1}$ for $m_1 \gg q^{\sqrt{m}}$, the third one in $\mathbb{F}_q^{m_2}$ for $m_2 \gg q^{\sqrt{m_1}}$ and so on. Since the m_i's increase exponentially, we only need about $\log^* k$ levels of subspace designs. Each level incurs about a factor $1/\varepsilon$ increase in the dimension of the "period subspace" (which is W when we begin). With a careful technical argument and choice of parameters, we are able to obtain the bounds of Theorem 1.2, part (ii).

In the Gabidulin case, the relevant field size is too large for us to even afford a dimension 1 affine space as the list of solutions. Therefore, we are not able to use our subspace design based approach for finding efficiently list decodable subcodes. So for the Gabidulin case, we only construct subcodes using h.s.e sets.

3. PERIODIC SUBSPACES

In this section we formalize a certain "periodic" property of affine subspaces that will arise in our list decoding application. A property of similar nature was formulated in our earlier work [15]; here we give a more restrictive definition which turns out to more accurately capture the kind of subspaces we encounter. This in turn facilitates pruning the list of candidate solutions in the subspace via appropriate pre-coding of the messages.

For a vector $\mathbf{y} = (y_1, y_2, \dots, y_m) \in \mathbb{F}_q^m$ and positive integers $t_1 \leqslant t_2 \leqslant m$, we denote by $\text{proj}_{[t_1,t_2]}(\mathbf{y}) \in \mathbb{F}_q^{t_2-t_1+1}$ its projection onto coordinates t_1 through t_2, i.e., $\text{proj}_{[t_1,t_2]}(\mathbf{y}) = (y_{t_1}, y_{t_1+1}, \dots, y_{t_2})$. When $t_1 = 1$, we use $\text{proj}_t(\mathbf{y})$ to denote $\text{proj}_{[1,t]}(\mathbf{y})$. These notions are extended to subsets of strings in the obvious way: $\text{proj}_{[t_1,t_2]}(S) = \{\text{proj}_{[t_1,t_2]}(\mathbf{x}) \mid \mathbf{x} \in S\}$.

Definition 1 (Periodic subspaces). *For positive integers r, b, Λ and $\kappa := b\Lambda$, an affine subspace $H \subset \mathbb{F}_q^\kappa$ is said to be (r, Λ, b)-periodic if there exists a subspace $W \subseteq \mathbb{F}_q^\Lambda$ of dimension at most r such that for every $j = 1, 2, \dots, b$, and every "prefix" $\mathbf{a} \in \mathbb{F}_q^{(j-1)\Lambda}$, the projected affine subspace of $\mathbb{F}_q^\Lambda$ defined as $\{\text{proj}_{[(j-1)\Lambda+1, j\Lambda]}(\mathbf{x}) \mid \mathbf{x} \in H$ and $\text{proj}_{(j-1)\Lambda}(\mathbf{x}) = \mathbf{a}\}$ is contained in an affine subspace of $\mathbb{F}_q^\Lambda$ given by $W + \mathbf{v_a}$ for some vector $\mathbf{v_a} \in \mathbb{F}^\Lambda$ dependent on $\mathbf{a}$.*

The motivation of the above definition will be clear when we present our linear-algebraic list decoders, which will pin down the messages that must be output within an $(s-1, m, k)$-periodic (affine) subspace of $\mathbb{F}_q^{mk}$ (where q^m will be the alphabet size of the code, k its dimension, and s a parameter of the algorithm that governs how close the decoding performance approaches the Singleton bound).

The following properties of periodic affine spaces follow from the definition.

Claim 3.1. *Let H be an (r, Λ, b)-periodic affine subspace. Then for each $j = 1, 2, \dots, b$,*

1. *the projection of H to the first j blocks of Λ coordinates, $\text{proj}_{j\Lambda}(H) = \{\text{proj}_{j\Lambda}(\mathbf{x}) \mid \mathbf{x} \in H\}$, has dimension at most jr. (In particular H has dimension at most br.)*
2. *for each $\mathbf{a} \in \mathbb{F}_q^{(j-1)\Lambda}$, there are at most q^r extensions $\mathbf{y} \in \text{proj}_{j\Lambda}(H)$ such that $\text{proj}_{(j-1)\Lambda}(\mathbf{y}) = \mathbf{a}$.*

For an affine space H, its *underlying subspace* is the subspace S such that H is a coset of S.

Ultra-periodic subspaces. For our result on pre-coding algebraic-geometric codes with subspace designs, we will exploit an even stronger property that holds for the subspaces output by the linear-algebraic list decoder. We formalize this notion below.

Definition 2. *An affine subspace H of $\mathbb{F}_q^\kappa$ is said to be (r, Λ)-*ultra periodic *if for every integer ℓ, $1 \leqslant \ell \leqslant \frac{\kappa}{\Lambda}$, setting $b_\ell = \left\lfloor \frac{\kappa}{\ell\Lambda} \right\rfloor$, we have $\text{proj}_{b_\ell \cdot \ell\Lambda}(H)$ is $(\ell r, \ell\Lambda, b_\ell)$-periodic.*

The definition captures the fact that the subspace is periodic not only for blocks of size Λ, but also for block sizes that are multiples of Λ. Thus the subspace looks periodic in all "scales" simultaneously.

4. LIST DECODING RS AND AG CODES

In this section, we will present a linear-algebraic list decoding algorithm for algebraic-geometric (AG) codes based on evaluations of functions at rational points over a subfield. The algorithm will manage to correct a large fraction of errors, and pin down the possible messages to a well-structured affine subspace of dimension much smaller than that of the code. For simplicity, we begin with the case of Reed-Solomon codes in Section 4.1. This can be extended to a general framework for decoding AG codes based on constant field extensions. To obtain our result on AG subcodes (Theorem 1.2), we instantiate the general framework (with a slight twist) to codes based on the Garcia-Stichtenoth tower. Due to space restrictions, we omit the technical details concerning AG codes, and only state the final result for AG codes based on Garcia-Stichtenoth tower here. As usual, the skipped details may be found in the full version.

4.1 Decoding Reed-Solomon codes

Our list decoding algorithm will apply to Reed-Solomon codes with evaluation points in a subfield, defined below.

Definition 3. *Let $\mathbb{F}_q$ be a finite field with q elements, and m a positive integer. Let n, k be positive integers satisfying $1 \leqslant k < n \leqslant q$. The Reed-Solomon code $\mathsf{RS}^{(q,m)}[n,k]$ is a code over alphabet $\mathbb{F}_{q^m}$ that encodes a polynomial $f \in \mathbb{F}_{q^m}[X]$ of degree at most $k-1$ as $f(X) \mapsto (f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n))$ where $\alpha_1, \alpha_2, \dots, \alpha_n$ are an arbitrary sequence of n distinct elements of $\mathbb{F}_q$.*

Note that while the message polynomial has coefficients from $\mathbb{F}_{q^m}$, the encoding only contains its evaluations at points in the subfield $\mathbb{F}_q$. The above code has rate k/n, and minimum distance $(n-k+1)$.

We now present a list decoding algorithm for the above Reed-Solomon codes. Suppose the codeword $(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n))$ is received as $(y_1, y_2, \dots, y_n) \in \mathbb{F}_{q^m}^n$ with at most $e = \tau n$ errors (i.e., $y_i \neq f(\alpha_i)$ for at most e values of $i \in \{1, 2, \dots, n\}$). The goal is to recover the list of all polynomials of degree less than k whose encoding is within Hamming distance e from y. As is common in algebraic list decoders, the algorithm will have two steps: (i) interpolation to find an algebraic equation the message polynomials must satisfy, and (ii) solving the equation for the candidate message polynomials.

Interpolation step. Let $1 \leqslant s \leqslant m$ be an integer parameter of the algorithm. Choose the "degree parameter" $D = \left\lfloor \frac{n-k+1}{s+1} \right\rfloor$.

Definition 4 (Space of interpolation polynomials). *Let $\mathcal{P}$ be the space of polynomials $Q \in \mathbb{F}_{q^m}[X, Y_1, Y_2, \dots, Y_s]$ of the form $Q(X, Y_1, Y_2, \dots, Y_s) = A_0(X) + A_1(X)Y_1 + A_2(X)Y_2 + \cdots + A_s(X)Y_s$, with each $A_i \in \mathbb{F}_{q^m}[X]$ and $\deg(A_0) \leqslant D + k - 1$ and $\deg(A_i) \leqslant D$ for $i = 1, 2, \dots, s$.*

The lemma below follows because for our choice of D, the number of degrees of freedom for polynomials in $\mathcal{P}$ exceeds the number n of interpolation conditions (1).

Lemma 4.1. *There exists a nonzero polynomial $Q \in \mathcal{P}$ such that*

$$Q(\alpha_i, y_i, y_i^q, y_i^{q^2}, \cdots, y_i^{q^{s-1}}) = 0 \quad \textit{for} \quad i = 1, 2, \dots, n\ . \quad (1)$$

Further such a Q can be found using $O(n^3)$ operations over $\mathbb{F}_{q^m}$.

Lemma 4.2 below shows that any polynomial Q given by Lemma 4.1 yields an algebraic condition that the message functions f we are interested in list decoding must satisfy.

Definition 5 (Frobenius action on polynomials). *For a polynomial $f \in \mathbb{F}_{q^m}[X]$ with $f(X) = f_0 + f_1 X + \cdots + f_{k-1}X^{k-1}$, define the polynomial $f^\sigma \in \mathbb{F}_{q^m}[X]$ as $f^\sigma(X) = f_0^q + f_1^q X + \cdots + f_{k-1}^q X^{k-1}$.*

For $i \geqslant 2$, we define f^{σ^i} recursively as $(f^{\sigma^{i-1}})^\sigma$.

The following simple fact is key to our analysis: If $\alpha \in \mathbb{F}_q$, then $f(\alpha)^{q^j} = (f^{\sigma^j})(\alpha)$ for all poisitive integers j.

Lemma 4.2. *Suppose $Q \in \mathcal{P}$ satisfies the interpolation conditions (1). Suppose $f \in \mathbb{F}_{q^m}[X]$ of degree less than k satisfies $f(\alpha_i) \neq y_i$ for at most e values of $i \in \{1, 2, \dots, n\}$ with $e \leqslant \frac{s}{s+1}(n-k)$. Then $Q(X, f(X), f^\sigma(X), f^{\sigma^2}(X), \cdots, f^{\sigma^{s-1}}(X)) = 0$.*

Proof. Define the polynomial $\Phi \in \mathbb{F}_{q^m}[X]$ by $\Phi(X) := Q(X, f(X), f^\sigma(X), f^{\sigma^2}(X), \cdots, f^{\sigma^{s-1}}(X))$. By the construction of Q and the fact that $\deg(f) \leqslant k-1$, we have $\deg(\Phi) \leqslant D + k - 1 \leqslant \frac{n-k+1}{s+1} + k - 1 = \frac{n}{s+1} + \frac{s}{s+1}(k-1)$.

Suppose $y_i = f(\alpha_i)$. By the above fact, we have $y_i^q = f(\alpha_i)^q = (f^\sigma)(\alpha_i)$, and similarly $y_i^{q^j} = (f^{\sigma^j})(\alpha_i)$ for $j = 2, 3, \dots$. Thus for each i such that $f(\alpha_i) = y_i$, we have $\Phi(\alpha_i) = Q(\alpha_i, f(\alpha_i), f^\sigma(\alpha_i), \cdots, f^{\sigma^{s-1}}(\alpha_i)) = Q(\alpha_i, y_i, y_i^q, \cdots, y_i^{q^{s-1}}) = 0$. Thus Φ has at least $n - e \geqslant \frac{n}{s+1} + \frac{s}{s+1}k$ zeroes. Since this exceeds the upper bound on the degree of Φ, Φ must be the zero polynomial. □

Finding candidate solutions. The previous two lemmas imply that the polynomials f whose encodings differ from $(y_1, \cdots, y_n)$ in at most $\frac{s}{s+1}(n-k)$ positions can be found amongst the solutions of the functional equation $A_0 + A_1 f + A_2 f^\sigma + \cdots + A_s f^{\sigma^{s-1}} = 0$. We now prove that these solutions form a well-structured affine space over $\mathbb{F}_q$.

Lemma 4.3. *For integers $1 \leqslant s \leqslant m$, the set of solutions $f = \sum_{i=0}^{k-1} f_i X^i \in \mathbb{F}_{q^m}[X]$ to the equation*

$$A_0(X) + A_1(X)f(X) + A_2(X)f^\sigma(X) + \cdots + A_s(X)f^{\sigma^{s-1}}(X) = 0 \quad (2)$$

when at least one of $\{A_0, A_1, \dots, A_s\}$ is nonzero is an affine subspace over $\mathbb{F}_q$ of dimension at most $(s-1)k$. Further, fixing an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$ and viewing each f_i as an element of $\mathbb{F}_q^m$, the solutions are an $(s-1, m, k)$-periodic subspace of $\mathbb{F}_q^{mk}$, and a representation of this periodic subspace can be computed in $\mathrm{poly}(k, m, \log q)$ time.

Proof. If f, g are two solutions to (2), then so is $\alpha f + \beta g$ for any $\alpha, \beta \in \mathbb{F}_q$ with $\alpha + \beta = 1$. So the solutions to (2) form an affine $\mathbb{F}_q$-subspace. We now proceed to analyze the structure of the subspace.

First, by factoring out a common powers of X that divide all of $A_0(X), A_1(X), \dots, A_s(X)$, we can assume that at least one $A_{i^*}(X)$ for some $i^* \in \{0,1,\dots,s\}$ is not divisible by X, and has nonzero constant term. Further, if $A_1(X),\dots,A_s(X)$ are all divisible by X, then so is $A_0(X)$, so we can take $i^* > 0$.

Let us denote $A_\iota(X) = a_{\iota,0} + a_{\iota,1}X + a_{\iota,2}X^2 + \cdots$ for $\iota = 0,1,2,\dots,s$. For $l = 0,1,2,\dots,k-1$, define the linearized polynomial

$$B_l(X) = a_{1,l}X + a_{2,l}X^q + a_{3,l}X^{q^2} + \cdots + a_{s,l}X^{q^{s-1}} \ . \tag{3}$$

We know that $a_{i^*,0} \neq 0$, and therefore $B_0 \neq 0$. This implies that the solutions $\beta \in \mathbb{F}_{q^m}$ to $B_0(\beta) = 0$ is a subspace, say W, of $\mathbb{F}_{q^m}$ of dimension at most $s-1$.

Fix an $i \in \{0,1,\dots,k-1\}$. Expanding the equation (2) and equating the coefficient of X^i to be 0, we get

$$a_{0,i} + B_i(f_0) + B_{i-1}(f_1) + \cdots + B_1(f_{i-1}) + B_0(f_i) = 0 \ . \tag{4}$$

This implies $f_i \in W + \theta_i$ for some $\theta_i \in \mathbb{F}_{q^m}$ that is determined by $f_0, f_1, \dots, f_{i-1}$. Therefore, for each choice of $f_0, f_1, \dots, f_{i-1}$, f_i must belong to a fixed coset of the subspace W of dimension at most $s-1$. Thus, the solutions belong to an $(s-1,m,k)$-periodic subspace. Also, it is clear from (4) that a representation of the periodic subspace can be computed in $\mathrm{poly}(k, m, \log q)$ time. □

Combining Lemmas 4.2 and 4.3, we see that one can find an affine space of dimension $(s-1)k$ that contains all messages differing from the input received word in at most a fraction $\frac{s}{s+1}(1-R)$ of the positions. Note the dimension of the message space of the Reed-Solomon code $\mathsf{RS}^{(q,m)}[n,k]$ over $\mathbb{F}_q$ is km. The above lemma pins down the candidate polynomials to a space of dimension $(s-1)k$. For $s \ll m$, this is a lot smaller.

In Sections 5 and 6, we will see two approaches to pick subcodes of RS codes based on subspace designs and hierarchical subspace-evasive sets respectively. These will enable efficient pruning of the subspace of solutions to a much smaller list.

4.2 Garcia-Stichtenoth codes

By applying the above techniques to AG codes based on constant field extensions $\mathbb{F}_{q^m} \cdot K_e$ of function fields $K_e/\mathbb{F}_q$ from the e'th level of the Garcia-Stichtenoth tower of function fields [6, 7], we can obtain a list decoding of Garcia-Stichtenoth codes with constant alphabet size and other similar parameters. Our formal result is as follows.

Theorem 4.4. *Let q be the even power of a prime. Let $1 \leqslant s \leqslant m$ be integers, and let $R \in (0,1)$. Then for infitely many N (all integers of the form $q^{e/2}(\sqrt{q}-1)$), there is a deterministic polynomial time construction of an $\mathbb{F}_{q^m}$-linear code $\mathrm{GS}^{(q,m)}[N,k]$ of block length N and dimension $k = R \cdot N$ that can be list decoded in $\mathrm{poly}(N, m, \log q)$ time from $\frac{s}{s+1}(N-k) - \frac{3N}{\sqrt{q}-1}$ errors, pinning down the messages to one of $q^{O(mN)}$ possible $(s-1,m)$-ultra periodic $\mathbb{F}_q$-affine subspaces of $\mathbb{F}_q^{mk}$.*

The main idea of list-decoding in this case is that we recover the message in terms of the coefficients of its local expansion at a point called P_∞. Moreover, by choosing a set of k functions $\{h_1,\dots,h_k\}$ in a Riemann-Roch space with their first k local expansions forming the $k \times k$ identity matrix, our encoding and decoding become efficient, even when a subset of $\mathbb{F}_{q^m}^k$ is chosen as the message space. (This allows us to freely pick subcodes of the AG code, as we will do in Section 7.2.) More precisely, a message $(a_1,\dots,a_k) \in \mathbb{F}_{q^m}^k$ is encoded into the function $f := \sum_{i=1}^k a_i h_i$. To list decode, we just output the first k coefficients of the local expansion of the possible candidate functions f at P_∞, which by the choice of the h_i's must equal the message $(a_1, a_2, \dots, a_k)$.

5. SUBSPACE DESIGNS

The linear-algebraic list decoder discussed in the previous sections pins down the coefficients of the message to a periodic subspace. This subspace has linear dimension, so we need to restrict the coefficients further so that the subspace can be pruned to a small list of solutions. In this section, we will use a special collection of subspaces, which we call a *subspace design* to achieve this.

Definition 6. *Let Λ be a positive integer, and q a prime power. For positive integers $r < \Lambda$ and d, an (r,d)-subspace design in $\mathbb{F}_q^\Lambda$ is a collection of subspaces of $\mathbb{F}_q^\Lambda$ such that for every r-dimensional subspace $W \subset \mathbb{F}_q^\Lambda$, we have*
$\sum_{H \in \mathcal{H}} \dim(W \cap H) \leqslant d$.
The cardinality of a subspace design $\mathcal{H}$ is the number of subspaces in its collection, i.e., $|\mathcal{H}|$. If all subspaces in $\mathcal{H}$ have the same dimension t, then we refer to t as the dimension *of the subspace design $\mathcal{H}$.*

The usefulness of subspace designs in the context of pruning periodic subspaces is captured by the following key lemma.

Lemma 5.1. *Suppose $H_1, H_2, \dots, H_b$ are subspaces in an (r,d)-subspace design in $\mathbb{F}_q^\Lambda$, and T is a (r,Λ,b)-periodic affine subspace of $\mathbb{F}_q^{\Lambda b}$ with underlying subspace S. Then the set $\mathcal{T} = \{(\mathbf{f_1}, \mathbf{f_2}, \dots, \mathbf{f_b}) \in T \mid \mathbf{f_j} \in H_j$ for $j = 1,2,\dots,b\}$ is an affine subspace of $\mathbb{F}_q^{\Lambda b}$ of dimension at most d. Also, the underlying subspace of $\mathcal{T}$ is contained in $\mathcal{S} \stackrel{\text{def}}{=} S \cap (H_1 \times H_2 \times \cdots \times H_b)$.*

Constructing subspace designs. We now turn to the construction of subspace designs of large size and dimension. We first analyze the performance of a random collection of subspaces.

Lemma 5.2. *Let $\eta > 0$ and q be a prime power. Let r, Λ be integers $\Lambda \geqslant 8/\eta$ and $r \leqslant \eta\Lambda/2$. Consider a collection $\mathcal{H}$ of subspaces of $\mathbb{F}_q^\Lambda$ obtained by picking, independently at random, $q^{\eta\Lambda/8}$ subspaces of $\mathbb{F}_q^\Lambda$ of dimension $(1-\eta)\Lambda$ each. Then, with probability at least $1 - q^{-\Lambda r}$, $\mathcal{H}$ is an $(r, 8r/\eta)$-subspace design.*

Note that given a collection $\mathcal{H}$ of subspaces, one can deterministically check if it is an (r,d)-subspace design in $\mathbb{F}_q^\Lambda$ in $q^{O(\Lambda r)}|\mathcal{H}|$ time by doing a brute-force check of all r-dimensional subspaces W of $\mathbb{F}_q^\Lambda$, and for each computing $\sum_{H \in \mathcal{H}} \dim(W \cap H)$ using $|\mathcal{H}|\Lambda^{O(1)}$ operations over $\mathbb{F}_q$. Thus the above lemma already gives a *Las Vegas* construction of an (r,d)-subspace design with many subspaces each of large dimension $(1-\eta)m$ (recorded formally in Lemma 5.3 below). We next prove that the construction can in fact be derandomized using the method of conditional expectations, thus giving a deterministic construction in similar runtime.

Lemma 5.3. *For parameters η, r, Λ as in Lemma 5.2, for any $b \leqslant q^{\eta\Lambda/8}$, one can compute an $(r, 8r/\eta)$-subspace design* *in $\mathbb{F}_q^\Lambda$ of dimension $(1-\eta)\Lambda$ and cardinality b deterministically in time polynomial in $q^{\Lambda(\Lambda+r)}(br/\eta)^{r/\eta}$. One can also compute such a subspace in $q^{O(\Lambda r)}$* Las Vegas *time.*[2]

Finally, we record the construction of subspaces with low-dimensional intersection with every periodic subspace based on the above subspace designs. This form will be convenient for later use in pre-coding Reed-Solomon codes.

Theorem 5.4. *Let $\eta \in (0,1)$ and q be a prime power, and r, Λ, b be integers such that $\Lambda \geqslant 8/\eta$, $r \leqslant \eta\Lambda/2$ and $b \leqslant q^{\eta\Lambda/8}$. Then, one can construct a subspace V of $\mathbb{F}_q^{b\Lambda}$ of dimension at least $(1-\eta)b\Lambda$ in either deterministic $q^{O(\Lambda^2)}$ time or Las Vegas $q^{O(\Lambda r)}$ time with the following guarantee: For every (r, Λ, b)-periodic subspace $T \subset \mathbb{F}_q^{b\Lambda}$, $V \cap T$ is an $\mathbb{F}_q$-affine subspace of dimension at most $8r/\eta$.*

Proof. We will take $V = H_1 \times H_2 \times \cdots H_b$ where the H_i's belong to a $(r, 8r/\eta)$-subspace design in $\mathbb{F}_q^\Lambda$ of size b and dimension at least $(1-\eta)\Lambda$ as guaranteed by Lemma 5.3. Clearly $\dim(V) \geqslant (1-\eta)b\Lambda$ since each H_i has dimension at least $(1-\eta)\Lambda$. The claim now follows using Lemma 5.1. □

Cascaded subspace designs

In preparation for our results about algebraic-geometric subcodes, whose block length $\gg q^m$ is much larger than the possible size of subspace designs in $\mathbb{F}_q^m$, we now formalize a notion that combines several "levels" of subspace designs.

Definition 7. *Let l be a positive integer. For positive integers $r_0 \leqslant r_1 \leqslant \cdots \leqslant r_l$ and $m_0 \leqslant m_1 \leqslant \cdots \leqslant m_l$ such that $m_{\iota-1}|m_\iota$ for $1 \leqslant \iota \leqslant l$, an $(r_0, r_1, \ldots, r_l)$*-cascaded subspace design *with length-vector $(m_0, m_1, \ldots, m_l)$ and dimension vector $(d_0, d_1, \ldots, d_{l-1})$ is a collection of l subspace designs, specifically an $(r_{\iota-1}, r_\iota)$-subspace design in $\mathbb{F}_{q^{m_{\iota-1}}}$ of cardinality $m_\iota/m_{\iota-1}$ and dimension $d_{\iota-1}$ for each $\iota = 1, 2, \ldots, l$.*

The $l = 1$ case of the above definition corresponds to an (r_0, r_1)-subspace design in $\mathbb{F}_q^{m_0}$ of dimension d_0 and cardinality m_1/m_0. In Lemma 5.1, we used the subspace $H_1 \times H_2 \times \cdots \times H_b$ based on a subspace design consisting of the H_i's to prune a periodic subspace. Generalizing this, we now define a subspace associated with a cascaded subspace design based on the subspace designs comprising it.

Definition 8 (Canonical subspace). *Let $\mathcal{M}$ be a cascaded subspace design with length-vector $(m_0, m_1, \ldots, m_l)$ such that the ι'th subspace design in $\mathcal{M}$ has subspaces $H_1^{(\iota)}, H_2^{(\iota)}, \cdots, H_{m_\iota/m_{\iota-1}}^{(\iota)} \subset \mathbb{F}_q^{m_{\iota-1}}$, for $1 \leqslant \iota \leqslant l$.*

The canonical subspace *associated with such a cascaded subspace design, denoted $U(\mathcal{M})$, is a subspace of $F_q^{m_l}$ defined as follows: A vector $\mathbf{x} \in \mathbb{F}_q^{m_l}$ belongs to $U(\mathcal{M})$ if and only if for every $\iota \in \{1, 2, \ldots, l\}$, each of the m_ι-sized blocks of $\mathbf{x}$ given $\mathrm{proj}_{[jm_\iota+1,(j+1)m_\iota]}(\mathbf{x})$ for $0 \leqslant j < m_l/m_\iota$) belongs $H_1^{(\iota)} \times H_2^{(\iota)} \times \cdots \times H_{m_\iota/m_{\iota-1}}^{(\iota)}$.*

The following simple fact gives a lower bound on the dimension of a canonical subspace.

Observation 5.5. *For a cascaded subspace design $\mathcal{M}$ as above, if the ι'th subspace design has dimension at least $(1-\xi_{\iota-1})m_{\iota-1}$ for $1 \leqslant \iota \leqslant l$, then the dimension of the canonical subspace $U(\mathcal{M})$ is at least $\Big(1 - (\xi_0 + \xi_1 + \cdots + \xi_{l-1})\Big)m_l$.*

The following is the crucial claim about pruning ultra-periodic subspaces using (the canonical subspace of) a cascaded subspace design. It generalizes Lemma 5.1 which corresponds to the $l = 1$ case. The idea is to apply Lemma 5.1 inductively, for increasing periods $m_0, m_1, \ldots, m_{l-1}$.

Lemma 5.6. *Let $\mathcal{M}$ be a $(r_0, r_1, \ldots, r_l)$-cascaded subspace design with length-vector $(m_0, m_1, \ldots, m_l)$. Let T be a (r_0, m_0)-ultra periodic affine subspace of $\mathbb{F}_q^{m_l}$. Then the dimension of the affine space $T \cap U(\mathcal{M})$ is at most r_l.*

We conclude this section by recording a good construction of a canonical subspace that has low-dimensional intersection with ultra-periodic subspaces. This statement will be used later in pre-coding algebraic-geometric codes based on the Garcia-Stichtenoth tower.

Theorem 5.7. *Let $\eta \in (0,1)$, $q \geqslant 4$ be a prime power, and integers r, Λ satisfy $\Lambda \geqslant \Omega(1/\eta^2)$ and $r \leqslant \eta\Lambda/2$. For all large enough multiples κ of Λ, we can construct a subspace U of $\mathbb{F}_q^\kappa$ of dimension at least $(1-\eta)\kappa$ such that for every (r, Λ)-ultra periodic affine subspace $T \subset \mathbb{F}_q^\kappa$, the dimension of the affine subspace $U \cap T$ is at most $r \cdot (1/\eta)^{O(\log^* \kappa)} 2^{O((\log^* \kappa)^2)}$. The subspace U can be constructed in deterministically in $\kappa^{O(\log_q^3 \kappa)}$ time.*

The theorem is proved by taking U to be the canonical subspace $U(\mathcal{M})$ of an appropriate cascaded subspace design $\mathcal{M}$ whose length-vector has exponentially increasing components. For the rather technical details, see the full version. (The construction time can now be made $\mathrm{poly}(\kappa)$ using the explicit subspace designs of [9]; the bound on $\dim(U \cap T)$ will, however, be slightly worse with a doubly exponential dependence on $\log^* \kappa$.)

6. SUBSPACE-EVASIVE SETS

For our code constructions, we will need to pre-code the messages into large subsets of $\mathbb{F}_q^\kappa$ that have small intersection with the sort of subspaces of the message space $\mathbb{F}_q^\kappa$ output by the linear-algebraic list decoder. We already saw one approach to accomplish this using subspace designs by exploiting the periodic nature of the subspaces we encounter. In this section, we will develop a different approach that will lead to better parameters at the expense of settling for Monte Carlo constructions. We begin by recalling the notion of a *subspace-evasive* set [14].

Definition 9. *For positive integer parameters r, ℓ, a set $S \subset \mathbb{F}_q^\kappa$ is (r, ℓ)-subspace evasive if for every affine subspace H of $\mathbb{F}_q^\kappa$ of dimension at most r, $|S \cap H| \leqslant \ell$.*

Let $\mathcal{F}$ be a family of affine subspaces of $\mathbb{F}_q^\kappa$ each of dimension at most r. A set $S \subset \mathbb{F}_q^\kappa$ is $(\mathcal{F}, r, \ell)$-subspace evasive if $|S \cap H| \leqslant \ell$ for every affine subspace $H \in \mathcal{F}$.

We now turn to a more specific notion of subspace evasiveness, tailored to periodic subspaces. This will enable the efficient computation of the intersection of the subspace-evasive set with the candidate periodic subspace.

[2] Following this work, an explicit construction of $(r, O(r^2/\eta))$-subspace designs with size $q^{\Omega(\eta\Lambda/r)}$ was given in [9]. When the field size satisfies $q > \Lambda$, one gets an $(r, O(r/\eta))$-subspace design.

Hierarchical subspace-evasive sets. We now define the special subspace-evasive sets that are useful for efficient pruning of candidate messages belonging to a (r, Λ, b)-periodic subspace. This notion is the same as the one from our previous work [15].

Definition 10. *Let $\mathcal{F}$ be a family of (r, Λ, b)-periodic subspaces of $\mathbb{F}_q^{b\Lambda}$, and $L \geqslant 1$ an integer. A subset $S \subset \mathbb{F}_q^{b\Lambda}$ is said to be $(\mathcal{F}, r, \Lambda, b, L)$-h.s.e (for hierarchically subspace evasive) if for every affine subspace $H \in \mathcal{F}$, the following bound holds for $j = 1, 2, \dots, b$: $|\mathrm{proj}_{j\Lambda}(S) \cap \mathrm{proj}_{j\Lambda}(H)| \leqslant L$.*

Due to space restrictions we directly state our final result on the construction of h.s.e sets. Though the notion of h.s.e sets is from our earlier work [15], here we make some simplifications and improvements.

Theorem 6.1. *Suppose b, c, Δ, r are positive integers, $k = b\Delta$, q a power of a prime p, and $\zeta \in (0, 1/6)$ satisfying the conditions $r < \zeta\Delta/4$ and $ck < q^r$. Let $\mathcal{F}$ be a family of (r, Δ, b)-periodic subspaces of $\mathbb{F}_q^k$ with $|\mathcal{F}| \leqslant q^{ck}$. Then there exists a randomized $\mathrm{poly}(k, 1/\zeta, \log q)$ time construction of an injective map $\widetilde{\mathsf{HSE}} : \mathbb{F}_q^{(1-3\zeta)k} \to \mathbb{F}_q^k$ such that*

1. *$\widetilde{\mathsf{HSE}}$ is computable in deterministic $\mathrm{poly}(k, 1/\zeta, \log q)$ time.*
2. *With high probability, the image of $\widetilde{\mathsf{HSE}}$ is $(\mathcal{F}, br, 2c/\zeta)$-subspace evasive as a subset of $\mathbb{F}_q^k$.*

   Further, given a (r, Δ, b)-periodic subspace $H \in \mathcal{F}$, one can compute the set $\{\mathbf{x} \in \mathbb{F}_q^{(1-3\zeta)k} \mid \widetilde{\mathsf{HSE}}(\mathbf{x}) \in H\}$ of size at most $2c/\zeta$ in deterministic $\mathrm{poly}(k, p^{r^2}, \Delta^r, 1/\zeta, \log q)$ time.

7. LIST DECODABLE RS & AG SUBCODES

We now combine our code constructions with a pre-coding step that restricts coefficients to belong to either a subspace design or a hierarchical subspace-evasive set, and thereby obtain subcodes that are list decodable with smaller list-size in polynomial time.

7.1 Reed-Solomon codes

We begin with the case of Reed-Solomon codes. For a finite field $\mathbb{F}_q$, constant $\varepsilon > 0$, integers n, k, m, s satisfying $1 \leqslant k < n \leqslant q$ and $1 \leqslant s \leqslant \varepsilon m/12$, we will define subcodes of $\mathrm{RS}^{(q,m)}[n, k]$. Below for a polynomial $f \in \mathbb{F}_{q^m}[X]$ with k coefficients $f_0, f_1, \dots, f_{k-1}$, we denote by $\mathbf{f_0}, \mathbf{f_1}, \dots, \mathbf{f_{k-1}}$ the representation of these coefficients as vectors in $\mathbb{F}_q^m$ by fixing some $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$.

7.1.1 Subcode construction based on subspace designs

Define the subcode $\widehat{\mathsf{RS}}$ of $\mathrm{RS}^{(q,m)}[n, k]$ consisting of the encodings of $f \in \mathbb{F}_{q^m}[X]$ such that $(\mathbf{f_0}, \mathbf{f_1}, \dots, \mathbf{f_{k-1}}) \in V$ for a subspace $V \subseteq \mathbb{F}_q^{mk}$ guaranteed by Theorem 5.4, when applied with the parameter choices $\Lambda = m$; $b = k$; $r = s - 1$; and $\eta = \varepsilon$. Note that $\widehat{\mathsf{RS}}$ is an $\mathbb{F}_q$-linear code over the alphabet $\mathbb{F}_{q^m}$ of rate $(1 - \varepsilon)k/n$, and it can be constructed in deterministic $q^{O(m^2)}$ time, or Las Vegas $q^{O(ms)}$ time.

Theorem 7.1. *Given an input string $\mathbf{y} \in \mathbb{F}_{q^m}^n$, a basis of an affine subspace of dimension at most $O(s/\varepsilon)$ that includes all codewords of the above subcode within Hamming distance $\frac{s}{s+1}(n - k)$ from $\mathbf{y}$ can be found in deterministic $\mathrm{poly}(n, \log q, m)$ time.*

Proof. By Lemma 4.3, we can compute the $(s-1, m, k)$-periodic subspace T of messages whose Reed-Solomon encodings can be within Hamming distance $\frac{s}{s+1}(n - k)$ from $\mathbf{y}$. By Theorem 5.4, the intersection $T \cap V$ is an affine subspace over $\mathbb{F}_q$ of dimension $d = O(s/\varepsilon)$. Since both steps involve only basic linear algebra, they can be accomplished using $\mathrm{poly}(n, m)$ operations over $\mathbb{F}_q$. □

By picking $s = \Theta(1/\varepsilon)$ and $m = \Theta(1/\varepsilon^2)$ in the above construction, we can conclude the following.

Corollary 7.2. *For every $R \in (0, 1)$ and $\varepsilon > 0$, and all large enough integers $n < q$ with q a prime power, one can construct a rate R $\mathbb{F}_q$-linear subcode of a Reed-Solomon code of length n over $\mathbb{F}_{q^m}$, such that the code can be (i) encoded in $(n/\varepsilon)^{O(1)}$ time and (ii) list decoded from a fraction $(1-\varepsilon)(1-R)$ of errors in $(n/\varepsilon)^{O(1)}$ time, outputting a subspace over $\mathbb{F}_q$ of dimension $O(1/\varepsilon^2)$ including all closeby codewords. The code can be constructed deterministically in $q^{\varepsilon^{-O(1)}}$ time.*

We note that the above list decoding guarantee is in fact weaker than what is achieved for folded RS codes in [14], where the codewords were pinned down to a dimension $O(1/\varepsilon)$ subspace. The main point of the above result is not the parameters but that an explicit subcode of RS codes has optimal list decoding radius with polynomial complexity.

7.1.2 Subcode construction based on h.s.e sets

We now pre-code the messages of the RS code with an h.s.e set instead of subspace designs. This gives a much better list size, but we only get a randomized construction. Define the subcode of $\mathrm{RS}^{(q,m)}[n, k]$ consisting of the encodings of $f \in \mathbb{F}_{q^m}[X]$ such that $(\mathbf{f_0}, \mathbf{f_1}, \dots, \mathbf{f_{k-1}}) = \widetilde{\mathsf{HSE}}(\mathbf{x})$ for some $\mathbf{x} \in \mathbb{F}_q^{(1-\varepsilon)mk}$ where $\widetilde{\mathsf{HSE}}$ is the (randomized) map guaranteed by Theorem 6.1 for parameters $\zeta = \varepsilon/3$, $\Delta = m$, $b = k$ and $r = s - 1$. By definition, the above is a code of rate $(1 - \varepsilon)k/n$ over the alphabet $\mathbb{F}_{q^m}$. It is also encodable in $\mathrm{poly}(n, m, \log q, 1/\varepsilon)$ time, since both $\widetilde{\mathsf{HSE}}$ and the Reed-Solomon encoding can be computed in this time. We now turn to the list decoding.

Theorem 7.3. *Given an input string $\mathbf{y} \in \mathbb{F}_{q^m}^n$, a list of size at most $O(1/(R\varepsilon))$ that includes all codewords of the above subcode within Hamming distance $\frac{s}{s+1}(n - k)$ from $\mathbf{y}$ can be found in deterministic $\mathrm{poly}(n, \log q, 1/\varepsilon, m^s, p^{s^2})$ time, where $p = \mathrm{char}(\mathbb{F}_q)$.*

By picking $q \leqslant 2n$ to be a power of 2 and setting $s = \Theta(1/\varepsilon)$ and $m = \Theta(1/\varepsilon^2)$ in the above construction (so that the requirement $s \leqslant \varepsilon m/12$ is met), we can conclude the following.

Corollary 7.4. *For every $R \in (0, 1)$ and $\varepsilon > 0$, there is a Monte Carlo construction of a rate R subcode of a Reed-Solomon code of length n over a field of characteristic 2 and size at most $n^{O(1/\varepsilon^2)}$ (with evaluation points in a subfield) that can be encoded in $(n/\varepsilon)^{O(1)}$ time and that with high probability can be list decoded from a fraction $(1-\varepsilon)(1-R)$ of errors in deterministic $\mathrm{poly}(n, \exp(1/\varepsilon^2))$ time, outputting a list of size at most $O(1/(R\varepsilon))$.*

7.2 Subcodes of Garcia-Stichtenoth codes

We now pre-code the codes constructed in Section 4.2. For a finite field $\mathbb{F}_q$, constant $\varepsilon > 0$, and integers s, m satisfying $1 \leqslant s \leqslant \varepsilon m/12$ and $m \geqslant \Omega(1/\varepsilon^2)$, we will define subcodes of $\mathrm{GS}^{(q,m)}[N,k]$ guaranteed by Theorem 4.4. Note that messages space of this code can be identified with $\mathbb{F}_q^{mk}$.

7.2.1 Subcode construction based on cascaded subspace designs

Define the subcode $\widehat{GS}$ of $\mathrm{GS}^{(q,m)}[N,k]$ consisting of the encodings of a subspace $U \subseteq \mathbb{F}_q^{mk}$ guaranteed by Theorem 5.7, when applied with the parameter choices $\eta = \varepsilon$; $r = s-1$; $\Lambda = m$; and $\kappa = km$. Note that $\widehat{GS}$ is an $\mathbb{F}_q$-linear code over the alphabet $\mathbb{F}_{q^m}$ of rate $(1-\varepsilon)k/N$. Also, it can be constructed in deterministic $(km)^{O(\log_q^3(km))}$ time by virtue of the construction complexity of U.

The following lemma can be proved by combining Theorems 4.4 and 5.7.

Lemma 7.5. *Given an input string $\mathbf{y} \in \mathbb{F}_{q^m}^N$, a basis of an affine subspace of dimension at most*

$$s \cdot (1/\varepsilon)^{O(\log^*(km))} \cdot 2^{O((\log^*(km))^2)}$$

that includes all codewords of the above subcode within Hamming distance $\frac{s}{s+1}(N-k) - 3N/(\sqrt{q}-1)$ from $\mathbf{y}$ can be found in deterministic $\mathrm{poly}(n, \log q, m)$ time.

By taking $q = \Theta(1/\varepsilon^2)$, and choosing $s = \Theta(1/\varepsilon)$ and $m = \Theta(1/\varepsilon^2)$ in the above lemma, we conclude the following.

Theorem 7.6 (Main deterministic codes). *For every $R \in (0,1)$ and $\varepsilon > 0$, for $q = \Theta(1/\varepsilon^2)$, we can construct an $\mathbb{F}_q$-linear family of codes of rate R over an alphabet of size $q^{O(\varepsilon^{-2})}$ such that a code of block length N in the family can be (i) encoded in $(N/\varepsilon)^{O(1)}$ time, and (ii) list decoded from a fraction $(1-R-\varepsilon)$ of errors in $(N/\varepsilon)^{O(1)}$ time, outputting a subspace over $\mathbb{F}_q$ of dimension at most $2^{O((\log^* N)^2)}$ (for large enough N) that includes all closeby codewords. The code can be constructed* deterministically *in $N^{O(\log_q^3 N)}$ time.*

7.2.2 Subcode construction based on h.s.e. sets

By pre-coding the messages of the Garcia Stichtenoth code with an h.s.e set, we get a much better list size, at the expense of a randomized construction. The parameters match our earlier result for folded algebraic-geometric codes from [15]. The proof is similar to Corollary 7.4.

Theorem 7.7. *For every $R \in (0,1)$ and $\varepsilon > 0$, there is a Monte Carlo construction of a rate R subcode of an algebraic-geometric code of length N over a field of characteristic 2 and size at most $(1/\varepsilon)^{O(1/\varepsilon^2)}$ that can be encoded in $(N/\varepsilon)^{O(1)}$ time and that with high probability can be list decoded from a fraction $(1-R-\varepsilon)$ of errors in deterministic* $\mathrm{poly}(N, \exp(1/\varepsilon^2))$ *time, outputting a list of size at most $O(1/(R\varepsilon))$.*

8. REFERENCES

[1] A. Ben-Aroya and I. Shinkar. A note on subspace evasive sets. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:95, 2012.

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

[3] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *J. Comb. Theory, Ser. A*, 25(3):226–241, 1978.

[4] Z. Dvir and S. Lovett. Subspace evasive sets. In *Proceedings of the 44th ACM Symposium on Theory of Computing*, pages 351–358, 2012.

[5] E. M. Gabidulin. Theory of codes with maximal rank distance. *Problems of Information Transmission*, 21(7):1–12, 1985.

[6] A. Garcia and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlădut bound. *Inventiones Mathematicae*, 121:211–222, 1995.

[7] A. Garcia and H. Stichtenoth. On the asymptotic behavior of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[8] V. Guruswami. Cyclotomic function fields, Artin-Frobenius automorphisms, and list error-correction with optimal rate. *Algebra and Number Theory*, 4(4):433–463, 2010.

[9] V. Guruswami and S. Kopparty. Explicit subspace designs. In preparation, 2013.

[10] V. Guruswami, S. Narayanan, and C. Wang. List decoding subspace codes from insertions and deletions. In *Proceedings of Innovations in Theoretical Computer Science (ITCS 2012)*, pages 183–189, January 2012.

[11] V. Guruswami and A. Rudra. Limits to list decoding Reed-Solomon codes. *IEEE Transactions on Information Theory*, 52(8):3642–3649, August 2006.

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

[13] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and Algebraic-geometric codes. *IEEE Trans. on Information Theory*, 45(6):1757–1767, 1999.

[14] V. Guruswami and C. Wang. Linear-algebraic list decoding for variants of Reed-Solomon codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:73, 2012.

[15] V. Guruswami and C. Xing. Folded codes from function field towers and improved optimal rate list decoding. *CoRR*, abs/1204.4209, 2012. Extended abstract appeared in the Proceedings of the 44th ACM Symposium on Theory of Computing (STOC'12).

[16] J. W. P. Hirschfield. *Projective Geometries over Finite Fields.* Oxford Univ. Press, 1979.

[17] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

[18] S. Kopparty. List-decoding multiplicity codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:44, 2012.

[19] H. Mahdavifar and A. Vardy. Algebraic list-decoding on the operator channel. In *Proceedings of the IEEE International Symposium on Information Theory*, pages 1193–1197, 2010.

[20] H. Mahdavifar and A. Vardy. List-decoding of subspace codes and rank-metric codes up to Singleton bound. *CoRR*, abs/1202.0866, 2012.

[21] F. Parvaresh and A. Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 285–294, 2005.

[22] W. W. Peterson. Encoding and error-correction procedures for Bose-Chaudhuri codes. *IEEE Transactions on Information Theory*, 6:459–470, 1960.

[23] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Trans. on Information Theory*, 54(9):3951–3967, 2008.

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

[25] A. Wachter-Zeh. Bounds on list decoding Gabidulin codes. *CoRR*, abs/1205.0345, 2012.

[26] H. Wang, C. Xing, and R. Safavi-Naini. Linear authentication codes: Bounds and constructions. *IEEE Transactions on Information Theory*, 49(4):866–872, 2003.