Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 214 (2026)

Algebraic-Geometric Parvaresh–Vardy Subspace Designs and Rank Condensers

Gil Cohen* Dean Doron† Noam Goldgraber‡

Abstract

A subspace design is a collection of subspaces $H_1, \ldots, H_n$ of $\mathbb{F}_q^k$ with the property that no low-dimensional subspace W intersects the collection "too much". Subspace designs and related objects in linear-algebraic pseudorandomness have found a broad range of applications, ranging from list decoding and recovery, to derandomizing algorithms.

We construct explicit strong subspace designs over *every* finite field. In the extremal case where the co-dimension t of each H_i is equal to the dimension of W, for every constant field size our construction attains $n = \Omega(k)$ and matches the probabilistic intersection bound up to a constant factor. All previous constructions required the field size to grow with t (or k). Our subspace designs also imply new constructions of rank condensers over arbitrary finite fields. This result is the first to achieve an optimal dependence on k while maintaining both a constant output entropy rate and a constant field size. As an application, we construct lossless rank extractors for linear sources of rank r, for all $r < q$, with parameters matching those of Guo, Raj, Shangguan and Zhang (FOCS '26), thereby generalizing their result to prime fields and smaller field sizes.

Our construction is based on an algebraic-geometric version of the Parvaresh–Vardy codes (Parvaresh–Vardy FOCS '05, Guruswami ECCC '05), extending the framework underlying the condensers of Guruswami, Umans and Vadhan (JACM '09). We view our construction as a linear-algebraic analysis – tailored to affine sources – of the GUV construction, generalized to functions over algebraic curves. More specifically, inspired by Ta-Shma and Umans (CCC '12) we develop a two-level evaluation scheme, where we first evaluate a function on a curve at extension-field points, and then evaluate a corresponding affine-linear polynomial to obtain outputs over the base field.

*Tel Aviv University. gil@tauex.tau.ac.il. Supported by ERC starting grant 949499 and by the Israel Science Foundation grant 2989/24.

†Ben Gurion University. deand@bgu.ac.il. Supported in part by NSF-BSF grant 2022644.

‡Ben Gurion University and Tel Aviv University. goldgrab@post.bgu.ac.il. Supported by NSF-BSF grant 2022644.

ISSN 1433-8092

Contents

1 Introduction **1**
1.1 Proof technique 5

2 Preliminaries **9**
2.1 Function fields 11
2.1.1 The Garcia–Stichtenoth tower 13

3 Algebraic-Geometric Parvaresh–Vardy Subspace Designs **16**
3.1 Construction framework 16
3.2 The subspace-design property 17
3.3 Instantiating with the Garcia–Stichtenoth function field 20

4 An Improved, Double-Evaluation Construction **22**
4.1 Subspace designs construction 22
4.2 Evaluation in a function field tower with many degree-d places 25
4.3 Rank condensers and extractors 28
4.4 Strong blocking sets over arbitrary finite fields 30
4.5 Condensers for affine sources 31

A Missing Proofs **40**

1 Introduction

Algebraic pseudorandomness studies algebraic analogues of traditional, combinatorial, pseudorandom objects, wherein the families of tests we wish to fool are characterized by *linear subspaces* rather than arbitrary sets. Often, we seek to efficiently construct a collection of linear subspaces that enjoy random-like properties with respect to an arbitrary linear subspace. Such examples include subspace designs, rank extractors and condensers, and dimension expanders (see [GR08, FS12, GK16, FG15, CI17, GXY18] for a sample of earlier works). Beyond being natural and interesting in their own right, the linear-algebraic pseudorandom objects have found many applications, the earlier of which include, e.g., list decoding [GX12], randomness extractors [GR08], and polynomial identity testing [KS11, FS12].

Very recently, research in linear-algebraic pseudorandomness has regained renewed momentum, with new constructions [GRSZ26, GGH26] and exciting applications. These applications include, most prominently, subspace design codes and new results in list decoding and list recovery [CZ25, BCDZ26, GGH26, GG26]. Other applications include strong blocking sets [GRSZ26], tensor rank [Dvi25], and the breakthrough result of bipartite matching in **NC** [CGG$^+$26] (see also [KS26]).

Subspace Designs. The object this work focuses on is *subspace designs*, first defined by Guruswami and Xing [GX12].

Definition 1.1 (Subspace design)**.** *Let q be a prime power, let $1 \le r \le t \le k$, let $n \ge 1$ be an integer and $A \ge 0$, and let $\mathscr{H} = (H_i)_{i\in[n]}$ be a collection of subspaces of $\mathbb{F}_q^k$, each of codimension at most t. We say that $\mathscr{H}$ is an* (r,A)-weak subspace design *if every r-dimensional subspace $W \le \mathbb{F}_q^k$ satisfies*

$$\left|\{i \in [n] : H_i \cap W \neq \{0\}\}\right| \le A.$$

We say that $\mathscr{H}$ is an (r,A)-strong subspace design *if for every such W we have*

$$\sum_{i=1}^{n} \dim(H_i \cap W) \le A.$$

In either case, we say that the design has codimension t.

Naturally, our goal is to minimize A and maximize n, while keeping t as close to r as possible. In this paper, our primary focus is on strong subspace designs, which we simply refer to as *subspace designs*.

The probabilistic method guarantees the existence of a subspace design with $n = q^{\Omega(t)}$ and

$A = O(rk/t)$ when $t \geq 2r$[1] (see [GK16, Lemma 4]). In the regime $r = t$,[2] the behavior is quite different. There, it yields $n = \Omega(r(k-r)\log^{1/2}(q))$ and $A = (1+o_q(1))r(k-r)$ (see [GRSZ26, Theorem A.1]).

Our goal is to provide *explicit* constructions, meaning we seek an algorithm that outputs such an object in time $\text{poly}(k,q,n,A)$. Similarly, throughout this paper, by *explicit* we mean that the object can be constructed by a deterministic algorithm running in time polynomial in the relevant parameters. We allow the running time to be $\text{poly}(q)$ rather than $\text{poly}(\log q)$ because whenever $q > \text{poly}(k)$, there are already strictly better constructions [GK16] that achieve poly-logarithmic time. We therefore disregard this technicality and simply bound the running time by $\text{poly}(q)$.

When $t \geq 2r$, the first explicit constructions with essentially optimal intersection bounds, due to Guruswami and Kopparty [GK16], require $q > k$. Later, Guruswami, Xing, and Yuan [GXY18] generalized the [GK16] construction to function fields, which provided a construction over every finite field, but with the weaker bound

$$A = O\left(\frac{rk\log_q k}{t-r+1}\right).$$

When $t = O(r)$, the size of this collection is $n = \frac{k}{t}q^{O(1)}$, which again requires q to grow with k in order to provide a non-trivial result. Recently, Goyal, Guruswami and Hsieh [GGH26] used the expander-based Alon-Edmonds-Luby (AEL) framework to construct subspace designs over any finite field with $A = O(rk/t)$, but with $t = \text{poly}(r)\cdot q^{r^2}$.

In this paper, our focus is on the regime $r = t$. Guo, Raj, Shangguan, and Zhang [GRSZ26] recently constructed explicit subspace designs with $A = O(rk)$ and $n \geq q^{1/4}A$, for all non-prime field sizes q such that $q \geq \text{poly}(r)$. For prime fields in this regime, and for smaller field sizes, they obtain subspace designs with larger bounds on A; That is, either multiplied by a super-polynomial factor in r, or by an exponential factor in r, respectively. Hence, their construction achieves the optimal value of A up to a constant, whenever $q \geq \text{poly}(r)$. This is the first construction that achieves near-optimal parameters and field size independent of the ambient-space dimension k, but rather depends only on the dimension of the test subspace r.

The main contribution of this work is a new, explicit construction of strong subspace designs.

Theorem 1.2 (Corollary 4.7, simplified)**.** *Let q be a prime power, let $0 < \gamma < 1$, and let $k \geq 2$. For every $1 \leq r \leq k$, there exists an explicit (r,A) subspace design $\mathscr{H}$ of n subspaces of $\mathbb{F}_q^k$,*

[1] More precisely, this holds for any $t \geq \alpha r$ where $\alpha > 1$.

[2] This is the extremal case, as the sum of the dimensions of a subspace in the collection and the test subspace exactly equals the dimension of the ambient space. Any increase in either dimension trivially forces a non-zero intersection; thus, this is the regime where one expects the largest bound A.

each of codimension at most r, satisfying

$$A = O\left(\frac{q^3 rk}{\gamma^5}\right), \qquad \frac{A}{n} \leq \left(\frac{1}{q} + \gamma\right) r.$$

Moreover, every nonzero subspace $W \leq \mathbb{F}_q^k$ of dimension at most r satisfies

$$\mathbb{E}_{H \in \mathscr{H}} \dim(W \cap H) < \left(\frac{1}{q} + \gamma\right) \dim W.$$

Crucially, our construction applies to arbitrary field sizes while simultaneously achieving $t = r$. Moreover, it achieves the optimal value of A up to a $\mathrm{poly}(q)$ factor, which is simply a constant when q itself is constant. For fields of square size, we further improve this bound to $A = 6rk$ (see Theorem 3.8).

We also consider related linear-algebraic pseudorandom objects, whose constructions follow primarily from our results on subspace designs.

Lossy rank condensers. We first consider *lossy rank condensers*, originally introduced by Forbes, Saptharishi and Shpilka in [FSS14] for applications to read-once algebraic branching programs (though they specifically considered the *lossless* variant; see Definition 1.5). Later, Forbes and Guruswami [FG15] constructed lossy rank condensers via a reduction from the subspace designs of [GK16], and applied them to construct dimension expanders. We begin with the definition.

Definition 1.3 (Lossy rank condenser)**.** *Let q be a prime power, let $1 \leq r \leq t \leq k$, let $n \geq 1$ be an integer, let $\varepsilon, \delta \in [0,1]$, and let $\mathscr{E} = (E_i)_{i \in [n]}$ be a collection of matrices in $\mathbb{F}_q^{t \times k}$. We say that $\mathscr{E}$ is an (r, ε, δ)-*lossy rank condenser *if every rank-r matrix $M \in \mathbb{F}_q^{k \times r}$ satisfies*

$$\left|\{i \in [n] : \mathrm{rank}(E_i M) < (1-\varepsilon) r\}\right| \leq \delta n.$$

In [FG15], lossy rank condensers were defined as the special case $\delta = 1 - 1/n$ of the above definition. In this case, for every rank-r matrix M, at least one matrix E_i satisfies $\mathrm{rank}(E_i M) \geq (1-\varepsilon) r$. We find it more natural to refer to this object as a *lossy rank disperser*.

Our subspace designs yield lossy rank condensers with output dimension $t = r$.

Theorem 1.4 (Corollary 4.8)**.** *Let q be a prime power, and let $\varepsilon, \delta \in (0,1]$ satisfy $q > 1/(\varepsilon\delta)$. For every integers $1 \leq r \leq k$, there exists an explicit (r, ε, δ)-lossy rank condenser $\mathscr{E} = (E_i)_{i \in [n]} \subseteq \mathbb{F}_q^{r \times k}$ of size*

$$n = O\left(\frac{q^3 k}{(\varepsilon\delta - 1/q)^5}\right).$$

The primary feature of this construction is that it works over any constant field size q while maintaining a constant output entropy rate – by choosing a constant $\varepsilon < 1$. Previously, all constructions required either a growing field size (e.g., [FG15, GRSZ26]) or a vanishing output entropy rate (e.g., [GXY18, GGH26]) – that is, the rank of their promised output subspace was sublinear in the dimension of the output space[3]. We refer the reader to Section 4.5, where we also spell out the implications of our result (and previous results) to linear seeded condensers for affine sources, which might be useful from a pseudorandomness perspective.

Lossless rank extractors. A *lossless rank extractor* is simply an $(r, 0, \delta)$ lossy rank condenser in which $r = t$, and therefore retains all the entropy.

Definition 1.5 (Lossless rank extractor)**.** *Let q be a prime power, let $1 \le r \le k$, let $n \ge 1$, and let $\mathscr{E} = (E_i)_{i\in[n]}$ be a collection of matrices in $\mathbb{F}_q^{r\times k}$. For $\delta > 0$, we say that $\mathscr{E}$ is an* (r, δ)-lossless rank extractor *if every rank-r matrix $M \in \mathbb{F}_q^{k\times r}$ satisfies*

$$\left|\{i \in [n] : \operatorname{rank}(E_i M) < r\}\right| \le \delta n.$$

The collection $\mathscr{E}$ is called an r-lossless rank disperser *if for every rank-r matrix $M \in \mathbb{F}_q^{k\times r}$ there exists $i \in [n]$ such that* $\operatorname{rank}(E_i M) = r$.

Observe that to obtain r-lossless rank dispersers over $\mathbb{F}_q$, it suffices to construct a subspace design with $t = r$ such that $A < n$. Any subset of size $A+1$ from this design then yields an r-lossless rank disperser. This observation was used in both [FG15] and [GRSZ26]. The former, which relied on the subspace designs of [GK16], required $q > r(k-r)$. The latter provided the first construction over a field size independent of k, requiring only $q \ge \operatorname{poly}(r)$. Furthermore, for non-prime fields they achieved $A = O(rk)$ for infinitely many $k \ge r$ (or $A = O(qrk)$ for all $k \ge r$), whereas over large prime fields they incurred the weaker bound $A = O(r^{O(\log r)}rk)$. By contrast, our construction improves the field size requirement to $q > r/\delta$ and applies to both prime and non-prime fields, at the cost of increasing A by a $\operatorname{poly}(r, q)$ multiplicative factor.

Theorem 1.6 (Corollary 4.9)**.** *Let $1 \le r \le k$ be integers, and let $0 < \delta < 1$. For every prime power $q > r/\delta$, there exists an explicit (r, δ)-lossless rank extractor $\mathscr{E} = (E_i)_{i\in[n]} \subseteq \mathbb{F}_q^{r\times k}$ of size*

$$n = O\left(\frac{q^3 r^5 k}{(\delta - r/q)^5}\right).$$

In particular, for every prime power $q > r$, there exists an explicit r-lossless rank disperser over $\mathbb{F}_q$ of size $O(r^5 k q^8)$.

[3] An exception is [GUV09], which allows any field and achieves constant entropy, but with significantly larger n.

Strong blocking sets. Introduced by [Ric56], blocking sets are classical objects in finite geometry, that characterize the minimal structure necessary to guarantee large intersection with all subspaces of a given codimension. More formally, for $1 \le s \le k-1$, a strong s-blocking set in $\mathrm{PG}(k-1,q)$ satisfies that its intersection with an arbitrary codimension-s projective subspace, spans this subspace. The challenge is to explicitly construct strong blocking sets of minimal size. As shown in [FS14, FS16], lossless rank dispersers imply strong blocking sets. Applying this reduction to our $(s+1)$-lossless rank dispersers gives, for every prime power $q > s+1$ and every $k \ge s+1$, an explicit strong s-blocking set of size $O(s^5 k q^{s+8})$; see Corollary 4.12. Let c_0 be the absolute constant in [GRSZ26, Corollary 6.2]. When $q < (2s)^{c_0}$, our bound $O\left(kq^s s^{O(1)}\right)$ improves all applicable previous bounds, by an exponential factor. For a prime $(2s)^{c_0} \le q \le \mathrm{poly}(s)$, it improves upon previous results by a quasipolynomial factor in s. We give a detailed discussion, together with the formal definitions and statements, in Section 4.4.

1.1 Proof technique

As in the work of Guruswami, Umans, and Vadhan [GUV09], our subspace designs are based on Parvaresh–Vardy codes. Conceptually, our basic construction can be viewed as (a function field generalization of) the GUV construction, equipped with a linear-algebraic analysis that exploits the affine structure of the sources. In this subsection, we adopt the dual perspective of rank condensers to draw a more direct comparison with their construction.

The GUV construction evaluates low degree polynomials over a finite field, and the seed of the condenser is parametrized by field elements. In the context of rank condensers, this means that each map corresponds to a unique element of the underlying field – and therefore the field size must grow together with other parameters.

To circumvent this, we instead use functions over algebraic curves, with a growing number of points. Combined with our linear-algebraic analysis, this approach yields lossy rank condensers over fields of square size, larger than 49. To extend this result to arbitrary finite fields, we apply a second evaluation step, following a technique from [TSU12]. We now describe these ideas in more detail.

The GUV construction. GUV construct their condenser by evaluating the correlated polynomials of Parvaresh–Vardy codes [PV05]. Let $k \ge 2$ and $1 \le r \le k$, and identify $\mathbb{F}_q^k$ with the space V of polynomials in $\mathbb{F}_q[X]$ of degree less than k. Fix an irreducible polynomial $Q \in \mathbb{F}_q[X]$ of degree k and an integer $h \ge 2$. For $f \in V$ and $0 \le i \le r-1$, define

$$\tau_i(f) = f^{h^i} \bmod Q,$$

considered as a polynomial of degree less than k. In particular, $\tau_0(f) = f$. For an element $a \in \mathbb{F}_q$, the GUV construction is

$$E_a(f) = \big(\tau_0(f)(a), \ldots, \tau_{r-1}(f)(a)\big), \qquad \mathrm{Cond}(f,a) = \big(a, E_a(f)\big).$$

The GUV analysis follows the list-decoding argument for PV codes. Given an output set $T \subseteq \mathbb{F}_q^{r+1}$, we seek to bound, in terms of $|T|$, the size of the list

$$\mathrm{LIST}(T) = \{f \in V : \mathrm{Cond}(f,a) \in T \text{ for every } a \in \mathbb{F}_q\}.$$

We first interpolate a nonzero polynomial $R \in \mathbb{F}_q[X, Y_0, \ldots, Y_{r-1}]$ vanishing on T. For every $f \in \mathrm{LIST}(T)$, we have

$$R\big(a, \tau_0(f)(a), \ldots, \tau_{r-1}(f)(a)\big) = 0 \qquad \text{for every } a \in \mathbb{F}_q.$$

Provided that T is sufficiently small, we can choose the degree bounds on R so that the univariate polynomial $R(X, \tau_0(f), \ldots, \tau_{r-1}(f))$ has degree less than q. Since it vanishes on all q field elements, it is identically zero.

We now view each $f \in V$ as an element of the extension field $\mathbb{F}_q[X]/(Q)$. The relations $\tau_i(f) \equiv f^{h^i} \bmod Q$ imply that every $f \in \mathrm{LIST}(T)$ is a root of

$$R^*(Z) = R(X, Z, Z^h, \ldots, Z^{h^{r-1}}) \bmod Q \in \big(\mathbb{F}_q[X]/(Q)\big)[Z].$$

The monomials in $Y_0, \ldots, Y_{r-1}$ are chosen to become distinct powers of Z, and R can be chosen to remain nonzero modulo Q. Thus, R^* is nonzero, which yields $|\mathrm{LIST}(T)| \le \deg R^*$.

A linear-algebraic analysis. Linear condensers for affine sources can equivalently be viewed as lossy rank condensers (as we explain in Section 4.5). Henceforth, we proceed using the latter formulation. Similarly to [Che10, Corollary 2.23], we instantiate the same construction with $h = q$. With this choice, the maps τ_i and E_a become $\mathbb{F}_q$-linear, and our lossy rank condenser is simply the collection $\{E_a\}_{a \in \mathbb{F}_q}$. We next present our analysis.

Fix an s-dimensional subspace $W \le V$, where $1 \le s \le r$. The rank loss of E_a at W is $s - \dim E_a(W)$. Our goal is to bound the total rank loss over all evaluation points a. We obtain this bound from the determinant of a matrix associated with a basis of W.

Let $\mathscr{B} = (f_1, \ldots, f_s)$ be an $\mathbb{F}_q$-basis of W. We define the *PV-Moore matrix* by

$$M_{\mathscr{B}} = \big(\tau_i(f_j)\big)_{0 \le i \le s-1,\, 1 \le j \le s}. \tag{1.1}$$

Reducing $M_{\mathscr{B}}$ modulo Q gives the Moore matrix of the residue classes of $f_1, \ldots, f_s$, in $\mathbb{F}_q[X]/(Q) \cong \mathbb{F}_{q^k}$. Since reduction modulo Q is injective on V, these classes are linearly independent over $\mathbb{F}_q$. The Moore-matrix criterion therefore implies that $\Delta_{\mathscr{B}} := \det M_{\mathscr{B}}$ is nonzero.

We next relate the rank loss of E_a to the vanishing of $\Delta_{\mathscr{B}}$ there. The matrix $M_{\mathscr{B}}(a)$ represents the first s coordinates of $E_a|_W$, so its kernel has dimension at least $s - \dim E_a(W)$. On the other hand, the dimension of the kernel is at most the multiplicity of a as a root of $\Delta_{\mathscr{B}}$: by multiplying by an invertible matrix with $\mathbb{F}_q$-coefficients, we can obtain $\dim\ker(E_a|_W)$ columns of $M_{\mathscr{B}}$ divisible by $X - a$. Since each entry has degree less than k, the determinant has degree at most $s(k-1)$. Summing over all evaluation points gives

$$\sum_{a \in \mathbb{F}_q} \big(s - \dim E_a(W)\big) \leq s(k-1).$$

This bound is non-trivial only whenever $q \geq k$; consequently, the field size must grow.

Passing to function fields. To keep q fixed while increasing the number of evaluation points, we pass to function fields. This extension of the Parvaresh–Vardy framework was previously studied by Guruswami [Gur05] in the context of list decoding. Consequently, his analysis relies on polynomial interpolation, and is similar to the later GUV analysis presented above. The idea is to replace low-degree polynomials, which are evaluated over elements in $\mathbb{F}_q$, with a space of "low-degree" functions over an algebraic curve, which can be evaluated over the curve points. In our rank condensers setting, by taking curves with many evaluation points relative to their "complexity" – measured by their *genus* – we are able to increase the number of evaluation points, and hence the number of linear transformations, without increasing the field size. We provide the formal definitions in Section 2.1.

Let $1 \leq r \leq k$, and let $F/\mathbb{F}_q$ be a function field of genus $g \leq k$ with N rational places (i.e., curve points), plus an additional rational place P_∞. We identify $\mathbb{F}_q^k$ with $V = \mathscr{L}(dP_\infty)$, where $d = k + g - 1$ – that is, the space of functions of "degree" at most d. By the Riemann–Roch theorem, it has dimension k. Analogous to the choice of an irreducible polynomial of degree k, choose a *place* Q of degree $m = d + 1$.[4] Since $m > d$, the residue map π_Q (i.e., reducing a function "mod Q") is injective on V, so each function $f \in V$ is uniquely represented by an element of $\mathbb{F}_{q^m}$.

To define the correlated functions $\tau_i(f)$, we lift powers of $\pi_Q(f)$ back to functions in F. These powers need not correspond to functions in V, so we allow the lifts to have slightly larger "degree". Following [Gur05], we use the Riemann–Roch theorem to choose these lifts linearly over $\mathbb{F}_q$, with "degree" at most $\widetilde{d} = m + 2g - 1 < 6k$. Taking $\tau_0(f) = f$, the resulting maps satisfy

$$\tau_i(f) = f^{q^i} \mod Q \qquad (0 \leq i \leq r-1).$$

Thus, the functions $\tau_i(f)$ satisfy the same relations modulo Q as in the polynomial construction.

[4] More precisely, m is chosen to be a prime number between d and $2d$, which allows us to find such a place explicitly (see Proposition 3.7). For the sake of simplicity, we omit this technicality here.

Let $\mathscr{P}$ denote the N rational evaluation places. Evaluating the functions $\tau_i(f)$ at each $P \in \mathscr{P}$ gives maps $E_P \colon V \to \mathbb{F}_q^r$ as before. The same determinant argument now applies. For an s-dimensional subspace $W \leq V$, where $1 \leq s \leq r$, the PV-Moore matrix of a basis $\mathscr{B}$ of W, defined similarly to Equation (1.1), reduces to a nonsingular Moore matrix modulo Q, so its determinant $\Delta_{\mathscr{B}}$ is nonzero. This determinant has "degree" at most $d + (s-1)\widetilde{d}$, and hence at most that many rational zeros, counted with multiplicity. As before, the rank loss of E_P is bounded by the multiplicity of P as a zero of $\Delta_{\mathscr{B}}$. Thus,

$$\sum_{P \in \mathscr{P}} \big(s - \dim E_P(W)\big) \leq d + (s-1)\widetilde{d} < 6sk,$$

see Proposition 3.6.

To make the construction explicit, we must find Q efficiently; we accomplish this for the Garcia–Stichtenoth tower in Proposition 3.7.

This tower has many rational places relative to its genus. Evaluating it in the above construction gives, for every square q and infinitely many k, an explicit collection of $n = N$ linear maps satisfying

$$n \geq (\sqrt{q}-1)k, \qquad \frac{1}{n} \sum_{P \in \mathscr{P}} \big(s - \dim E_P(W)\big) < \frac{6s}{\sqrt{q}-1};$$

see Theorem 3.8. These maps construct an $(r, 6rk)$ subspace design of size n, or dually, an (r, ε, δ)-lossy rank condenser provided that $6/(\sqrt{q}-1) \leq \varepsilon\delta$.

Two restrictions remain. The tower used in this instantiation requires q to be a square, and the estimate above is non-trivial only whenever $q > 49$. We next modify the construction to overcome both restrictions.

Two evaluations over arbitrary finite fields. To relax the requirement $6/(\sqrt{q}-1) \leq \varepsilon\delta$, we seek a better ratio A/n between the number of evaluation maps and the bound on their total rank loss. For this, we want more evaluation places. Places of higher degree can be much more abundant than rational places, so we consider evaluating the functions $\tau_i(f)$ at places P of degree $\ell \geq 2$. The resulting maps are $E_P \colon V \to \mathbb{F}_{q^\ell}^r$. However, representing these outputs over $\mathbb{F}_q$ gives output dimension $t = \ell r$, whereas we want $t = r$. To retain this output dimension, we adapt an idea of Ta-Shma and Umans [TSU12] and apply a second polynomial evaluation: we view each output coordinate as a low-degree polynomial over $\mathbb{F}_q$ and evaluate it at a point over $\mathbb{F}_q$. We now describe the choice of places and polynomials for these two steps.

For the first evaluation, we seek for a tower of function fields over $\mathbb{F}_q$ with many degree-ℓ places. We obtain it from the Garcia–Stichtenoth tower over $\mathbb{F}_{q^\ell}$; its defining equations have coefficients in $\mathbb{F}_q$, and hence can be considered directly over $\mathbb{F}_q$. We refer to this tower as the

ℓ-descended GS tower. In Proposition 4.5, we show that this tower has many degree-ℓ places (relative to its genus). More precisely, it contains N degree-ℓ places satisfying

$$N \geq \frac{q^{\ell/2}-1}{2\ell}\, g.$$

Moreover, we show that the required function spaces, evaluation places and the large-degree place Q can also be computed efficiently. By restricting ℓ to be an even integer, we guarantee that q^ℓ is a perfect square regardless of q. This bypasses the previous requirement that the base field itself be of square order.

For the second evaluation, we identify $\mathbb{F}_{q^\ell}$ with $\mathbb{F}_q^\ell$, and view each vector $b = (b_0, \ldots, b_{\ell-1})$ as the affine-linear polynomial

$$g_b(X) = b_0 + \sum_{j=1}^{\ell-1} b_j X_j.$$

Here $X = (X_1, \ldots, X_{\ell-1})$. For each $a \in \mathbb{F}_q^{\ell-1}$, we evaluate the polynomials representing all coordinates of $E_P(f)$ at the same point a. This gives an $\mathbb{F}_q$-linear map $E_{P,a} \colon V \to \mathbb{F}_q^r$, and hence a collection of $n = Nq^{\ell-1}$ maps. Using linear multivariate polynomials rather than univariate polynomials of degree $< \ell$, minimizes the degree of each polynomial, although at the cost of additional evaluation points. In our parameter regime of small q and ℓ, an overhead of $q^{\ell-1}$ evaluation points is sufficiently small, making this trade-off attractive.

In Theorem 4.6, we show that, for every prime power q, every even $\ell \geq 2$ and every $1 \leq r \leq k$, this construction gives an explicit (r, A)-subspace design, where

$$A = \left(\frac{1}{q} + O(q^{-\ell/2})\right) rn,$$
$$n \leq q^{O(\ell)} \cdot k.$$

Dually, we obtain an (r, ε, δ)-lossy rank condenser of size n, provided that $\frac{1}{q} + O(q^{-\ell/2}) \leq \varepsilon\delta$. The bound on the average relative rank loss approaches $1/q$ as ℓ grows.

For any $0 < \gamma < 1$, we can therefore choose an even integer ℓ such that the average rank loss is less than $(1/q + \gamma)r$, yielding a collection of $n = O(q^3 k/\gamma^5)$ maps. These maps constitute an (r, ε, δ)-lossy rank condenser provided that $1/q + \gamma \leq \varepsilon\delta$. Consequently, the construction applies to every finite field, including $\mathbb{F}_2$; see Corollary 4.8.

2 Preliminaries

Throughout, $\mathbb{F}$ denotes an arbitrary field, and $\mathbb{F}_q$ denotes the finite field with q elements. We write $\log = \log_2$ unless a different base is specified. We view a matrix $E \in \mathbb{F}^{t \times k}$ as the linear map $x \mapsto Ex$ from $\mathbb{F}^k$ to $\mathbb{F}^t$, and use $\mathrm{rank}(E)$ and $\ker(E)$ for its rank and kernel, respectively.

We will use the following form of the reduction of Forbes and Guruswami [FG15, Proposition 6.7] from strong subspace designs to lossy rank condensers. A similar strengthening was also used recently in [DG26]. We include the proof here for completeness.

Proposition 2.1 (Strong subspace designs as lossy rank condensers)**.** *Let $\mathbb{F}$ be a field, let $1 \le r \le t \le k$, let $n \ge 1$ and $A \ge 0$ be integers, and let $\varepsilon, \delta \in [0,1]$. Let $\mathscr{H} = (H_i)_{i\in[n]}$ be an (r,A)-strong subspace design in $\mathbb{F}^k$ of size n and codimension t. For every $i \in [n]$, let $E_i \in \mathbb{F}^{t\times k}$ satisfy $\ker(E_i) = H_i$, and set $\mathscr{E} = (E_i)_{i\in[n]}$. If*

$$A < \big(\lfloor \delta n \rfloor + 1\big)\big(\lfloor \varepsilon r \rfloor + 1\big),$$

then $\mathscr{E}$ is an (r,ε,δ)-lossy rank condenser.

Proof. Fix a rank-r matrix $M \in \mathbb{F}^{k\times r}$, and let $W \le \mathbb{F}^k$ be its column space. The columns of M form a basis of W. Thus, for every $i \in [n]$, the matrix E_iM represents the restriction of E_i to W. We have

$$\operatorname{rank}(E_iM) = r - \dim_{\mathbb{F}}(W \cap H_i).$$

Let

$$\mathscr{B} = \{i \in [n] : \operatorname{rank}(E_iM) < (1-\varepsilon)r\}$$

be the set of bad indices. For every $i \in \mathscr{B}$, we have

$$\dim_{\mathbb{F}}(W \cap H_i) \ge \lfloor \varepsilon r \rfloor + 1.$$

The strong subspace design property therefore implies

$$A \ge \sum_{i=1}^{n} \dim_{\mathbb{F}}(W \cap H_i) \ge |\mathscr{B}|\big(\lfloor \varepsilon r \rfloor + 1\big).$$

The assumed bound on A now gives

$$|\mathscr{B}| \le \lfloor \delta n \rfloor.$$

Thus, at most δn indices are bad, as needed. □

Remark 2.2. *For $\delta = 1 - 1/n$, the hypothesis in the proposition becomes*

$$n > \frac{A}{\lfloor \varepsilon r \rfloor + 1},$$

which recovers [FG15, Proposition 6.7].

For $0 \ne f \in \mathbb{F}[X]$ and $a \in \mathbb{F}^t$, let $\operatorname{mult}_a(f)$ be the least total degree of a nonzero monomial in $f(a+Y)$. We make use of a variant of the Schwartz–Zippel lemma due to Dvir et al. [DKSS13, Lemma 8], which bounds the number of zeroes with multiplicity.

Lemma 2.3 (Multiplicity Schwartz–Zippel bound)**.** *Let $t \geq 1$, let S be a finite subset of a field $\mathbb{F}$, and let $0 \neq f \in \mathbb{F}[X_1, \ldots, X_t]$ have total degree at most D. Then*

$$\sum_{a \in S^t} \mathrm{mult}_a(f) \leq D|S|^{t-1}.$$

We will use the existence of prime numbers in large enough intervals, as guaranteed by Bertrand's postulate.

Fact 2.4 (Bertrand's postulate)**.** *For every integer $n > 1$, there exists a prime p such that $n < p < 2n$.*

2.1 Function fields

We assume familiarity with the basic theory of algebraic function fields, such as places, valuations, extensions, etc. A detailed exposition can be found in [Sti09]. We briefly recall the relevant definitions and results.

Algebraic function fields, valuations, and places. Let x be an indeterminate over $\mathbb{F}_q$. The rational function field $\mathbb{F}_q(x)$ consists of the rational functions in x with coefficients in $\mathbb{F}_q$. An algebraic function field $F/\mathbb{F}_q$ is a finite algebraic extension of $\mathbb{F}_q(x)$, and its elements are called functions. Throughout, we assume that $\mathbb{F}_q$ is the full constant field of F; that is, every element of F that is algebraic over $\mathbb{F}_q$ belongs to $\mathbb{F}_q$.

A discrete valuation on F is a map $v\colon F^\times \to \mathbb{Z}$ satisfying

$$v(fg) = v(f) + v(g) \qquad \text{and} \qquad v(f+g) \geq \min\{v(f), v(g)\},$$

and we extend it to F by setting $v(0) = \infty$. We consider valuations that are trivial on $\mathbb{F}_q^\times$ and normalized, meaning that $v(F^\times) = \mathbb{Z}$. Associated with such a valuation are its valuation ring, maximal ideal, and residue field,

$$\mathcal{O}_v = \{f \in F : v(f) \geq 0\}, \qquad \mathfrak{m}_v = \{f \in F : v(f) > 0\}, \qquad \kappa(v) = \mathcal{O}_v/\mathfrak{m}_v,$$

respectively. A place P of F is the maximal ideal associated with a normalized discrete valuation. We write v_P, $\mathcal{O}_P$, and $\mathfrak{m}_P$ for the corresponding valuation, valuation ring, and maximal ideal, and we write $\kappa(P) = \mathcal{O}_P/\mathfrak{m}_P$ for the residue field.

The degree of a place P is

$$\deg P = [\kappa(P) : \mathbb{F}_q].$$

For $f \in \mathcal{O}_P$, we denote the residue class of f modulo $\mathfrak{m}_P$ by $f(P) \in \kappa(P)$. A place of degree one is called *rational*; for a rational place P, we have $\kappa(P) = \mathbb{F}_q$ and thus $f(P) \in \mathbb{F}_q$.

Divisors, principal divisors, and pole divisors. A divisor of F is a finite formal sum

$$D = \sum_P n_P P, \qquad n_P \in \mathbb{Z}.$$

Its support and degree are

$$\operatorname{supp}(D) = \{P : n_P \neq 0\}, \qquad \deg D = \sum_P n_P \deg P.$$

For divisors D_1 and D_2, we write $D_1 \geq D_2$ if the coefficient of every place in D_1 is at least the corresponding coefficient in D_2. A divisor D is effective if $D \geq 0$.

Every nonzero function $f \in F^\times$ determines a divisor

$$(f) = \sum_P v_P(f) P.$$

The divisor (f) is called the principal divisor of f. Its zero divisor and pole divisor are, respectively,

$$(f)_0 = \sum_{P : v_P(f) > 0} v_P(f) P, \qquad (f)_\infty = \sum_{P : v_P(f) < 0} -v_P(f) P.$$

Thus, $(f) = (f)_0 - (f)_\infty$. We will repeatedly use the following standard fact about principal divisors.

Lemma 2.5 (Degree of a principal divisor)**.** *For every $f \in F^\times$,*

$$\deg((f)) = 0 \qquad \textit{and hence} \qquad \deg((f)_0) = \deg((f)_\infty).$$

Riemann–Roch spaces and the genus. For a divisor D, its Riemann–Roch space is

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

This is a finite-dimensional $\mathbb{F}_q$-vector space, and we write $\ell(D) = \dim_{\mathbb{F}_q} \mathscr{L}(D)$. Thus, $\ell(D)$ measures the number of linearly independent functions whose poles are bounded by D. A direct corollary of Lemma 2.5 is the following lemma.

Lemma 2.6 (Negative-degree divisors)**.** *If D is a divisor of F with $\deg D < 0$, then*

$$\mathscr{L}(D) = \{0\}.$$

Theorem 2.7 (Riemann–Roch)**.** *For every function field $F/\mathbb{F}_q$, there exists a unique nonnegative integer $g = g(F)$ such that*

$$\ell(D) \geq \deg D - g + 1$$

for every divisor D of F, with equality whenever $\deg D \geq 2g - 1$. The integer g is called the genus of F.

Bounds on the number of rational places. The Hasse–Weil theorem bounds the number of rational places in terms of the genus and the size of the constant field.

Theorem 2.8 (Hasse–Weil)**.** *Let $F/\mathbb{F}_q$ be a function field of genus g. Then*

$$\left|N(F)-(q+1)\right| \leq 2g\sqrt{q}.$$

We will also use a consequence of the Hasse–Weil theorem for places of higher degree.

Corollary 2.9 (Number of degree-r places)**.** *Let $F/\mathbb{F}_q$ be a function field of genus g, let $r \geq 1$, and let $B_r = B_r(F)$ denote the number of places of F of degree r. Then,*

$$\left|B_r - \frac{q^r}{r}\right| < (2+7g)\cdot\frac{q^{r/2}}{r}.$$

Thus, for a fixed field $\mathbb{F}_q$, the number of rational places grows at most linearly with the genus. To describe the best possible asymptotic ratio, we use Ihara's constant.

Definition 2.10 (Ihara's constant)**.** *For every prime power q, let*

$$N_q(g) = \max\{N(F) : F/\mathbb{F}_q \text{ is a function field of genus } g\}$$

and define

$$A(q) = \limsup_{g\to\infty}\frac{N_q(g)}{g}.$$

The quantity $A(q)$ is called Ihara's constant.

Theorem 2.11 (Drinfeld–Vladut bound)**.** *For every prime power q,*

$$A(q) \leq \sqrt{q}-1.$$

2.1.1 The Garcia–Stichtenoth tower

When q is a square, the Drinfeld–Vladut bound is attained by the Garcia-Stichtenoth tower of function fields. A detailed exposition of this tower can be found in [GS95]. We briefly recall the relevant definitions and results.

Definition 2.12 (Garcia–Stichtenoth tower)**.** *Let $\mathbb{F}_q$ be a finite field of size $q = \ell^2$, where ℓ is a prime power. The* Garcia–Stichtenoth tower *is the sequence of function fields*

$$F_1 \subseteq F_2 \subseteq \cdots$$

defined recursively by

$$F_1 = \mathbb{F}_q(x_1),$$

and for every $i \geq 1$,

$$F_{i+1} = F_i(x_{i+1}),$$

where the new variable x_{i+1} *satisfies the equation*

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

The following theorem records the parameters of this tower that we use in the construction.

Theorem 2.13 (The Garcia–Stichtenoth tower)**.** *Let* $(F_i)_{i\geq 1}$ *be the Garcia–Stichtenoth tower over* $\mathbb{F}_q$*, where* $q = \ell^2$*. For* $i \geq 1$*, let* $N_i = N(F_i)$ *and* $g_i = g(F_i)$*. Then*

$$[F_i : F_1] = \ell^{i-1}, \qquad N_i \geq \ell^i(\ell-1)+1,$$

and

$$g_i = \begin{cases} \left(\ell^{i/2}-1\right)^2, & \text{if } i \text{ is even,} \\ \left(\ell^{(i+1)/2}-1\right)\left(\ell^{(i-1)/2}-1\right), & \text{if } i \text{ is odd.} \end{cases}$$

In particular, $g_i \leq \ell^i$ *and*

$$\limsup_{i\to\infty} \frac{N_i}{g_i} \geq \ell - 1 = \sqrt{q} - 1.$$

We record two further features of the tower that will be useful later.

Rational places. At every level, let P_∞ denote the unique place above the pole of x_1 in F_1. This place is rational and totally ramified throughout the tower. For each $\alpha_1 \in \mathbb{F}_q$ satisfying $\alpha_1^{\ell} + \alpha_1 \neq 0$, the zero of $x_1 - \alpha_1$ in F_1 splits completely in F_i. Indeed, these places may be represented by the tuples $(\alpha_1, \ldots, \alpha_i) \in \mathbb{F}_q^i$ such that $\alpha_1^{\ell} + \alpha_1 \neq 0$ and

$$\alpha_{j+1}^{\ell} + \alpha_{j+1} = \frac{\alpha_j^{\ell}}{\alpha_j^{\ell-1}+1} \qquad (1 \leq j < i).$$

There are $q - \ell$ possible values of α_1 and ℓ choices for each subsequent coordinate. We denote the set of these places by $\mathscr{R}_i$. We have

$$|\mathscr{R}_i| = \ell^i(\ell-1). \tag{2.1}$$

Together with P_∞, these places give the lower bound on N_i in Theorem 2.13.

Riemann–Roch spaces. For $i \geq 2$, define

$$h_j = x_j^{\ell-1} + 1, \qquad \pi_j = h_1 h_2 \cdots h_j \qquad (1 \leq j < i).$$

Every function in F_i whose poles are supported at P_∞ admits an expression of the form

$$\sum_{\nu_2=0}^{\ell-1} \cdots \sum_{\nu_i=0}^{\ell-1} p_\nu(x_1) \frac{x_2^{\nu_2} x_3^{\nu_3} \cdots x_i^{\nu_i}}{\pi_1 \pi_2 \cdots \pi_{i-1}}, \qquad p_\nu \in \mathbb{F}_q[x_1].$$

Moreover, the algorithm of Shum et al. [SAK+01] computes an explicit $\mathbb{F}_q$-basis of $\mathscr{L}(\mu P_\infty)$ in this form in time $\mathrm{poly}(\log q, g_i, \mu)$.

For every $P \in \mathscr{R}_i$, all the values $h_j(P)$ and $\pi_j(P)$ are nonzero. Hence the basis functions, and therefore every element of $\mathscr{L}(\mu P_\infty)$ given in this basis, can be evaluated at the places in $\mathscr{R}_i$ by substituting their coordinate tuples. In particular, these evaluations can be computed in time $\mathrm{poly}(\log q, \mu, N_i)$.

Constant-field extensions and places of higher degree. Let $F/\mathbb{F}_q$ be a function field with full constant field $\mathbb{F}_q$. For an integer $a \geq 1$, we write

$$F^{(a)} = F \cdot \mathbb{F}_{q^a}$$

for its constant-field extension to $\mathbb{F}_{q^a}$. The following lemma relates the rational places of $F^{(a)}$ to the places of F.

Lemma 2.14 (Places under a constant-field extension)**.** *The function field $F^{(a)}/\mathbb{F}_{q^a}$ has the same genus as $F/\mathbb{F}_q$. Moreover, a place of F of degree d splits in $F^{(a)}$ into $\gcd(d,a)$ places, each of degree $d/\gcd(d,a)$. Consequently,*

$$N\big(F^{(a)}\big) = \sum_{d \mid a} d B_d(F). \tag{2.2}$$

In Section 4 we apply the lemma to a Garcia–Stichtenoth tower over constant field extensions to obtain a family of function fields with many places of a given degree.

We finally record a local linear-algebra estimate used in the constructions.

Lemma 2.15 (Kernel dimension and determinant valuation)**.** *Let P be a place of a function field $F/\mathbb{F}_q$, and let $A \in \mathscr{O}_P^{s\times s}$ have nonzero determinant. Denote the reduction of A modulo P coordinate-wise by $A(P) \in \kappa(P)^{s\times s}$. Then*

$$\dim_{\kappa(P)} \ker A(P) \leq v_P(\det A).$$

Proof. Set $u = \dim_{\kappa(P)} \ker A(P)$. Choose $\overline{C} \in \mathrm{GL}_s(\kappa(P))$ whose first u columns form a basis of $\ker A(P)$, and lift $\overline{C}$ to a matrix $C \in \mathscr{O}_P^{s\times s}$. The reduction of $\det C$ modulo P is $\det \overline{C} \neq 0$, so $\det C$ is a unit in $\mathscr{O}_P$. Hence

$$v_P(\det(AC)) = v_P(\det A).$$

The first u columns of AC vanish modulo P. Every term in the Leibniz formula for $\det(AC)$ therefore has valuation at least u, and hence $v_P(\det A) \geq u$. □

3 Algebraic-Geometric Parvaresh–Vardy Subspace Designs

3.1 Construction framework

Let $F/\mathbb{F}_q$ be a function field with full constant field $\mathbb{F}_q$, genus g, and N rational places. Fix integers $1 \leq r \leq k$, and assume that $g \leq k$. Set

$$d = k + g - 1.$$

Suppose that F contains a rational place P_∞ and a place $Q \neq P_\infty$ of degree m, where $d < m < 2d$.

Let $V = \mathscr{L}(dP_\infty)$. Since $d \geq 2g-1$, the Riemann–Roch theorem gives

$$\dim_{\mathbb{F}_q} V = d + 1 - g = k.$$

Write $\kappa(Q) = \mathscr{O}_Q/\mathfrak{m}_Q \cong \mathbb{F}_{q^m}$ for the residue field of Q, and let $\pi_Q \colon \mathscr{O}_Q \to \kappa(Q)$ be the residue map. Its restriction to V is injective, since

$$\ker(\pi_Q|_V) = \mathscr{L}(dP_\infty - Q) = \{0\},$$

by $\deg(dP_\infty - Q) = d - m < 0$. This map is not necessarily surjective, so we now lift it to a larger space.

Let $\widetilde{d} = m + 2g - 1$, and consider the space

$$\widetilde{V} = \mathscr{L}(\widetilde{d}P_\infty).$$

The restriction of π_Q to $\widetilde{V}$ *is* surjective. Indeed, its kernel is $\mathscr{L}(\widetilde{d}P_\infty - Q)$. Since $\deg(\widetilde{d}P_\infty - Q) = 2g-1$, the Riemann–Roch theorem gives

$$\begin{aligned}\dim_{\mathbb{F}_q} \widetilde{V} &= m + g,\\ \dim_{\mathbb{F}_q} \ker(\pi_Q|_{\widetilde{V}}) &= g.\end{aligned}$$

Thus, the image has dimension $m = \deg Q = \dim_{\mathbb{F}_q} \kappa(Q)$. Fix an $\mathbb{F}_q$-linear right inverse

$$I \colon \kappa(Q) \longrightarrow \widetilde{V} \qquad \text{such that} \qquad \pi_Q \circ I = \mathrm{id}_{\kappa(Q)}.$$

For every $0 \le i \le r-1$, define an $\mathbb{F}_q$-linear map $\tau_i \colon V \to \widetilde{V}$ by

$$\tau_0(f) = f, \qquad \tau_i(f) = I\big(\pi_Q(f)^{q^i}\big) \quad \text{for } i \ge 1.$$

These maps satisfy

$$\pi_Q(\tau_i(f)) = \pi_Q(f)^{q^i}, \tag{3.1}$$

for every $f \in V$ and $0 \le i \le r-1$.

Definition 3.1 (AGPV subspace design)**.** *Let $F/\mathbb{F}_q$ be a function field as above. Let $\mathscr{P}$ be a set of rational places of F different from P_∞. The functions in $\widetilde{V}$ are regular at every place in $\mathscr{P}$. Thus, for each $P \in \mathscr{P}$, we may define the $\mathbb{F}_q$-linear map*

$$E_P \colon V \longrightarrow \mathbb{F}_q^r, \qquad E_P(f) = \big(\tau_0(f)(P), \ldots, \tau_{r-1}(f)(P)\big),$$

and let

$$H_P = \ker E_P \le V.$$

Each H_P has codimension at most r in V. We define the indexed collection

$$\mathscr{H} = \mathscr{H}(F, \mathscr{P}, P_\infty, Q, k, r) = (H_P)_{P \in \mathscr{P}},$$

which has size $n = |\mathscr{P}|$.

3.2 The subspace-design property

In the following part, we show that the collection $\mathscr{H}$ is a strong subspace design.

In our analysis, we will make use of a generalization of the Moore Matrix, presented by E.H. Moore [Moo96].

Definition 3.2 (Moore Matrix)**.** *Let $F/\mathbb{F}_q$ be a field extension. Let $a_1, \ldots, a_s$ be elements of F. Their associated* Moore matrix *is defined as*

$$M(a_1, \ldots, a_s) = \begin{pmatrix} a_1 & a_2 & \cdots & a_s \\ a_1^q & a_2^q & \cdots & a_s^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{s-1}} & a_2^{q^{s-1}} & \cdots & a_s^{q^{s-1}} \end{pmatrix} \in F^{s \times s}.$$

A standard fact is that the elements $a_1, \ldots, a_s$ are linearly independent over $\mathbb{F}_q$ if and only if $M(a_1, \ldots, a_s)$ is invertible over F. The following definition generalizes the Moore matrix to the lifted Frobenius maps τ_i.

Definition 3.3 (PV-Moore matrix)**.** *Let $1 \le s \le r$, and let $\mathscr{B} = (f_1, \dots, f_s)$ be an ordered tuple of elements of V as defined above. We define its* Parvaresh–Vardy Moore (PV-Moore) matrix *by*

$$M_{\mathscr{B}} = \begin{pmatrix} \tau_0(f_1) & \cdots & \tau_0(f_s) \\ \tau_1(f_1) & \cdots & \tau_1(f_s) \\ \vdots & \ddots & \vdots \\ \tau_{s-1}(f_1) & \cdots & \tau_{s-1}(f_s) \end{pmatrix} \in F^{s \times s}.$$

The usual Moore-matrix criterion remains valid for the lifted Frobenius maps. We include the proof here for completeness.

Proposition 3.4. *Let $1 \le s \le r$, and let $\mathscr{B} = (f_1, \dots, f_s)$ be an ordered tuple of elements of V. Then $\mathscr{B}$ is linearly independent over $\mathbb{F}_q$ if and only if $M_{\mathscr{B}}$ is invertible over F.*

Proof. If $\mathscr{B}$ is linearly dependent over $\mathbb{F}_q$, then the $\mathbb{F}_q$-linearity of the maps τ_i gives a nontrivial linear dependence among the columns of $M_{\mathscr{B}}$.

Conversely, suppose that $\mathscr{B}$ is linearly independent over $\mathbb{F}_q$. Since π_Q is injective on V, the elements

$$\alpha_j = \pi_Q(f_j), \qquad 1 \le j \le s,$$

are linearly independent over $\mathbb{F}_q$. By Equation (3.1), reducing $M_{\mathscr{B}}$ modulo Q gives the Moore matrix

$$M_{\mathscr{B}}(Q) := \left(\alpha_j^{q^i}\right)_{0 \le i \le s-1, 1 \le j \le s} \in \kappa(Q)^{s \times s}.$$

If this matrix were singular, there would exist $a_0, \dots, a_{s-1} \in \kappa(Q)$, not all zero, such that the nonzero $\mathbb{F}_q$-linear polynomial

$$L(X) = \sum_{i=0}^{s-1} a_i X^{q^i}$$

vanishes at every α_j. It would then vanish on their $\mathbb{F}_q$-span, which has q^s distinct elements. This is impossible because $\deg L \le q^{s-1}$. Hence $M_{\mathscr{B}}(Q)$ is invertible, which implies that $M_{\mathscr{B}}$ is invertible. □

Next, we show that the dimension of the intersection of a subspace $W \le V$ with H_P is closely related to the determinant of the PV-Moore matrix of a basis of W.

Lemma 3.5. *Let $W \le V$ be a subspace of dimension s, where $1 \le s \le r$, and let $\mathscr{B} = (f_1, \dots, f_s)$ be an $\mathbb{F}_q$-basis of W. Then, for every $P \in \mathscr{P}$,*

$$\dim_{\mathbb{F}_q}(W \cap H_P) \le v_P(\det M_{\mathscr{B}}).$$

Proof. Evaluating the entries of $M_{\mathscr{B}}$ at P gives

$$M_{\mathscr{B}}(P) = \big(\tau_i(f_j)(P)\big)_{0\le i\le s-1,\,1\le j\le s} \in \mathbb{F}_q^{s\times s}.$$

Every $f \in W$ can be written uniquely as

$$f = \sum_{j=1}^{s} c_j f_j, \qquad c_j \in \mathbb{F}_q.$$

Since the maps τ_i are $\mathbb{F}_q$-linear, $f \in W \cap H_P$ implies

$$M_{\mathscr{B}}(P)(c_1,\dots,c_s)^T = 0.$$

Consequently,

$$\dim_{\mathbb{F}_q}(W \cap H_P) \le \dim_{\mathbb{F}_q} \ker M_{\mathscr{B}}(P).$$

The matrix $M_{\mathscr{B}}$ has entries in $\mathscr{O}_P$, and its determinant is nonzero by Proposition 3.4. The result now follows from Lemma 2.15. □

We are ready to prove that $\mathscr{H}$ is a strong subspace design.

Proposition 3.6. *For every subspace $W \le V$ of dimension $1 \le s \le r$,*

$$\sum_{P\in\mathscr{P}} \dim_{\mathbb{F}_q}(W \cap H_P) \le d + (s-1)\widetilde{d} \le s\widetilde{d}.$$

Consequently, $\mathscr{H}$ is an $(r, d+(r-1)\widetilde{d})$-strong subspace design of size $|\mathscr{P}|$ whose members have codimension at most r. In particular, $\mathscr{H}$ is an $(r, 6rk)$-strong subspace design.

Proof. Fix a subspace $W \le V$ of dimension $1 \le s \le r$, and let $\mathscr{B}$ be an $\mathbb{F}_q$-basis of W. By Proposition 3.4, the determinant of $M_{\mathscr{B}}$ is nonzero. The entries in its first row belong to $\mathscr{L}(dP_\infty)$, whereas the entries in each of the remaining $s-1$ rows belong to $\mathscr{L}(\widetilde{d}P_\infty)$. Therefore

$$0 \ne \det M_{\mathscr{B}} \in \mathscr{L}((d+(s-1)\widetilde{d})P_\infty).$$

Together with Lemma 3.5, we obtain

$$\begin{aligned}\sum_{P\in\mathscr{P}} \dim_{\mathbb{F}_q}(W \cap H_P) &\le \sum_{P\in\mathscr{P}} v_P(\det M_{\mathscr{B}}) \\ &\le \deg((\det M_{\mathscr{B}})_0) \\ &= \deg((\det M_{\mathscr{B}})_\infty) \\ &\le d + (s-1)\widetilde{d}.\end{aligned}$$

Since $d \le \widetilde{d}$, the latter quantity is at most $s\widetilde{d}$. Together,

$$\widetilde{d} = m + 2g - 1 < 2d + 2g - 1 = 2k + 4g - 3 < 6k,$$

which gives the final assertion. □

3.3 Instantiating with the Garcia–Stichtenoth function field

Recall that our construction requires explicitly finding a place Q of degree m satisfying $d < m < 2d$. The following proposition guarantees the existence and efficient construction of such a place for our instantiation.

Proposition 3.7 (Explicit place of prime degree)**.** *Let q be a prime power, let $\ell \geq 1$, and suppose that $q^\ell = r^2$ for a prime power r. Let $F_i/\mathbb{F}_q$ be the i'th field in the ℓ-descended Garcia–Stichtenoth tower, defined by*

$$F_1 = \mathbb{F}_q(x_1), \qquad F_{j+1} = F_j(x_{j+1}), \qquad x_{j+1}^r + x_{j+1} = \frac{x_j^r}{x_j^{r-1}+1} \qquad (j \geq 1),$$

and suppose that F_i has genus $g \geq 2$. Given a prime number m with $2g-1 < m \leq 2(2g-1)$, there is a deterministic $\mathrm{poly}(q,\ell,g)$-time algorithm that outputs an explicit representation $K \cong \mathbb{F}_{q^m}$ and elements $a_1,\ldots,a_i \in K$ such that the evaluation $x_j \mapsto a_j$ represents a degree-m place Q of $F_i/\mathbb{F}_q$. In particular, the residue map at Q is explicit.

Proof. Suppose first that $\mathbb{F}_q$ has odd characteristic. Fix such a prime m, and write

$$\phi(X) = \frac{X^r}{X^{r-1}+1}.$$

Write $q = p^e$ and $r = p^s$, so that $e\ell = 2s$. After extending the constant field to $\mathbb{F}_{q^\ell} = \mathbb{F}_{r^2}$, the tower is the Garcia–Stichtenoth tower of Definition 2.12. Its genus is g, and Theorem 2.13 gives

$$g \geq (r-1)^2 \geq s.$$

Since m is an odd prime and $m > 2g-1 \geq 2s-1$, we have $m > 2s \geq e$. Consequently,

$$\gcd(m,s) = \gcd(m,e) = 1.$$

Using Shoup's algorithm [Sho90], deterministically construct an irreducible polynomial $h \in \mathbb{F}_p[T]$ of degree m. Since $\gcd(m,e) = 1$, h remains irreducible over $\mathbb{F}_q$. We may therefore set

$$L = \mathbb{F}_p[T]/(h), \qquad K = \mathbb{F}_q[T]/(h),$$

and let $u = T + (h) \in L$, viewed also as an element of K. Then $L \cong \mathbb{F}_{p^m}$ is a subfield of $K \cong \mathbb{F}_{q^m}$, and u generates both $L/\mathbb{F}_p$ and $K/\mathbb{F}_q$. The $\mathbb{F}_p$-linear map $A\colon L \to L$ given by $A(z) = z^r + z$ is invertible, with inverse given by

$$A^{-1}(b) = \frac{1}{2}\sum_{k=0}^{m-1} (-1)^k b^{r^k}.$$

Set $a_1 = u$ and, for $1 \le j < i$, recursively compute in L

$$a_{j+1} = A^{-1}(\phi(a_j)) = \frac{1}{2}\sum_{k=0}^{m-1}(-1)^k \phi(a_j)^{r^k}.$$

If $a_j \neq 0$, then the injectivity of A gives

$$a_j^{r-1} + 1 = \frac{A(a_j)}{a_j} \neq 0.$$

Thus $\phi(a_j)$ is defined and nonzero, and hence so is $a_{j+1} = A^{-1}(\phi(a_j))$. By induction, all coordinates are nonzero and none of the denominators vanishes.

The evaluation $x_j \mapsto a_j$ satisfies the defining equations of F_i, which defines a place Q. Since $a_1 = u$ generates $K/\mathbb{F}_q$, the residue field of Q is K, and therefore $\deg Q = m$. The field K, the elements $a_1, \ldots, a_i$, and the resulting evaluation map can all be computed in time $\mathrm{poly}(q, \ell, g)$.

The characteristic 2 case follows the same recursion, but requires a modified argument to find the first element. We defer this proof to Appendix A. □

We now instantiate the construction with the Garcia–Stichtenoth tower to obtain explicit strong subspace designs.

Theorem 3.8. *Let $q = \ell^2$, where ℓ is a prime power. There are infinitely many integers k such that, for every $1 \le r \le k$, there exists an explicit $(r, 6rk)$-strong subspace design $\mathscr{H}$ in $\mathbb{F}_q^k$ of codimension r. Moreover, $\mathscr{H}$ is an $(s, 6sk)$-strong subspace design for every $1 \le s \le r$. The integers k may be taken to be the positive genera in the Garcia–Stichtenoth tower. If $n = |\mathscr{H}|$ and $W \le \mathbb{F}_q^k$ has dimension $s \le r$, then*

$$n \ge (\sqrt{q} - 1)k \qquad \text{and} \qquad \mathbb{E}_{H \in \mathscr{H}} \dim_{\mathbb{F}_q}(W \cap H) \le \frac{6}{\sqrt{q} - 1} \dim_{\mathbb{F}_q} W.$$

Proof. Let $F = F_e/\mathbb{F}_q$ be the e'th field in the Garcia–Stichtenoth tower with $e \ge 2$, let $k = g(F)$ and let $\mathscr{P} = \mathscr{R}_e$. Set

$$d = k + g - 1 = 2g - 1.$$

By Fact 2.4, there is a prime number m such that $d < m < 2d$; such a prime can be found deterministically by enumeration. By Proposition 3.7, we can efficiently compute a place Q of degree m in F. We may therefore apply Definition 3.1 and Proposition 3.6. For every $1 \le s \le r$, the resulting collection is an $(s, 6sk)$-strong subspace design of size $n = |\mathscr{R}_e|$.

By Equation (2.1) we have,

$$n = \ell^e(\ell - 1) \ge (\ell - 1)k = (\sqrt{q} - 1)k.$$

Dividing the intersection bound by n gives

$$\mathbb{E}_{H\in\mathscr{H}} \dim_{\mathbb{F}_q}(W\cap H) \leq \frac{6}{\sqrt{q}-1} \dim_{\mathbb{F}_q} W.$$

Finally, explicitness follows from Proposition 3.7 and Section 2.1.1. The former provides the place Q, its residue field, and the residue map π_Q, while the latter provides the rational places, bases of the required Riemann–Roch spaces, and their evaluations. The remaining maps and subspaces in the construction are obtained by linear algebra over $\mathbb{F}_q$. □

4 An Improved, Double-Evaluation Construction

The preceding construction has two shortcomings. First, its explicit instantiation is restricted to square fields. Second, its normalized intersection bound is $6/(\sqrt{q}-1)$ times the dimension of the test subspace. Consequently, for an r-dimensional test subspace, this estimate yields a nontrivial lossless rank extractor only when $\sqrt{q}-1 > 6r$, and hence does not apply over fields of size less than 49.

In this section, we give a variant of the AGPV construction that works over all finite fields, and produces subspace designs with a better ratio between the intersection bound and the number of subspaces. A direct consequence is the existence of explicit lossy rank condensers over *every* finite field, and lossless rank extractors whenever $q > r$. Building on the framework presented in Section 3, we present the construction of subspace designs, and then derive the consequences for rank condensers and extractors.

4.1 Subspace designs construction

Let $\ell \geq 2$ be even. Our construction has two steps. The first step is the same as the AGPV construction, but we evaluate at places of degree ℓ instead of at rational places. In the second step, we represent each residue-field element as an affine-linear polynomial in $\ell-1$ variables over $\mathbb{F}_q$, and evaluate these polynomials at all points of $\mathbb{F}_q^{\ell-1}$. Evaluating these polynomials at all points of $\mathbb{F}_q^{\ell-1}$ yields a normalized intersection bound that approaches $1/q$ as ℓ grows. The use of a second polynomial evaluation follows the idea of [TSU12].

We begin by analyzing the second step of the construction, which is independent of the function field.

Lemma 4.1. *Let $s,t \geq 1$ and $D \geq 1$ be integers, let $X = (X_1,\ldots,X_t)$, and let $B(X) \in \mathbb{F}_q[X]^{s\times s}$ have entries of total degree at most D. Set*

$$u = \dim_{\mathbb{F}_q(X)} \ker B(X).$$

Then,

$$\sum_{a\in\mathbb{F}_q^t} \dim_{\mathbb{F}_q} \ker B(a) \le q^{t-1}\big(qu + D(s-u)\big).$$

Proof. The assertion is immediate if $u = s$. Otherwise, choose an $(s-u)\times(s-u)$ minor $C(X)$ of $B(X)$ whose determinant $h(X)$ is nonzero. Then, $\deg h \le D(s-u)$.

For $a \in \mathbb{F}_q^t$, set $v_a = \dim_{\mathbb{F}_q} \ker C(a)$. Since C is a minor of B, we have

$$\dim_{\mathbb{F}_q} \ker B(a) - u \le v_a.$$

Choose $R_a \in \mathrm{GL}_{s-u}(\mathbb{F}_q)$ whose last v_a columns span $\ker C(a)$. These columns of $C(X)R_a$ vanish at a, so the determinant has multiplicity at least v_a there. Since $\det R_a$ is a nonzero constant, it follows that

$$v_a \le \mathrm{mult}_a(h).$$

Applying Lemma 2.3 with $S = \mathbb{F}_q$ gives

$$\sum_{a\in\mathbb{F}_q^t} \big(\dim_{\mathbb{F}_q} \ker B(a) - u\big) \le Dq^{t-1}(s-u).$$

Adding $q^t u$ to both sides proves the result. □

We now define the construction. Recall the framework presented in Section 3.1.

Definition 4.2 (Affine-evaluation AGPV construction)**.** *Let $F/\mathbb{F}_q$ be a function field, let $\ell \ge 2$ be even and let $\mathscr{P}_\ell$ be a set of degree-ℓ places of F. Let Q be the place given by Section 3.1. For each $P \in \mathscr{P}_\ell$, fix an $\mathbb{F}_q$-basis $\{1, \omega_{P,1}, \dots, \omega_{P,\ell-1}\}$ of $\kappa(P)$. For*

$$b = b_0 + \sum_{j=1}^{\ell-1} b_j \omega_{P,j} \in \kappa(P),$$

define

$$g_{P,b}(X_1,\dots,X_{\ell-1}) = b_0 + \sum_{j=1}^{\ell-1} b_j X_j.$$

For $a \in \mathbb{F}_q^{\ell-1}$, let $\lambda_{P,a}\colon \kappa(P) \to \mathbb{F}_q$ be the linear map $b \mapsto g_{P,b}(a)$. Let $E_{P,a}\colon V \longrightarrow \mathbb{F}_q^r$ be defined by

$$E_{P,a}(f) = \big(\lambda_{P,a}(\tau_0(f)(P)), \dots, \lambda_{P,a}(\tau_{r-1}(f)(P))\big),$$

and set $H_{P,a} = \ker E_{P,a}$. Finally, let

$$\mathscr{H} = \mathscr{H}(F, \mathscr{P}_\ell, P_\infty, Q, k, r, \ell) = \big(H_{P,a}\big)_{P\in\mathscr{P}_\ell, a\in\mathbb{F}_q^{\ell-1}},$$
$$\mathscr{E} = \mathscr{E}(F, \mathscr{P}_\ell, P_\infty, Q, k, r, \ell) = \big(E_{P,a}\big)_{P\in\mathscr{P}_\ell, a\in\mathbb{F}_q^{\ell-1}}.$$

The collections have size $n = q^{\ell-1}|\mathscr{P}_\ell|$.

Remark 4.3. *This construction introduces only one parameter beyond those of Definition 3.1, namely ℓ.*

We first analyze the construction over an arbitrary function field.

Proposition 4.4 (Affine-evaluation kernel bound)**.** *In the setting of Definition 4.2, for $1 \le s \le r$ let*

$$A_s = q^{\ell-2}\left(sN + (q-1)\left\lfloor \frac{d+(s-1)\widetilde{d}}{\ell} \right\rfloor\right).$$

Then, $\mathscr{H} = \mathscr{H}(F, \mathscr{P}_\ell, P_\infty, Q, k, r, \ell)$ is an (s, A_s)-strong subspace design for every $1 \le s \le r$.

Proof. Fix $1 \le s \le r$, an s-dimensional subspace $W \le V$, and an $\mathbb{F}_q$-basis $\mathscr{B} = (f_1, \dots, f_s)$ of W. Set

$$D_s = d + (s-1)\widetilde{d}, \qquad b_s = \left\lfloor \frac{D_s}{\ell} \right\rfloor.$$

For each $P \in \mathscr{P}_\ell$, define

$$B_P(X) = \left(g_{P,\tau_{i-1}(f_j)(P)}(X)\right)_{i,j\in[s]}, \qquad u_P = \dim_{\mathbb{F}_q(X)} \ker B_P(X).$$

For $a \in \mathbb{F}_q^{\ell-1}$ and $f = \sum_{j=1}^{s} c_j f_j \in W$, by the definition of $H_{P,a}$ we have $f \in H_{P,a}$ implies $B_P(a)(c_1, \dots, c_s)^T = 0$, and hence

$$\dim_{\mathbb{F}_q}(W \cap H_{P,a}) \le \dim_{\mathbb{F}_q} \ker B_P(a).$$

Applying Lemma 4.1 therefore gives

$$\sum_{a\in\mathbb{F}_q^{\ell-1}} \dim_{\mathbb{F}_q}(W \cap H_{P,a}) \le q^{\ell-2}\big(s + (q-1)u_P\big).$$

It remains to bound the sum of the kernel dimensions u_P. By Proposition 3.4, the determinant $\Delta_{\mathscr{B}} := \det M_{\mathscr{B}}$ is nonzero. Moreover, the first row of $M_{\mathscr{B}}$ has entries in $\mathscr{L}(dP_\infty)$, while each of the remaining $s-1$ rows has entries in $\mathscr{L}(\widetilde{d}P_\infty)$. Therefore,

$$0 \ne \Delta_{\mathscr{B}} \in \mathscr{L}(D_s P_\infty).$$

For every $P \in \mathscr{P}_\ell$, we have $B_P(\omega_{P,1}, \dots, \omega_{P,\ell-1}) = M_{\mathscr{B}}(P)$, and therefore

$$u_P \le \dim_{\kappa(P)} \ker M_{\mathscr{B}}(P).$$

Combining this with Lemma 2.15 gives

$$u_P \le v_P(\Delta_{\mathscr{B}}).$$

Since the places in $\mathscr{P}_\ell$ have degree ℓ, we obtain

$$\ell \sum_{P\in\mathscr{P}_\ell} u_P \le \ell \sum_{P\in\mathscr{P}_\ell} v_P(\Delta_{\mathscr{B}}) \le \deg((\Delta_{\mathscr{B}})_0) \le D_s.$$

Thus, $\sum_{P\in\mathscr{P}_\ell} u_P \le b_s$. Summing the preceding kernel bound over $P \in \mathscr{P}_\ell$ now gives

$$\begin{aligned}\sum_{P\in\mathscr{P}_\ell}\sum_{a\in\mathbb{F}_q^{\ell-1}} \dim_{\mathbb{F}_q}(W\cap H_{P,a}) &\le q^{\ell-2}\left(sN+(q-1)\sum_{P\in\mathscr{P}_\ell} u_P\right)\\ &\le q^{\ell-2}\big(sN+(q-1)b_s\big) = A_s.\end{aligned}$$

□

4.2 Evaluation in a function field tower with many degree-d places

To instantiate the preceding construction, we need an explicit family of function fields with many degree-d places, together with efficient algorithms for computing Riemann–Roch spaces and evaluating their elements at these places. We obtain these ingredients by descending the Garcia–Stichtenoth tower over $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$. We call the resulting family the d-descended Garcia–Stichtenoth function fields.

Proposition 4.5 (Function field family with many degree-d places)**.** *Let q be a prime power, let $d \ge 2$ be even, and set $r = q^{d/2}$. Let $(F_i)_{i\ge1}$ be the tower over $\mathbb{F}_q$ defined by*

$$F_1 = \mathbb{F}_q(x_1), \qquad F_{i+1} = F_i(x_{i+1}),$$

where

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

Let $g_i = g(F_i)$. There exists an explicit set $\mathscr{P}_d^{(i)}$ of degree-d places in F_i, represented by evaluation tuples in $\mathbb{F}_{q^d}^i$, such that

$$B_d(F_i) \ge |\mathscr{P}_d^{(i)}| \ge \frac{q^{d/2}-1}{2d}\, g_i.$$

For every $i \ge 1$, there exists a unique pole P_∞ of x_1 in F_i and it is rational. For every integer $\mu \ge 0$, an explicit $\mathbb{F}_q$-basis of $\mathscr{L}(\mu P_\infty)$ can be computed in time $\mathrm{poly}(q,d,g_i,\mu)$*. Moreover, given a degree-d place represented by an evaluation tuple in $\mathbb{F}_{q^d}^i$, every element of $\mathscr{L}(\mu P_\infty)$ can be evaluated at this place in time* $\mathrm{poly}(q,d,g_i,\mu)$.

The proof of Proposition 4.5 is given in Appendix A.

Theorem 4.6 (Strong subspace designs over arbitrary finite fields)**.** *Let q be a prime power, let $\ell \geq 2$ be even, and let $k \geq 2$. For every $1 \leq r \leq k$, there exists an explicit collection $\mathscr{H}$ of n subspaces of $\mathbb{F}_q^k$, each of codimension at most r, such that, for every $1 \leq s \leq r$, the collection is an (s, A_s)-strong subspace design, where*

$$A_s = C_\ell(q) sn, \qquad C_\ell(q) = \frac{1}{q} + \frac{12(q-1)}{q(q^{\ell/2}-1)}.$$

Moreover,

$$n \leq q^{\ell-1} \left\lceil \frac{q^{\ell/2}-1}{2\ell} q^\ell k \right\rceil.$$

Proof. Let $\widetilde{k}$ be the smallest genus in the ℓ-descended Garcia–Stichtenoth tower that is at least k, and let $F/\mathbb{F}_q$ be the corresponding function field. The genus formula in Theorem 2.13 shows that consecutive positive genera grow by a factor of at most $q^{\ell/2}+1 \leq q^\ell$. Hence

$$k \leq \widetilde{k} < q^\ell k.$$

Let P_∞ be the unique pole of x_1 in F, and set $d = 2\widetilde{k} - 1$. By Fact 2.4, there is a prime number m such that $d < m < 2d$, and we can find such a prime deterministically by enumeration. Applying Proposition 3.7 to the ℓ-descended tower gives an explicit place Q of degree m. Set

$$N = \left\lceil \frac{q^{\ell/2}-1}{2\ell} \widetilde{k} \right\rceil.$$

By Proposition 4.5, we may choose a set $\mathscr{P}_\ell$ of N degree-ℓ places of F. Applying Proposition 4.4 gives an explicit collection $\widetilde{\mathscr{H}} = \mathscr{H}(F, \mathscr{P}_\ell, P_\infty, Q, \widetilde{k}, r, \ell)$ of $n = q^{\ell-1}N$ subspaces in $\mathbb{F}_q^{\widetilde{k}}$, each of codimension at most r, which form an (s, A_s)-subspace design for every $1 \leq s \leq r$.

Fix some k-dimensional subspace $U \leq V$, identify it with $\mathbb{F}_q^k$, and set

$$\mathscr{H} := (H \cap U)_{H \in \widetilde{\mathscr{H}}}.$$

For every $H \in \widetilde{\mathscr{H}}$ and $W \leq U$, we have

$$W \cap (H \cap U) = W \cap H, \qquad \operatorname{codim}_U (H \cap U) \leq \operatorname{codim}_V H \leq r.$$

Thus, $\mathscr{H}$ is a collection of n subspaces in $\mathbb{F}_q^k$, each of codimension at most r, which forms an (s, A_s)-subspace design. Moreover, since $m < 2d$, we have $d + (s-1)\widetilde{d} < 6s\widetilde{k}$. Thus, for every s-dimensional subspace $W \leq U$ we obtain,

$$\frac{1}{n} \sum_{H \in \mathscr{H}} \dim_{\mathbb{F}_q}(W \cap H) < \left(\frac{1}{q} + \frac{6(q-1)\widetilde{k}}{q\ell N} \right) s \leq C_\ell(q) s.$$

This proves the asserted value of A_s. The bound on n follows from $\widetilde{k} < q^{\ell}k$.

Finally, the construction is explicit by Propositions 3.7 and 4.5. The former gives the place Q, an explicit representation of its residue field, and the residue map at Q. The latter gives bases of the required Riemann–Roch spaces on the descended tower, as well as the degree-ℓ places and the evaluations at these places. Using these, we compute the right inverse I, the lifted Frobenius maps τ_j, and the kernels defining the subspaces in $\widetilde{\mathscr{H}}$ by linear algebra over $\mathbb{F}_q$. The subspace U and the intersections defining $\mathscr{H}$ are obtained from $\widetilde{\mathscr{H}}$ by linear algebra. □

The following corollary instantiates the preceding theorem so that the normalized intersection bound is within an arbitrary additive γ of $1/q$.

Corollary 4.7 (Strong subspace designs over arbitrary finite fields)**.** *Let q be a prime power, let $0 < \gamma < 1$, and let $k \geq 2$. For every $1 \leq r \leq k$, there exists an explicit collection $\mathscr{H}$ of n subspaces of $\mathbb{F}_q^k$, each of codimension at most r, satisfying*

$$n \leq q\left(1+\frac{12}{\gamma}\right)^2 \left\lceil \frac{3q^2(1+12/\gamma)^2 k}{\gamma} \right\rceil = O\left(q^3 k/\gamma^5\right).$$

For every $1 \leq s \leq r$, the collection is an (s, A_s)-strong subspace design, where

$$A_s = \left(\frac{1}{q}+\gamma\right) sn.$$

In particular, every nonzero subspace $W \leq \mathbb{F}_q^k$ of dimension at most r satisfies

$$\frac{1}{n}\sum_{H\in\mathscr{H}} \dim_{\mathbb{F}_q}(W \cap H) < \left(\frac{1}{q}+\gamma\right)\dim_{\mathbb{F}_q} W.$$

Proof. Set

$$\ell = 2\left\lceil \log_q\left(1+\frac{12}{\gamma}\right)\right\rceil.$$

Let $\widetilde{k}$ be the tower genus chosen in the proof of Theorem 4.6, and set

$$N = \left\lceil \frac{6\widetilde{k}}{\ell\gamma} \right\rceil.$$

Then ℓ is even and

$$q^{\ell/2} - 1 \geq \frac{12}{\gamma},$$

and hence $C_\ell(q) - 1/q < \gamma$. Moreover,

$$N \leq \left\lceil \frac{q^{\ell/2}-1}{2\ell}\widetilde{k} \right\rceil.$$

Applying the construction in the proof of Theorem 4.6 with this choice of N gives a collection of size $n = q^{\ell-1}N$. If $\dim_{\mathbb{F}_q} W = s \le r$, then

$$\begin{aligned}\frac{1}{n}\sum_{H\in\mathscr{H}} \dim_{\mathbb{F}_q}(W\cap H) &< \left(\frac{1}{q} + \frac{6(q-1)\widetilde{k}}{q\ell N}\right) s \\ &\le \left(\frac{1}{q} + \frac{q-1}{q}\gamma\right) s < \left(\frac{1}{q} + \gamma\right) s.\end{aligned}$$

This proves the asserted value of A_s.

Finally,

$$q^{\ell-1} \le q\left(1+\frac{12}{\gamma}\right)^2, \qquad N \le \left\lceil \frac{3q^2(1+12/\gamma)^2 k}{\gamma} \right\rceil,$$

where the second inequality follows from $\widetilde{k} < q^\ell k \le q^2(1+12/\gamma)^2 k$. This gives the claimed bound on n. □

4.3 Rank condensers and extractors

We now record the consequences for lossy rank condensers and lossless rank extractors.

Corollary 4.8 (Lossy rank condensers over arbitrary finite fields)**.** *Let $\varepsilon, \delta \in (0,1]$, and let q be a prime power satisfying*

$$q > \frac{1}{\varepsilon\delta}.$$

For every integer $k \ge 2$ and every $1 \le r \le k$, there exists an explicit (r, ε, δ)-lossy rank condenser $\mathscr{E} = (E_i)_{i\in[n]} \subseteq \mathbb{F}_q^{r\times k}$ of size

$$n = O\left(\frac{q^3 k}{(\varepsilon\delta - 1/q)^5}\right).$$

Proof. Set

$$\gamma = \varepsilon\delta - \frac{1}{q}, \qquad \ell = 2\left\lceil \log_q\left(1+\frac{12}{\gamma}\right)\right\rceil.$$

Let $\widetilde{k}$ be the tower genus chosen in the proof of Theorem 4.6, and set

$$N = \left\lceil \frac{6\widetilde{k}}{\ell\gamma} \right\rceil.$$

The choice of ℓ gives

$$q^{\ell/2} - 1 \ge \frac{12}{\gamma},$$

and hence

$$N \le \left\lceil \frac{q^{\ell/2}-1}{2\ell}\widetilde{k} \right\rceil.$$

We may therefore apply the construction in the proof of Theorem 4.6 with this choice of N. By Proposition 4.4, the resulting collection is an (r,A_r)-strong subspace design of size $n = q^{\ell-1}N$, where

$$\frac{A_r}{rn} < \frac{1}{q} + \frac{6(q-1)\widetilde{k}}{q\ell N} \le \frac{1}{q} + \frac{q-1}{q}\gamma < \varepsilon\delta.$$

Consequently,

$$A_r < \varepsilon\delta rn < \big(\lfloor \varepsilon r \rfloor + 1\big)\big(\lfloor \delta n \rfloor + 1\big),$$

and the claim follows from Proposition 2.1.

Finally, the definition of ℓ gives $q^{\ell-1} = O(q/\gamma^2)$ and $q^\ell = O(q^2/\gamma^2)$, while $N = O(\widetilde{k}/\gamma) = O(q^2k/\gamma^3)$. This proves the stated bound on n, since $\gamma = \varepsilon\delta - 1/q$. □

Taking the rank loss in the preceding corollary to be smaller than $1/r$ gives lossless rank extractors.

Corollary 4.9 (Explicit lossless rank extractors)**.** *Let $1 \le r \le k$ be integers, and let $0 < \delta < 1$. For every prime power $q > r/\delta$, there exists an explicit (r,δ)-lossless rank extractor $\mathscr{E} = (E_i)_{i\in[n]} \subseteq \mathbb{F}_q^{r\times k}$ of size*

$$n = O\left(\frac{q^3r^5k}{(\delta - r/q)^5}\right).$$

In particular, for all integers $1 \le r \le k$ and every prime power $q > r$, there exists an explicit r-lossless rank disperser over $\mathbb{F}_q$ of size $O(r^5kq^8)$.

Proof. Let

$$\varepsilon = \frac{1}{2}\left(\frac{1}{r} + \frac{1}{q\delta}\right).$$

Since $q > r/\delta$, we have $\varepsilon r < 1$. Moreover,

$$\varepsilon\delta - \frac{1}{q} = \frac{1}{2}\left(\frac{\delta}{r} - \frac{1}{q}\right) = \frac{\delta - r/q}{2r} > 0.$$

Applying Corollary 4.8 with loss parameter ε and bad-map fraction δ gives an explicit collection of size

$$n = O\left(\frac{q^3r^5k}{(\delta - r/q)^5}\right).$$

Every good map preserves rank at least $(1-\varepsilon)r > r-1$, and hence preserves rank r. Thus, at most $\lfloor \delta n \rfloor \le \delta n$ maps fail to preserve the rank of each rank-r input.

For the final assertion, assume that $r < q$ and set $\delta_0 = (2r+1)/(2q)$. Then $r/q < \delta_0 < 1$, and the preceding bound becomes $n = O(r^5kq^8)$. Since $\delta_0 < 1$, at least one map preserves the rank of each rank-r input, so the collection is an r-lossless rank disperser. □

4.4 Strong blocking sets over arbitrary finite fields

Fancsali and Sziklai [FS14, FS16] gave a reduction from lossless rank dispersers to strong blocking sets (stated formally in [GRSZ26, Lemma 6.1]). Hence, our results imply new strong blocking sets. We begin with the definitions.

Definition 4.10 (Projective space and projective subspace)**.** *The projective space* $\mathrm{PG}(k-1,q)$ *is the set of one-dimensional subspaces of* $\mathbb{F}_q^k$*. For every nonzero subspace* $U \leq \mathbb{F}_q^k$*, the set*

$$\mathrm{PG}(U) = \{L \leq U : \dim_{\mathbb{F}_q}(L) = 1\}$$

is a projective subspace *of* $\mathrm{PG}(k-1,q)$*. Its dimension is* $\dim_{\mathbb{F}_q}(U)-1$*, and its codimension in* $\mathrm{PG}(k-1,q)$ *is* $k-\dim_{\mathbb{F}_q}(U)$*. For a nonempty set* $S \subseteq \mathrm{PG}(k-1,q)$*, its* projective span *is the smallest projective subspace containing* S*.*

Definition 4.11 (Strong blocking set)**.** *Let* $1 \leq s \leq k-1$*. A set* $B \subseteq \mathrm{PG}(k-1,q)$ *is a* strong s-blocking set *if, for every codimension-*s *projective subspace* $\Sigma \subseteq \mathrm{PG}(k-1,q)$*, the intersection* $B \cap \Sigma$ *spans* Σ*; that is,* Σ *is the smallest projective subspace containing* $B \cap \Sigma$*.*

We next describe the above reduction. Let $\mathscr{E} = (E_i)_{i\in[M]} \subseteq \mathbb{F}_q^{(s+1)\times k}$ be an $(s+1)$-lossless rank disperser, and set $V_i = \mathrm{rowspan}(E_i)$. Then

$$B = \bigcup_{i\in[M]} \mathrm{PG}(V_i)$$

is a strong s-blocking set in $\mathrm{PG}(k-1,q)$ and

$$|B| \leq M\frac{q^{s+1}-1}{q-1} \leq 2Mq^s. \tag{4.1}$$

Using our lossless rank extractors, we obtain the following corollary.

Corollary 4.12 (Strong blocking sets over arbitrary finite fields)**.** *Let* q *be a prime power, and let* $s \geq 1$ *satisfy*

$$q > s+1.$$

For every integer $k \geq s+1$*, there exists an explicit strong* s*-blocking set* $B \subseteq \mathrm{PG}(k-1,q)$ *satisfying*

$$|B| = O\big(s^5 k q^{s+8}\big).$$

Proof. Set $r = s+1$. Since $q > r$, Corollary 4.9 gives an explicit lossless rank disperser of size $M = O(r^5 k q^8)$. Thus, Equation (4.1) gives an explicit strong s-blocking set satisfying

$$|B| \leq 2Mq^s = O\big(r^5 k q^{s+8}\big) = O\big(s^5 k q^{s+8}\big).$$

□

Comparison with previous results. Table 1 compares our construction with the results in [GRSZ26, Table 1]. Let $c_0 > 0$ be the sufficiently large absolute constant in [GRSZ26, Corollary 6.2]. We first consider the range $s+1 < q < (2s)^{c_0}$. In this range, our bound $O(s^5 k q^{s+8}) = kq^s s^{O(1)}$ improves all applicable previous bounds in the table as $s \to \infty$. In particular, it replaces the exponential factors appearing in [GRSZ26, Corollary 6.2(3), Proposition 6.8] and [BT26, Theorem 17] by a polynomial in s. We next consider $q \geq (2s)^{c_0}$. For prime q, our construction replaces the quasipolynomial factor $(2s)^{O(\log(2s))}$ in [GRSZ26, Corollary 6.2(2)] by $O(s^5 q^8)$, which is polynomial in s and q. Thus, whenever $q = s^{O(1)}$, it improves the dependence on s from quasipolynomial to polynomial. For non-prime q in this upper range, [GRSZ26, Corollary 6.2(1)] retains the smaller bound $O(s(k-s)q^{s+1})$ for every $k \geq s+1$, and the bound $O(s(k-s)q^s)$ for infinitely many such k. Finally, when $q \leq s+1$, our result does not apply, whereas [GRSZ26, Corollary 6.2(3), Proposition 6.8] and [BT26, Theorem 17] apply over every prime power.

Table 1: Explicit strong s-blocking sets in $\mathrm{PG}(k-1,q)$, extending [GRSZ26, Table 1]. The bounds shown hold for every $k \geq s+1$; the bounds in [GRSZ26, Corollary 6.2] improve by a factor of q for infinitely many k. Here $C > 0$ is a sufficiently large absolute constant, $o_{qs}(1)$ tends to zero as $qs \to \infty$, and $\mu_{s,q} = \max\{C\log(2s)/\log q, 2\}$.

Reference	Field size	Upper bound on $\lvert B\rvert$
[BT26, Theorem 16]	q square, $q \geq (2s)^{Cs}$	$2^{O(s^2\log(2s))} k q^s$
[BT26, Theorem 17]	Every prime power	$k q^{O(s^2)}$
[GRSZ26, Corollary 6.2(1)]	q non-prime, $q \geq (2s)^C$	$O(s(k-s)q^{s+1})$
[GRSZ26, Corollary 6.2(2)]	q prime, $q \geq (2s)^C$	$(2s)^{O(\log(2s))}(k-s)q^{s+1}$
[GRSZ26, Corollary 6.2(3)]	Every prime power	$O(\mu_{s,q}^{s+1} s(k-s)q^{s+1})$
[GRSZ26, Proposition 6.8]	Every prime power	$k q^{(2+o_{qs}(1))s}$
Corollary 4.12	$q > s+1$	$O(s^5 k q^{s+8})$

4.5 Condensers for affine sources

An affine (n,k)-source over $\mathbb{F}_q$ is the uniform distribution on an affine subspace of $\mathbb{F}_q^n$ of dimension at least k. A seeded condenser for affine sources maps such a source to a shorter one while

retaining most of its entropy. For a discrete random variable Z, its *min-entropy*[5] is

$$H_\infty(Z) = -\log\left(\max_z \mathbf{Pr}[Z=z]\right).$$

Seeded condensers for *general* weak sources, introduced in [RR99, RSW06], are a standard tool in pseudorandomness. Here we restrict attention to affine sources. Although *deterministic* condensers exist for affine sources, the seeded setting permits constructions that are linear in the source for every fixed seed, a property used in several works.

Definition 4.13 (seeded condenser for affine sources [GR08, DG26])**.** *Let q be a prime power, let $1 \le k \le n$ and $m, D \ge 1$ be integers, and let $0 \le k' \le \min\{k,m\}$ and $\varepsilon \in [0,1]$. We say that a map*

$$\mathrm{Cond}\colon \mathbb{F}_q^n \times [D] \longrightarrow \mathbb{F}_q^m$$

is a seeded affine $(k \to_\varepsilon k')$-condenser *if, for every affine (n,k)-source X,*

$$\left|\{y \in [D] : H_\infty(\mathrm{Cond}(X,y)) < k' \log q\}\right| \le \varepsilon D.$$

Its seed length is $d = \log D$. The condenser is lossless *if $k' = k$. The condenser is* linear *if for every fixed seed $y \in [D]$, the map $\mathrm{Cond}(\cdot, y) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ is linear.*[6]

For $i \in [D]$, let $E_i\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a linear map with $m \ge k$, and set $\mathrm{Cond}(x,i) = E_i x$. If X is uniform on $x_0 + W$, then

$$H_\infty(E_i X) = \mathrm{rank}(E_i|_W) \log q.$$

Thus, a (k, ε, δ)-lossy rank condenser is a linear seeded affine $(k \to_\delta (1-\varepsilon)k)$-condenser. This equivalence was recently made explicit, and refined, in [DG26]. Our work thus readily implies the following.

Corollary 4.14 (Condensers for affine sources)**.** *Let q be a prime power and let $\delta, \varepsilon \in (0,1)$ satisfy $\delta\varepsilon > 1/q$. For every integer $n \ge 1$ and every $1 \le k \le n$, there exists an explicit linear seeded affine $(k \to_\varepsilon (1-\delta)k)$-condenser $\mathrm{Cond}\colon \mathbb{F}_q^n \times [D] \longrightarrow \mathbb{F}_q^k$. Its seed length satisfies*

$$d \le \log n + 3\log q + 5\log\left(\frac{1}{\delta\varepsilon - 1/q}\right) + O(1).$$

For fixed q, δ, and ε, the construction has $d = \log n + O_{q,\delta,\varepsilon}(1)$.

[5] For an affine source, min-entropy equals Shannon entropy because the distribution is uniform on its support.

[6] An alternative definition requires that, for every affine (n,k)-source X and an independent uniform seed $Y \in [D]$, the joint distribution $(Y, \mathrm{Cond}(X,Y))$ be ε-close to a distribution with min-entropy at least $d + k' \log q$. The definition above implies this condition. Conversely, for linear condensers, the alternative definition with error ε implies the definition above with error at most $\varepsilon/(1-1/q) \le 2\varepsilon$ ([Rao09, Proposition 2.9]). Thus, for linear condensers, the two definitions are equivalent up to a factor of 2 in the error.

Proof. Set $\gamma = \delta\varepsilon - 1/q$. Apply Corollary 4.8 with ambient dimension n, rank k, loss parameter δ, and bad-map fraction ε, and set $\mathrm{Cond}(x,i) = E_i x$ for the resulting maps $E_i \in \mathbb{F}_q^{k\times n}$. The construction in that corollary uses

$$D = O\left(\frac{q^3 n}{(\delta\varepsilon - 1/q)^5}\right).$$

Taking logarithms gives the seed-length bound. □

Note that with, say, $\varepsilon = \delta = 3/4$, one can even take $q = 2$.

Comparison with previous results Table 2 compares the seed length, output dimension and parameter restrictions of previous constructions. For every fixed q, δ, and ε satisfying $\delta\varepsilon > 1/q$, our construction has $m = k$ and seed length $\log n + O(1)$. Over constant-sized fields, the earlier bounds below either get worse seed length or vanishing output entropy rate. Our construction is the first to achieve both optimal seed length dependence on n, and constant output entropy rate, over all fixed fields – and in particular over $\mathbb{F}_2$ (when ε, δ are large enough).

The lossless rank extractors of Gabizon and Raz [GR08, Theorem 5] and Forbes and Shpilka [FS12, Theorem 4.1] give lossless affine extractors. Forbes and Shpilka improve the number of bad maps from nk^2 to $nk - \binom{k+1}{2}$, thereby saving a $\log k$ term in the seed length. However, both families are indexed by elements of $\mathbb{F}_q$, so achieving error ε requires $q = \Omega(nk^2/\varepsilon)$ and $q = \Omega(nk/\varepsilon)$, respectively.

The lossless condensers of Guruswami, Umans, and Vadhan [GUV09, Theorem 1.7], later made linear by Cheraghchi [Che10, Corollary 2.23], apply to arbitrary sources over any field, at the cost of a constant-factor increase in seed length. Their second construction [GUV09, Theorem 4.4] avoids this constant-factor increase in seed length, but has vanishing output entropy rate.

The folded Reed-Solomon construction of Guruswami and Kopparty [GK16, Theorem 14], together with the lossy analysis of Forbes and Guruswami [FG15, Proposition 6.8], allows every $k \le m < n$. Its seed length is $\log(n/(m-k+1)) + \log(1/(\delta\varepsilon)) + O(1)$, but requires the field size be larger than n. Applying the field reduction of [FG15, Proposition 8.5] gives seed length $\log(n/k) + \log(1/(\delta\varepsilon)) + O(1)$ over every field, at the cost of vanishing output entropy rate.

Guruswami, Xing, and Yuan [GXY18, Theorem 1.2] gave a function field generalization of the construction of [GK16], which relaxes the field-size restriction, but their condenser bounds require either a growing field or a vanishing output entropy rate. Indeed, for output dimension $m \ge 4k$, their construction supplies $\Omega((n/m)q^{\lfloor m/(2k)\rfloor})$ maps, whereas $O(n\log_q n/(m\delta\varepsilon))$ maps suffice to obtain a $(k \to_\varepsilon (1-\delta)k)$-condenser. Thus their bounds guarantee sufficiently many maps when $q^{\lfloor m/(2k)\rfloor} \gtrsim \frac{\log_q n}{\delta\varepsilon}$. For fixed loss and error, keeping $m = O(k)$ therefore requires q

to grow with n, although polylogarithmic field size suffices. Over a fixed field, this condition instead requires $m/k = \Omega(\log_q \log_q n)$, so the guaranteed output entropy rate $(1-\delta)k/m$ tends to zero.

Goyal, Guruswami, and Hsieh [GGH26] work over every field size and allow arbitrary positive loss and error, but their output dimension grows exponentially with k^2, so their guaranteed output entropy rate vanishes as k grows.

Finally, Guo, Raj, Shangguan, and Zhang [GRSZ26] obtain $m = k$ and seed length $\log n + O(1)$ for infinitely many input dimensions, but require q to grow polynomially with k; over prime fields, their seed length also contains an additional polylogarithmic term in k.

In the $q = 2$ regime, a recent work of Doron and Goodman [DG26] interpreted subspace designs as linear seeded condensers for affine sources, and combined [GK16, FG15] with other objects from extractor theory. They were able to get a $(k \to_\varepsilon (1/2+\beta)m)$ seeded linear affine condenser from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with seed length $\log(n/k) + O(\log\log n)$ and $m \geq \frac{k}{\text{polylog(n)}}$ for *some* nontrivial ε, and some constant $\beta > 0$. For an arbitrary $\varepsilon > 0$, they get seed length $O(\log(n/k) + \log(1/\varepsilon) + \log\log n)$.

AI Usage. All ideas, constructions, and proofs, were developed by the authors, except for the case $\operatorname{char}\mathbb{F}_q \neq 2$ of Proposition 3.7, for which we assisted GPT-5.6 Sol. GPT-5.6 Sol was also used for language editing.

Table 2: $(k \to_\varepsilon (1-\delta)k)$ seeded linear affine condensers from $\mathbb{F}_q^n$ to $\mathbb{F}_q^m$ with seed length d. Seed lengths are upper bounds, with additive $O(1)$ terms omitted. All implicit constants are absolute. When δ does not appear, the construction is lossless (i.e. $\delta = 0$). The output entropy rate is $\frac{(1-\delta)k}{m}$.

Reference	Field size	Output dimension m	Seed length d
[GR08, Theorem 5 and Remark 6.2]	$q \geq \Omega(nk^2/\varepsilon)$	k	$\log(n/\varepsilon) + 2\log k$
[FS12, Theorem 4.1]	$q \geq \Omega(nk/\varepsilon)$	k	$\log(nk/\varepsilon)$
[Che10, Corollary 2.23]	Every q	$O(k) + d$	$O(\log(nk/\varepsilon) + \log(q))$
[GUV09, Theorem 4.4]	Every q	$O(kd)$	$\log(nk/\varepsilon) + \log(q)$
[GK16, Theorem 14]	$q \geq \Omega\left(\frac{mn}{\delta\varepsilon(m-k+1)}\right)$	$m \geq k$	$\log\frac{n}{m-k+1} + \log\frac{1}{\delta\varepsilon}$
[FG15, Proposition 8.5]	Every q	$O\left(k\left(1+\log_q\frac{n}{\delta\varepsilon}\right)\right)$	$\log(n/(\delta\varepsilon k))$
[GXY18, Theorem 1.2]	$q \geq \left(\frac{\log n}{\delta\varepsilon}\right)^{O(k/m)}$	$m \geq 4k$	$\log(n/(\delta\varepsilon m)) + \log\log_q n$
[GGH26, Theorem 1.1]	Every q	$\mathrm{poly}(k, 1/(\delta\varepsilon))q^{k^2}$	$\log(n/(m\delta\varepsilon))$
[GRSZ26, Theorem 4.5]	$q \geq \mathrm{poly}(k, 1/(\delta\varepsilon))$; non-prime	k	$\log(n/(\delta\varepsilon))$
[GRSZ26, Theorem 5.10]	$q \geq \mathrm{poly}(k, 1/(\delta\varepsilon))$; prime	k	$\log(n/(\delta\varepsilon))$ $+O(\log k \cdot \log(k/(\delta\varepsilon)))$
[DG26]	$q = 2$	see discussion above	
Corollary 4.14	$q > 1/(\delta\varepsilon)$	k	$\log n + O\left(\log\frac{q}{\delta\varepsilon - 1/q}\right)$

References

[BCDZ26] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. From random to explicit via subspace designs with applications to local properties and matroids. In *Proceedings of the 58th Annual Symposium on Theory of Computing (STOC)*, pages 619–630. ACM, 2026.

[BT26] Anurag Bishnoi and István Tomon. Explicit constructions of optimal blocking sets and minimal codes. *Combinatorica*, 46(2), 2026. Article 13.

[CGG+26] Abhranil Chatterjee, Sumanta Ghosh, Rohit Gurjar, Roshan Raj, and Thomas Thierauf. Bipartite matching is in NC. Technical Report TR26-100, Electronic Colloquium on Computational Complexity (ECCC), 2026.

[Che10] Mahdi Cheraghchi. *Applications of Derandomization Theory in Coding*. PhD thesis, EPFL, 2010.

[CI17] Mahdi Cheraghchi and Piotr Indyk. Nearly optimal deterministic algorithm for sparse Walsh–Hadamard transform. *ACM Transactions on Algorithms*, 13(3), March 2017. Preliminary version in Proceedings of SODA 2016.

[CZ25] Yeyuan Chen and Zihan Zhang. Explicit folded Reed-Solomon and multiplicity codes achieve relaxed generalized Singleton bounds. In *Proceedings of the 57th Annual Symposium on Theory of Computing (STOC)*, pages 1–12. ACM, 2025.

[DG26] Dean Doron and Jesse Goodman. Manuscript, 2026.

[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.

[Dvi25] Zeev Dvir. Tensor rank and dimension expanders. arXiv preprint arXiv:2511.02670, 2025.

[FG15] Michael A. Forbes and Venkatesan Guruswami. Dimension expanders via rank condensers. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2015.

[FS12] Michael A. Forbes and Amir Shpilka. On identity testing of tensors, low-rank recovery and compressed sensing. In *Proceedings of the 44th Annual Symposium on Theory of Computing (STOC)*, pages 163–172. ACM, 2012.

[FS14] S. L. Fancsali and P. Sziklai. Lines in Higgledy-Piggledy arrangement. *The Electronic Journal of Combinatorics*, 21(2):P2.56, 2014.

[FS16] Szabolcs L. Fancsali and Péter Sziklai. Higgledy-piggledy subspaces and uniform subspace designs. *Designs, Codes and Cryptography*, 79(3):625–645, 2016.

[FSS14] Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *Proceedings of the 46th Annual Symposium on Theory of Computing (STOC)*, page 867–875. ACM, 2014.

[GG26] Rohan Goyal and Venkatesan Guruswami. Optimal proximity gaps for subspace-design codes and (random) Reed–Solomon codes. In *Proceedings of the 58th Annual Symposium on Theory of Computing (STOC)*. ACM, 2026.

[GGH26] Rohan Goyal, Venkatesan Guruswami, and Jun-Ting Hsieh. Explicit constant-alphabet subspace design codes. arXiv preprint arXiv:2604.15218, 2026.

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

[GR08] Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. *Combinatorica*, 28(4):415–440, 2008.

[GRSZ26] Zeyu Guo, Roshan Raj, Chong Shangguan, and Zihan Zhang. Explicit rank extractors and subspace designs via function fields, with applications to strong blocking sets. In *Proceedings of the 67th IEEE Symposium on Foundations of Computer Science (FOCS)*, 2026. Also available as ECCC Technical Report TR26-058.

[GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Inventiones Mathematicae*, 121(1):211–222, December 1995.

[Gur05] Venkatesan Guruswami. Algebraic-geometric generalizations of the Parvaresh–Vardy codes. Technical Report TR05-132, Electronic Colloquium on Computational Complexity, 2005.

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

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

[GXY18] Venkatesan Guruswami, Chaoping Xing, and Chen Yuan. Subspace designs based on algebraic function fields. *Transactions of the American Mathematical Society*, 370(12):8757–8775, 2018.

[KS11] Zohar S. Karnin and Amir Shpilka. Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in. *Combinatorica*, 31(3):333–364, May 2011.

[KS26] Swastik Kopparty and Shubhangi Saraf. On the CGGRT criterion for detecting bipartite perfect matchings in NC. arXiv preprint arXiv:2607.15554, 2026.

[Moo96] Eliakim Hastings Moore. A two-fold generalization of Fermat's theorem. *Bulletin of the American Mathematical Society*, 2(7):189–199, 1896.

[PV05] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *Proceedings of the 46th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 285–294. IEEE, 2005.

[Rao09] Anup Rao. Extractors for low-weight affine sources. In *Proceedings of the 24th Annual Conference on Computational Complexity (CCC)*, pages 95–101. IEEE, 2009.

[Ric56] Moses Richardson. On finite projective games. *Proceedings of the American Mathematical Society*, 7(3):458–465, 1956.

[RR99] Ran Raz and Omer Reingold. On recycling the randomness of states in space bounded computation. In *Proceedings of the 31st Annual Symposium on Theory of Computing (STOC)*, pages 159–168. ACM, 1999.

[RSW06] Omer Reingold, Ronen Shaltiel, and Avi Wigderson. Extracting randomness via repeated condensing. *SIAM Journal on Computing*, 35(5):1185–1209, 2006.

[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.

[Sho90] Victor Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54(189):435–447, 1990.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[TSU12] Amnon Ta-Shma and Christopher Umans. Better condensers and new extractors from Parvaresh-Vardy codes. In *Proceedings of the 27th Conference on Computational Complexity (CCC)*, pages 309–315. IEEE, 2012.

A Missing Proofs

We begin with the proof of the case $\operatorname{char}\mathbb{F}_q = 2$ of Proposition 3.7.

Proof of Proposition 3.7. It remains to consider characteristic 2. Write $q = 2^e$ and $r = 2^s$, so that $e\ell = 2s$. Using Shoup's algorithm, construct an irreducible polynomial $h \in \mathbb{F}_2[T]$ of degree m, and set

$$L = \mathbb{F}_2[T]/(h), \qquad K = \mathbb{F}_q[T]/(h).$$

The condition $\gcd(m,e) = 1$ implies that h remains irreducible over $\mathbb{F}_q$. Thus $L \cong \mathbb{F}_{2^m}$ is a subfield of $K \cong \mathbb{F}_{q^m}$. Write $\tau = \mathrm{Tr}_{L/\mathbb{F}_2}$; since m is odd, $\tau(1) = 1$. The $\mathbb{F}_2$-linear map

$$A\colon L \longrightarrow L, \qquad A(z) = z^r + z$$

has kernel $\mathbb{F}_2$. Indeed, $A(z) = 0$ if and only if $z^{2^s} = z$, and the fixed field of $z \mapsto z^{2^s}$ in $L \cong \mathbb{F}_{2^m}$ is $\mathbb{F}_{2^{\gcd(s,m)}} = \mathbb{F}_2$. Moreover, Frobenius invariance of the trace gives

$$\tau(A(z)) = \tau(z^{2^s}) + \tau(z) = 0$$

for every $z \in L$, and hence $\mathrm{im}(A) \subseteq \ker(\tau)$. Both spaces have dimension $m-1$ over $\mathbb{F}_2$: the first because $\dim_{\mathbb{F}_2} \ker(A) = 1$, and the second because $\mathrm{im}(\tau) = \mathbb{F}_2$. Therefore $\mathrm{im}(A) = \ker(\tau)$. Consequently, whenever $\tau(b) = 0$, we can solve $A(z) = b$ by Gaussian elimination over $\mathbb{F}_2$.

We first construct $c \in L^\times$ such that

$$\mathbb{F}_2(c) = L, \qquad \tau(c) = \tau(c^{-1}) = 0.$$

Set $M = 2m+1$. Since $m \geq 5$, the group $L^\times$ contains more than M elements. Enumerate any $M+1$ of them, and choose one, denoted by u, such that $u^M \neq 1$. Such an element exists because $X^M - 1$ has at most M roots. In particular, $u \notin \mathbb{F}_2$, so u has degree m over $\mathbb{F}_2$, since the prime-degree extension $L/\mathbb{F}_2$ has no proper intermediate fields. Its Frobenius orbit is disjoint from that of u^{-1}. Indeed, an equality $u^{2^a} = u^{-1}$ with $0 \leq a < m$ would, after applying the 2^a-power Frobenius once more, give

$$u^{2^{2a}} = (u^{-1})^{2^a} = (u^{2^a})^{-1} = u.$$

Since the Frobenius orbit of u has size m, this gives $m \mid 2a$, and hence $a = 0$. But then $u = u^{-1}$, which in characteristic two implies $u = 1$, a contradiction. Thus

$$S = \{1\} \cup \{u^{2^a} : 0 \leq a < m\} \cup \{u^{-2^a} : 0 \leq a < m\}$$

has M distinct nonzero elements.

We claim that there is some $1 \leq j \leq M$ with $\tau(u^j + u^{-j}) = 0$. Otherwise, for every such j we would have

$$\sum_{a \in S} a^j = 1 + \tau(u^j + u^{-j}) = 0.$$

Enumerate $S = \{s_1, \ldots, s_M\}$ and consider the matrix

$$V = (s_k^j)_{1 \le j,k \le M}.$$

This matrix is invertible. Indeed, multiplying its kth column by s_k^{-1} gives the Vandermonde matrix $(s_k^{j-1})_{1 \le j,k \le M}$, which is invertible because the elements of S are distinct. On the other hand, the preceding equalities say that $V(1, \ldots, 1)^\top = 0$, a contradiction. We find a suitable j by testing all M choices.

We next verify that $u^j \neq 1$. Let n be the multiplicative order of u. For every positive integer a, we have

$$u^{2^a} = u \quad \Longleftrightarrow \quad n \mid 2^a - 1.$$

Since the Frobenius orbit of u has size m, it follows that m is the multiplicative order of 2 modulo n. Now choose a prime divisor ρ of n. As $n \mid 2^m - 1$, the multiplicative order of 2 modulo ρ divides m. It cannot equal 1, since that would imply $\rho \mid 2 - 1$, and therefore equals m because m is prime. By Fermat's little theorem this order divides $\rho - 1$, so $m \mid \rho - 1$. Both m and ρ are odd, and hence $2m \mid \rho - 1$. Consequently,

$$n \ge \rho \ge 2m + 1 = M.$$

Equality $n = M$ would imply $u^M = 1$, contrary to the choice of u. Thus $n > M$.

Set $t = u^j$ and $c = t + t^{-1}$. Since $1 \le j \le M < n$, we have $t \neq 1$. It follows that $c \neq 0$, because in characteristic two the equality $t + t^{-1} = 0$ would imply $(t+1)^2 = 0$, and hence $t = 1$. The choice of j gives $\tau(c) = 0$. We now verify the corresponding assertion for c^{-1}. Since the characteristic is two,

$$c^{-1} = \frac{t}{t^2+1} = \frac{t}{(t+1)^2} = \frac{1}{t+1} + \frac{1}{(t+1)^2}.$$

Let $w = (t+1)^{-1}$. Then $c^{-1} = w + w^2$, and Frobenius invariance gives $\tau(w^2) = \tau(w)$. Therefore

$$\tau(c^{-1}) = \tau(w) + \tau(w^2) = 2\tau(w) = 0.$$

Finally, $c \notin \mathbb{F}_2$, because $c \neq 0$, $\tau(c) = 0$, and $\tau(1) = 1$. Since m is prime, c therefore generates $L/\mathbb{F}_2$.

We now construct the coordinates of Q. Solve $A(z) = c^{-1}$ and set $a_1 = z^{-1}$. Since $c^{-1} \neq 0$ whereas A vanishes on $\mathbb{F}_2$, every solution z lies outside $\mathbb{F}_2$. In particular, $z \neq 0$, so a_1 is well-defined, and

$$\phi(a_1) = \frac{1}{z^r + z} = c.$$

Since m is prime, $a_1 \notin \mathbb{F}_2$ generates $L/\mathbb{F}_2$. Moreover, $\tau(\phi(a_1)) = 0$. Suppose that $a_j \in L \setminus \mathbb{F}_2$ has been constructed with $\tau(\phi(a_j)) = 0$. Since the only elements of L fixed by $z \mapsto z^r$ lie in $\mathbb{F}_2$,

the value $\phi(a_j)$ is defined and nonzero. Solve $A(b) = \phi(a_j)$. As $\ker(A) = \mathbb{F}_2$, the two solutions are b and $b+1$; neither lies in $\mathbb{F}_2$, because their image under A is nonzero. Furthermore,

$$\phi(b+1) + \phi(b) = \frac{(b+1)^{r+1} + b^{r+1}}{A(b)} = 1 + \frac{1}{\phi(a_j)}.$$

Frobenius invariance gives $\tau(a_j^{-r}) = \tau(a_j^{-1})$, so $1/\phi(a_j) = a_j^{-1} + a_j^{-r}$ has trace zero. Therefore the two values $\phi(b)$ and $\phi(b+1)$ have different traces: taking the trace of both sides of the above equation gives

$$\tau(\phi(b+1)) + \tau(\phi(b)) = \tau(1) = 1.$$

Thus

$$a_{j+1} = b + \tau(\phi(b))$$

selects b if $\tau(\phi(b)) = 0$ and $b+1$ otherwise. It therefore satisfies

$$A(a_{j+1}) = \phi(a_j), \qquad \tau(\phi(a_{j+1})) = 0.$$

In either case, $a_{j+1} \notin \mathbb{F}_2$. This completes the induction and constructs $a_1, \dots, a_i$ without vanishing denominators.

The evaluation $x_j \mapsto a_j$ satisfies the defining equations of F_i, which defines a place Q. Since a_1 generates $L/\mathbb{F}_2$, its residue field is

$$\mathbb{F}_q(a_1, \dots, a_i) = \mathbb{F}_q(a_1) = \mathbb{F}_q L = K.$$

Therefore $\deg Q = m$. All steps can be carried out in time $\mathrm{poly}(q, \ell, g)$. □

Next, we prove Proposition 4.5.

Proof of Proposition 4.5. The tuple $(0, \dots, 0)$ defines a rational place of F_i, so F_i has full constant field $\mathbb{F}_q$. Its constant-field extension $F_i^{(d)}$ is the i'th level of the Garcia–Stichtenoth tower over $\mathbb{F}_{q^d} = \mathbb{F}_{r^2}$. It has the same genus g_i, and $g_i \le r^i$ by Theorem 2.13.

Let $\mathscr{S}_i$ be the set of evaluation tuples $(x_1, \dots, x_i) \in \mathbb{F}_{r^2}^i$ satisfying the tower equations and $x_1^r + x_1 \neq 0$. The trace map $z \mapsto z^r + z$ from $\mathbb{F}_{r^2}$ to $\mathbb{F}_r$ is surjective with kernel of size r. There are therefore $r^2 - r$ choices for x_1. Moreover, if $x_j^r + x_j \neq 0$, then

$$\frac{x_j^r}{x_j^{r-1} + 1} = \frac{x_j^{r+1}}{x_j^r + x_j} \in \mathbb{F}_r^\times,$$

so there are exactly r choices for x_{j+1}, all with nonzero trace. These tuples represent distinct affine rational places of $F_i^{(d)}$, and hence

$$|\mathscr{S}_i| = (r^2 - r) r^{i-1} = r^i (r-1).$$

For each proper divisor b of d, let $\mathscr{S}_i(b)$ consist of the tuples in $\mathscr{S}_i$ whose coordinates lie in $\mathbb{F}_{q^b}$. If d/b is even, then $z^r = z$ on $\mathbb{F}_{q^b}$. Thus, $\mathscr{S}_i(b)$ is empty in characteristic two, whereas in odd characteristic the recurrence $x_{j+1} = x_j/4$ gives $|\mathscr{S}_i(b)| = q^b - 1$.

If d/b is odd, then b is even. Setting $h = q^{b/2}$, we have $z^r = z^h$ on $\mathbb{F}_{q^b} = \mathbb{F}_{h^2}$. The tower equation is therefore

$$x_{j+1}^h + x_{j+1} = \frac{x_j^{h+1}}{x_j^h + x_j}.$$

Here $z^h + z$ and z^{h+1} are the trace and norm from $\mathbb{F}_{h^2}$ to $\mathbb{F}_h$. There are $h^2 - h$ choices for x_1 of nonzero trace and h choices at every subsequent step. Consequently,

$$|\mathscr{S}_i(b)| = h^i(h-1) \qquad \text{when } d/b \text{ is odd.}$$

A tuple in $\mathscr{S}_i$ has a q-Frobenius orbit of size less than d only if it belongs to $\mathscr{S}_i(b)$ for some proper divisor b of d. The even-quotient cases contribute fewer than

$$\sum_{b=1}^{d/2} q^b < 2r$$

tuples. In the odd-quotient cases, $b \le d/3$ and $h^i(h-1) < q^{b(i+1)/2}$. Hence these cases contribute fewer than

$$\sum_{b=1}^{\lfloor d/3 \rfloor} q^{b(i+1)/2} < 2r^{(i+1)/3}$$

tuples.

For $a = (a_1, \ldots, a_i) \in \mathscr{S}_i$, let $\widehat{P}_a$ be the affine rational place of $F_i^{(d)}$ represented by a, and let

$$\mathrm{Orb}_q(a) = \left\{ (a_1^{q^v}, \ldots, a_i^{q^v}) : 0 \le v < d \right\}$$

be its q-Frobenius orbit. By Lemma 2.14, if this orbit has size d, then the places $\widehat{P}_b$ with $b \in \mathrm{Orb}_q(a)$ lie above a unique degree-d place P_a of F_i. Moreover, two full orbits give the same place of F_i if and only if they are equal. Let $\mathscr{P}_d^{(i)}$ be the set of places obtained from the full orbits in $\mathscr{S}_i$. We can enumerate this set explicitly by representing each place by a representative from its orbit. Since every full orbit contains d tuples, for every $i \ge 2$ we have

$$d|\mathscr{P}_d^{(i)}| > (r-1)r^i - 2r - 2r^{(i+1)/3}.$$

The genus formula in Theorem 2.13 gives $g_i/r^i \to 1$. Therefore,

$$\liminf_{i\to\infty} \frac{|\mathscr{P}_d^{(i)}|}{g_i} \ge \frac{r-1}{d} = \frac{q^{d/2}-1}{d}.$$

We now deduce the bound on $B_d(F_i)$. It is trivial for $i = 1$, since $g_1 = 0$, so assume that $i \geq 2$. If $r \geq 4$, then

$$2r + 2r^{(i+1)/3} \leq \frac{r-1}{2} r^i.$$

The preceding construction of $\mathscr{P}_d^{(i)}$ therefore gives

$$dB_d(F_i) \geq d|\mathscr{P}_d^{(i)}| > (r-1)r^i - 2r - 2r^{(i+1)/3} \geq \frac{r-1}{2} r^i \geq \frac{r-1}{2} g_i.$$

The only cases with $r < 4$ are $(q,d) = (2,2)$ and $(q,d) = (3,2)$. In the first case, $\mathscr{S}_i(1)$ is empty, while in the second it has size two. Thus,

$$2B_2(F_i) \geq \begin{cases} 2^i, & r = 2, \\ 2 \cdot 3^i - 2, & r = 3, \end{cases} \geq \frac{r-1}{2} g_i.$$

Dividing by d proves the general bound.

It remains to prove the assertion about the Riemann–Roch spaces. Let $\widehat{F}_i = F_i^{(d)}$, and let $\widehat{P}_\infty$ be the unique pole of x_1 in $\widehat{F}_i$. Its restriction P_∞ to F_i is the unique pole of x_1 in F_i, and $\widehat{P}_\infty$ is the unique place above it. Since $\widehat{P}_\infty$ is rational, Lemma 2.14 implies that P_∞ is rational as well. The constant-field-extension theorem for Riemann–Roch spaces now gives

$$\mathscr{L}_{\widehat{F}_i}(\mu \widehat{P}_\infty) = \mathbb{F}_{q^d} \cdot \mathscr{L}_{F_i}(\mu P_\infty); \tag{A.1}$$

see [Sti09, Theorem 3.6.3(d)]. In particular, the two spaces have the same dimension over their respective constant fields.

The field $\widehat{F}_i/\mathbb{F}_{q^d}$ is a Garcia–Stichtenoth function field. By [SAK+01], we can compute an $\mathbb{F}_{q^d}$-basis $f_1, \ldots, f_t$ of $\mathscr{L}_{\widehat{F}_i}(\mu \widehat{P}_\infty)$ in polynomial time. Let σ be the q-Frobenius automorphism of $\widehat{F}_i/F_i$; that is, σ acts on the constants by $c \mapsto c^q$ and fixes the tower generators $x_1, \ldots, x_i$. By Equation (A.1), the σ-invariant subspace of $\mathscr{L}_{\widehat{F}_i}(\mu \widehat{P}_\infty)$ is precisely $\mathscr{L}_{F_i}(\mu P_\infty)$.

Choose an $\mathbb{F}_q$-basis $\beta_1, \ldots, \beta_d$ of $\mathbb{F}_{q^d}$. For $a \in [d]$ and $j \in [t]$, compute

$$h_{a,j} = \mathrm{Tr}_{\widehat{F}_i/F_i}(\beta_a f_j) = \sum_{v=0}^{d-1} \sigma^v(\beta_a f_j).$$

Each $h_{a,j}$ belongs to $\mathscr{L}_{F_i}(\mu P_\infty)$. Moreover, these elements span this space over $\mathbb{F}_q$. Indeed, the elements $\beta_a f_j$ form an $\mathbb{F}_q$-basis of $\mathscr{L}_{\widehat{F}_i}(\mu \widehat{P}_\infty)$, so their traces span the image of $\mathrm{Tr}_{\widehat{F}_i/F_i}$. This image is the entire descended Riemann–Roch space: for any $f \in \mathscr{L}_{F_i}(\mu P_\infty)$, choose $\beta \in \mathbb{F}_{q^d}$ with $\mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\beta) = 1$, which exists because finite fields are separable. Then

$$\mathrm{Tr}_{\widehat{F}_i/F_i}(\beta f) = f.$$

We can therefore select an $\mathbb{F}_q$-basis from the elements $h_{a,j}$ by Gaussian elimination.

Finally, let P be a degree-d place represented by a tuple $a \in \mathbb{F}_{q^d}^i$, and let $\widehat{P}_a$ be the corresponding rational place of $\widehat{F}_i$. Under the identification $\kappa(P) \cong \mathbb{F}_{q^d}$ determined by a, evaluation at P agrees with evaluation at $\widehat{P}_a$. The latter can be computed efficiently by the algorithm of [SAK+01]. □

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il