Subspace-Design Codes from LCL Derandomization: A Short Note

Fernando Granha Jeronimo Nikhil Shagrithaya

Abstract

Local LCL properties [Levi, Mosheiff, and Shagrithaya (LMS), FOCS 2025] give a language to express a broad range of linear properties of codes. Subspace design [Guruswami and Xing, 2013] is an elegant property about the linear structure of codes, and it governs important code behavior. In this note, we show that the subspace design property can be phrased as an LCL property. This allows us to recover the recent Goyal, Guruswami, and Hsieh result of constant-alphabet subspace-design codes from the earlier LCL derandomization framework [Jeronimo–Shagrithaya (JS), STOC 2026], with the same coarse alphabet dependence.

1 Introduction

Fix $k = \mathbb{F}_{q_0}$. For a finite-dimensional k-space W and a code $C \leq_k W^n$, put

$$\mathrm{rate}(C) = \frac{\dim_k C}{n \dim_k W}.$$

For $A \leq_k C$ and $i \in [n]$, let $A_i = \{a \in A : a_i = 0\}$. We call C a (τ, T)-subspace-design code [4, 3, 7] if

$$\frac{1}{n} \sum_{i=1}^{n} \dim_k A_i \leq \tau \dim_k A \quad \text{for every } A \leq_k C \text{ with } 1 \leq \dim_k A \leq T. \tag{1}$$

Theorem 1.1 (Explicit constant-alphabet subspace design)**.** *For every $T \in \mathbb{N}$ and fixed $R, \varepsilon \in (0,1)$, there is an explicit asymptotic family of k-linear codes*

$$C \leq_k \Sigma^N$$

of asymptotic rate R that are $(R+\varepsilon, T)$-subspace-design codes. The alphabet $\Sigma \cong k^D$ is independent of N with $D \leq \mathrm{poly}(1/\varepsilon) q_0^{O(T^2)}$.

This theorem is due to Goyal, Guruswami, and Hsieh [2]. The point here is that it can be recovered from the LCL/JS framework with an LCL phrasing and a routine base field adaptation.

2 Subspace Design as an LCL Property

Set $L = q_0^T$ and index the L columns by a fixed ordering of $x \in k^T$. For $1 \leq r \leq T$, let $\mathsf{proj}_r : k^r \to k^T$ be $v \mapsto (v, 0)$. For every subspace $V \leq k^r$, define

$$E_{r,V} := \left\{ (\lambda(x))_{x \in k^T} : \lambda \in (k^T)^*,\ \mathsf{proj}_r(V) \subseteq \ker \lambda \right\} \leq k^L, \tag{2}$$

and choose $M_{r,V} \in k^{L \times L}$ with $\ker_k M_{r,V} = E_{r,V}$.

Because W is a k-space, $z = (z_x)_{x \in k^T} \in W^L$ satisfies $M_{r,V} z^{\mathsf{T}} = 0$ exactly when it is the full table of a k-linear map $\lambda : k^T \to W$ whose kernel contains $\mathsf{proj}_r(V)$ (the 'full table' of λ is the vector of length q_0^T that contains all the outputs of λ). This follows by expanding W in a k-basis and applying (2) to every scalar component.

For $\tau \in [0,1]$, define an L-local LCL property $\mathcal{P}_{\tau,T}$ as the collection of all profiles with the following property. A profile fixes $r \in [T]$, uses the constraint types $M_{r,V}$ for $V \leq k^r$, and has rational frequencies satisfying

$$\sum_{V \leq k^r} f_V = 1, \qquad \sum_{V \leq k^r} f_V \dim_k V > \tau r. \tag{3}$$

A witness is an $n \times L$ matrix whose columns are pairwise distinct codewords and whose rows satisfy the assigned constraints. This is ordinary LCL containment in the sense of JS [5].

Proposition 2.1 (Exact equivalence)**.** *Let $C \leq_k W^n$ and assume $\dim_k C \geq T$. Then C contains a profile in $\mathcal{P}_{\tau,T}$ if and only if it violates* (1) *for some subspace of dimension at most T.*

Proof. Suppose $A \leq_k C$ has dimension $r \leq T$ and $\sum_i \dim_k A_i > \tau r n$. Extend a basis of A to T independent codewords, obtaining an injective map $\phi : k^T \to C$ with $\phi(\mathsf{proj}_r(k^r)) = A$. Observe that the matrix whose columns consist of all outputs of ϕ

$$X = (\phi(x))_{x \in k^T}$$

has pairwise distinct columns. Let $\pi_i : W^n \to W$ denote the projection to the ith coordinate, and put $V_i = \ker(\pi_i \circ \phi \circ \mathsf{proj}_r)$. Therefore, by definition of the matrices $M_{r,V}$, row i satisfies M_{r,V_i}, and injectivity of ϕ and proj_r gives $\dim_k A_i = \dim_k V_i$. Thus the empirical frequencies of the V_i satisfy (3).

Conversely, let X be an LCL witness with constraint types for the rows prescribed by V_i. That is, the columns of X belong to C, and each row is the full table of a map $\lambda_i : k^T \to W$ with $\mathsf{proj}_r(V_i) \subseteq \ker \lambda_i$. Define the k-linear map $\phi\colon k^T \to W^n$ as $\phi(x) = (\lambda_i(x))_{i \in [n]}$. Its values are the columns of X, and the pairwise distinctness of X makes ϕ injective. Hence we see that $A = \phi(\mathsf{proj}_r(k^r))$ has dimension r, and

$$\dim_k A_i = \dim_k \ker(\lambda_i \circ \mathsf{proj}_r) \geq \dim_k V_i.$$

Equation (3) now gives a violation of (1). □

We now give a short proof sketch of theorem 1.1. Theorem 4.1 of [1] (random k-linear codes are subspace design codes) implies that $R_{\mathcal{P}_{\tau,T}} \geq \tau$. Therefore, putting $\tau = R + \varepsilon$ implies that there exist random k-linear codes of rate R that are $(R + \varepsilon, T)$ subspace design codes. Next, we note that the explicit constructions of [5] go through even when the inner code is linear over a subfield. This allows us to set the inner code as a subspace design code of the appropriate parameters, having constant block length. Moreover, we can take the alphabet size of the inner code to be at most $q_0^{\mathrm{poly}(T/\varepsilon)}$. On denoting this alphabet size by q, Corollary 6.1 of [5] implies that the final alphabet size is at most q^d, where

$$d = O\left(\frac{L^2 T^3_{\mathcal{P}_{\tau,T}}}{\varepsilon^5}\right).$$

Here, $T_{\mathcal{P}_{\tau,T}}$ denotes the maximum number of constraint types appearing in any profile description. This is upper bounded by the number of k-dimensional subspaces of k^T, which is at most $q_0^{T^2}$. Recall that the value of L was q_0^T. Plugging in everything, we get that the final alphabet size is at most $q_0^{\mathrm{poly}(1/\varepsilon) q_0^{O(T^2)}}$.

3 Conclusion

The full-table encoding shows that the violation of the subspace-design inequality is an ordinary LCL property, and the observation that the proofs of [5] work with an inner code over a folded alphabet with base-field linearity allows one to obtain explicit constructions. This recovers the main theorem of [2] with the same coarse alphabet dependence. We note that the proof of this result in GGH is more straightforward and clear, as the construction is targeted specifically towards the subspace design property.

References

[1] J. Brakensiek, Y. Chen, M. Dhar, and Z. Zhang, *From Random to Explicit via Subspace Designs with Applications to Local Properties and Matroids*, in *Proceedings of the 58th Annual ACM Symposium on Theory of Computing (STOC 2026)*, pages 619–630, 2026; arXiv:2510.13777.

[2] R. Goyal, V. Guruswami, and J.-T. Hsieh, *Explicit Constant-Alphabet Subspace Design Codes*, ECCC TR26-057, 2026; arXiv:2604.15218.

[3] V. Guruswami and S. Kopparty, *Explicit Subspace Designs*, *Combinatorica* 36(2):161–185, 2016.

[4] V. Guruswami and C. Xing, *List Decoding Reed–Solomon, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound*, in *Proceedings of STOC*, pp. 843–852, 2013.

[5] F. G. Jeronimo and N. Shagrithaya, *Probabilistic Guarantees to Explicit Constructions: Local Properties of Linear Codes*, in *Proceedings of the 58th Annual ACM Symposium on Theory of Computing (STOC 2026)*, pages 806–813, 2026; arXiv:2510.06185.

[6] M. Levi, J. Mosheiff, and N. Shagrithaya, *Random Reed–Solomon Codes and Random Linear Codes Are Locally Equivalent*, in *Proceedings of FOCS*, pp. 2097–2131, 2025; arXiv:2406.02238.

[7] Y. Chen and Z. Zhang, *Explicit Folded Reed–Solomon and Multiplicity Codes Achieve Relaxed Generalized Singleton Bounds*, in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC 2025)*, pages 1–12, 2025; arXiv:2408.15925.