Erratum to “Random Gabidulin Codes Achieve List Decoding Capacity in the Rank Metric” and “Gabidulin Codes Achieve List Decoding Capacity with an Order-Optimal Column-To-Row Ratio”

Zeyu Guo Chaoping Xing Chen Yuan Zihan Zhang

July 15, 2026

Summary of the correction. We thank Hengjia Wei for pointing out that, in the proof of Theorem 4.7 of the original paper [GXYZ24], the first inequality in each of the last two displays in Case 3 is invalid. More precisely, the inequality

$$\dim\left(\bigcap_{i\in\Omega} V_i'\right) \le \dim\left(\bigcap_{i\in\Omega} V_i\right)$$

need not hold, since intersections of subspaces may increase in dimension under a linear projection.

In this erratum, we provide a new proof showing that Theorem 4.7 of [GXYZ24], and its applications, remain valid under the additional assumption

$$q \ge m-1.$$

The new proof also allows us to simplify the definition of s-admissibility: all the subspaces V_i may now be taken to be subspaces of

$$\mathrm{span}_{\mathbb{F}_q}\{Z_1,\dots,Z_n\}.$$

The more general formulation in which their elements may be nonlinear polynomials is no longer needed.

We also give a new direct proof of Proposition 5.1, removing its dependence on Theorem 4.7. Consequently, the generic-intersection formula and the equivalence results in Sections 5 and 6 remain valid over every finite field.

As a consequence of the additional assumption $q \ge m-1$ in Theorem 4.7, Theorems 1.17 and 1.18 of [GXYZ24] require $q \ge k-1$, while Theorem 1.3 and Corollary 1.4 require $q \ge n-k-1$. In addition, the main positive result of the follow-up paper [GXYZ25], stated as Theorem 4 and proved in its detailed form as Theorem 23, requires the assumption $q \ge n-k-1$.

1 Updated Formulations

Define

$$\mathcal{L} := \mathrm{span}_{\mathbb{F}_q}\{Z_1,\dots,Z_n\} \quad \text{and} \quad \mathbb{F} := \mathbb{F}_q(Z_1,\dots,Z_n).$$

Definition 1.1 (s-admissibility, updated)**.** A tuple $(V_i)_{i\in[m]}$ of $\mathbb{F}_q$-subspaces of $\mathcal{L}$ is called s-*admissible* if

$$\dim_{\mathbb{F}_q}\left(\sum_{i=1}^m V_i\right) \le s.$$

For integers $k \geq m \geq 1$ and $s \geq 0$, let $\mathcal{V}_{k,m,s}$ be the set of tuples $\mathcal{S} = ((V_i, r_i))_{i \in [m]}$ such that $(V_i)_{i \in [m]}$ is s-admissible, $r_i \in \mathbb{N}^+$, $\dim(V_i) + r_i \leq k$ for $i \in [m]$, and $\sum_{i=1}^m r_i = k$.

For $\mathcal{S} = ((V_i, r_i))_{i \in [m]} \in \mathcal{V}_{k,m,s}$, set

$$f_i(X) := \prod_{\alpha \in V_i} (X - \alpha)^{q^{k - \dim(V_i) - r_i}}. \tag{1}$$

Thus f_i is a monic q-linearized polynomial of q-degree $k - r_i$. Define $M_{\mathcal{S}} \in \mathbb{F}^{k \times k}$ by taking, for each i, the coefficient vectors of

$$f_i(X), f_i(X)^q, \ldots, f_i(X)^{q^{r_i - 1}}$$

as the r_i rows of the i-th block of $M_{\mathcal{S}}$, exactly as in Definition 4.5 of the original paper [GXYZ24].

Theorem 1.2 (Theorem 4.7 of [GXYZ24], restated)**.** *Let $\mathcal{S} = ((V_i, r_i))_{i \in [m]} \in \mathcal{V}_{k,m,s}$ and assume $q \geq m - 1$. Then $\det(M_{\mathcal{S}}) \neq 0$ if and only if, for every nonempty $\Omega \subseteq [m]$,*

$$\dim\left(\bigcap_{i \in \Omega} V_i\right) + \sum_{i \in \Omega} r_i \leq \max_{i \in \Omega}\{\dim(V_i) + r_i\}. \tag{2}$$

We use the following elementary lemma.

Lemma 1.3 (A hyperplane avoiding finitely many subspaces)**.** *Let E be a finite-dimensional vector space over $\mathbb{F}_q$, and let $U, V_1, \ldots, V_t \subseteq E$ be subspaces such that $V_i \not\subseteq U$ for every $i \in [t]$. If $q \geq t$, then there exists a hyperplane $H \subseteq E$ such that*

$$U \subseteq H \qquad \text{and} \qquad V_i \not\subseteq H \quad \text{for every } i \in [t].$$

Proof. If U is already a hyperplane, take $H = U$. Otherwise, let $\overline{E} = E/U$ and let $\overline{V}_i$ be the image of V_i in $\overline{E}$. Each $\overline{V}_i$ is nonzero, so its annihilator $\overline{V}_i^{\perp}$ is a proper subspace of $\overline{E}^*$. These t proper subspaces cannot cover $\overline{E}^*$. Indeed, writing $d = \dim \overline{E}^*$ and counting the zero functional only once,

$$\left|\bigcup_{i=1}^{t} \overline{V}_i^{\perp}\right| \leq 1 + t(q^{d-1} - 1) \leq q^d - q + 1 < q^d.$$

Choose $\varphi \in \overline{E}^*$ outside this union, and let H be the preimage of $\ker \varphi$ under the quotient map $E \to \overline{E}$. Then H is a hyperplane containing U, and $\varphi|_{\overline{V}_i} \neq 0$ implies $V_i \not\subseteq H$ for every $i \in [t]$. ☐

2 Corrected Proof of Theorem 1.2

We will use the following characterization, which is Lemma 4.8 of the original paper [GXYZ24]:

$$\begin{aligned} \det(M_{\mathcal{S}}) = 0 \iff & \text{ there are } q\text{-linearized } g_i, \text{ not all zero, such that} \\ & \deg_q(g_i) \leq r_i - 1 \text{ for all } i \text{ and } \sum_i g_i \circ f_i = 0. \end{aligned} \tag{3}$$

Proof of Theorem 1.2. The "only if" direction is unchanged. We prove the converse by induction on (k, m, s) in lexicographic order. The cases $m = 1$ and $s = 0$ are immediate, exactly as in the original proof. Assume henceforth that $k \geq m \geq 2$, $s \geq 1$, and that (2) holds.

Case 1. Suppose that there is $\Omega_1 \subseteq [m]$ with $2 \le |\Omega_1| \le m-1$ such that

$$\dim\left(\bigcap_{i\in\Omega_1} V_i\right) + \sum_{i\in\Omega_1} r_i = \max_{i\in\Omega_1}\{\dim(V_i) + r_i\}. \tag{4}$$

Set

$$V_0 := \bigcap_{i\in\Omega_1} V_i, \qquad r_0 := \sum_{i\in\Omega_1} r_i, \qquad \Omega_2 := \{0\} \cup ([m] \setminus \Omega_1).$$

Choose a complement U of V_0 in $\mathcal{L}$ and put $V_i' := V_i \cap U$ for $i \in \Omega_1$. Then $V_i = V_0 \oplus V_i'$. Define

$$\mathcal{S}_1 := ((V_i', r_i))_{i\in\Omega_1}, \qquad \mathcal{S}_2 := ((V_i, r_i))_{i\in\Omega_2},$$

where the pair indexed by 0 is (V_0, r_0). The same dimension calculations as in the original Case 1 show that $\mathcal{S}_1 \in \mathcal{V}_{r_0,|\Omega_1|,s}$ and $\mathcal{S}_2 \in \mathcal{V}_{k,|\Omega_2|,s}$, and that both tuples satisfy (2). Since $r_0 < k$ and $|\Omega_2| < m$, induction gives

$$\det(M_{\mathcal{S}_1}) \neq 0, \qquad \det(M_{\mathcal{S}_2}) \neq 0. \tag{5}$$

Let

$$f_0(X) := \prod_{\alpha\in V_0} (X-\alpha)^{q^{k-\dim(V_0)-r_0}}.$$

For $i \in \Omega_1$, put

$$t_i := r_0 - \dim(V_i') - r_i \quad \text{and} \quad f_i^*(X) := \prod_{\gamma\in f_0(V_i')} (X-\gamma)^{q^{t_i}}.$$

Then $\deg_q(f_i^*) = r_0 - r_i$ and

$$f_i = f_i^* \circ f_0. \tag{6}$$

Although the spaces $f_0(V_i')$ need not consist of linear forms, no enlarged notion of admissibility is required. Indeed, choose bases $Y_1, \ldots, Y_h$ of V_0 and $X_1, \ldots, X_{n-h}$ of U. The assignment

$$Y_a \longmapsto Y_a, \qquad X_b \longmapsto f_0(X_b)$$

defines an injective endomorphism τ of $\mathbb{F}$. To see injectivity, note that $f_0(X_b)$ is monic in X_b with leading term $X_b^{q^{k-r_0}}$ and coefficients in $\mathbb{F}_q[Y_1, \ldots, Y_h]$; distinct leading monomials therefore remain distinct under the assignment. Since f_0 is q-linearized, $\tau(\beta) = f_0(\beta)$ for every $\beta \in U$.

Let $\mathcal{S}_1^* := ((f_0(V_i'), r_i))_{i\in\Omega_1}$, with the same matrix definition as above. Applying τ coefficientwise gives

$$M_{\mathcal{S}_1^*} = \tau(M_{\mathcal{S}_1}), \qquad \det(M_{\mathcal{S}_1^*}) = \tau(\det(M_{\mathcal{S}_1})) \neq 0$$

by (5) and injectivity of τ.

Now suppose that $\sum_{i=1}^m g_i \circ f_i = 0$ with $\deg_q(g_i) \le r_i - 1$. Define

$$g_0 := \sum_{i\in\Omega_1} g_i \circ f_i^*.$$

By $\deg_q(f_i^*) = r_0 - r_i$, we have $\deg_q(g_0) \le r_0 - 1$. Using (6),

$$g_0 \circ f_0 + \sum_{i\notin\Omega_1} g_i \circ f_i = 0.$$

The nonsingularity of $M_{\mathcal{S}_2}$ and (3) imply that $g_0 = 0$ and $g_i = 0$ for $i \notin \Omega_1$. Then $\sum_{i\in\Omega_1} g_i \circ f_i^* = 0$, and the nonsingularity of $M_{\mathcal{S}_1^*}$ implies $g_i = 0$ for all $i \in \Omega_1$. Thus $M_{\mathcal{S}}$ is nonsingular.

Case 2. Assume that for every $\Omega \subseteq [m]$ with $2 \le |\Omega| \le m-1$,

$$\dim\left(\bigcap_{i\in\Omega} V_i\right) + \sum_{i\in\Omega} r_i \le \max_{i\in\Omega}\{\dim(V_i) + r_i\} - 1. \tag{7}$$

This single case replaces Cases 2 and 3 of the original proof.

Let $E := \sum_{i=1}^m V_i$ and $d := \dim(E)$. The spaces V_i are pairwise distinct: if $V_i = V_j$, then (2) for $\Omega = \{i,j\}$ would give

$$\dim(V_i) + r_i + r_j \le \dim(V_i) + \max\{r_i, r_j\},$$

a contradiction.

After relabeling the subspaces if necessary, assume that $\dim(V_m) = \min_{i\in[m]} \dim(V_i)$. By minimality, $V_i \not\subseteq V_m$ for every $i < m$. Since $q \ge m-1$, Lemma 1.3 yields a hyperplane $H \subseteq E$ such that

$$V_m \subseteq H \quad \text{and} \quad V_i \not\subseteq H \quad \text{ for } i < m.$$

Choose a basis $X_1, \dots, X_{d-1}$ of H and extend it by X_d to a basis of E. Put

$$V_i' := V_i \cap H.$$

Then $V_m' = V_m$, while $\dim(V_i') = \dim(V_i) - 1$ for $i < m$. For each $i < m$, after scaling a vector outside H, we may write

$$V_i = V_i' \oplus \operatorname{span}_{\mathbb{F}_q}\{X_d + v_i\} \qquad \text{for some } v_i \in H. \tag{8}$$

Set $k' := k - 1$. If $r_m > 1$, define

$$r_i' := r_i \text{ for } i < m, \qquad r_m' := r_m - 1, \qquad \mathcal{S}' := ((V_i', r_i'))_{i\in[m]}.$$

Every quantity $\dim(V_i') + r_i'$ equals $\dim(V_i) + r_i - 1$. For $2 \le |\Omega| \le m-1$, (7) gives

$$\dim\left(\bigcap_{i\in\Omega} V_i'\right) + \sum_{i\in\Omega} r_i' \le \max_{i\in\Omega}\{\dim(V_i') + r_i'\}.$$

For $\Omega = [m]$, the same conclusion follows from (2) after subtracting one from both $\sum_i r_i = k$ and the maximum. Thus $\mathcal{S}' \in \mathcal{V}_{k',m,s-1}$ satisfies (2).

If $r_m = 1$, instead define

$$\mathcal{S}' := ((V_i', r_i))_{i\in[m-1]}.$$

Here $\sum_{i<m} r_i = k'$. For every $\Omega \subseteq [m-1]$ with $|\Omega| \ge 2$, (7) gives (2) for $\mathcal{S}'$, while singleton sets are automatic. Hence $\mathcal{S}' \in \mathcal{V}_{k',m-1,s-1}$ satisfies (2). In either subcase, induction gives

$$\det(M_{\mathcal{S}'}) \ne 0. \tag{9}$$

It remains to derive a contradiction from a hypothetical relation in (3). Extend $X_1, \dots, X_d$ to a basis of $\mathcal{L}$ and regard $T := X_d$ as an indeterminate over

$$K := \mathbb{F}_q(X_1, \dots, X_{d-1}, X_{d+1}, \dots, X_n).$$

For $i < m$, write

$$a_i := k - \dim(V_i) - r_i.$$

By (8), every element of V_i can be written uniquely as $\alpha + \lambda(T + v_i)$ with $\alpha \in V_i'$ and $\lambda \in \mathbb{F}_q$. Therefore,

$$\begin{aligned} f_i(X) &= \prod_{\alpha \in V_i'} \prod_{\lambda \in \mathbb{F}_q} (X - \alpha - \lambda(T + v_i))^{q^{a_i}} \\ &= \prod_{\alpha \in V_i'} \Big((X-\alpha)^q - (X-\alpha)(T+v_i)^{q-1}\Big)^{q^{a_i}} \\ &= \prod_{\alpha \in V_i'} \Big((X-\alpha)^{q^{a_i+1}} - (X-\alpha)^{q^{a_i}}(T+v_i)^{(q-1)q^{a_i}}\Big). \end{aligned} \tag{10}$$

Here the second equality uses

$$\prod_{\lambda \in \mathbb{F}_q} (Y - \lambda Z) = Y^q - YZ^{q-1}.$$

Viewing f_i as a polynomial in T with coefficients in $K[X]$, each factor in (10) has T-degree $(q-1)q^{a_i}$ and leading coefficient $-(X-\alpha)^{q^{a_i}}$. Since

$$|V_i'| = q^{\dim(V_i)-1},$$

we obtain

$$\deg_T(f_i) = |V_i'|(q-1)q^{a_i} = (q-1)q^{k-r_i-1}.$$

Moreover, if $\mathrm{lc}_T(f_i)$ denotes the leading coefficient of f_i with respect to T, then

$$\begin{aligned} \mathrm{lc}_T(f_i) &= (-1)^{|V_i'|} \prod_{\alpha \in V_i'} (X-\alpha)^{q^{a_i}} \\ &= \lambda_i h_i(X), \end{aligned} \tag{11}$$

where $\lambda_i := (-1)^{|V_i'|} \in \mathbb{F}_q^\times$ and

$$h_i(X) := \prod_{\alpha \in V_i'} (X-\alpha)^{q^{k' - \dim(V_i') - r_i}} = \prod_{\alpha \in V_i'} (X-\alpha)^{q^{a_i}}.$$

Thus h_i is exactly the polynomial corresponding to (V_i', r_i) in the smaller instance $\mathcal{S}'$.

If $r_m > 1$, let h_m be the polynomial associated with (V_m', r_m') in $\mathcal{S}'$; then $h_m = f_m$. If $r_m = 1$, set $h_m := f_m$ for notational convenience. In either case h_m is independent of T.

Suppose that

$$\sum_{i=1}^{m} g_i \circ f_i = 0, \qquad \deg_q(g_i) \le r_i - 1,$$

with the g_i not all zero. Write

$$g_i(X) = \sum_{j=0}^{r_i-1} c_{i,j}(T) X^{q^j}, \qquad c_{i,j}(T) \in K(T).$$

After multiplying the relation by a common nonzero denominator, we may assume that $c_{i,j}(T) \in K[T]$ for all i, j. For $i < m$, set

$$\delta_i := \deg_T(f_i) = (q-1)q^{k-r_i-1},$$

and set $\delta_m := 0$. Then

$$\deg_T(f_i(X)^{q^j}) = q^j \delta_i.$$

For every pair (i, j) with $c_{i,j} \neq 0$, define

$$D_{i,j} := \deg_T(c_{i,j}) + q^j \delta_i,$$

and let

$$D := \max_{i,j \colon c_{i,j} \neq 0} D_{i,j}.$$

For $i < m$, let λ_i be as in (11), and set $\lambda_m := 1$. Define

$$\gamma_{i,j} := \begin{cases} \mathrm{lc}_T(c_{i,j}) \lambda_i^{q^j}, & \text{if } c_{i,j} \neq 0 \text{ and } D_{i,j} = D, \\ 0, & \text{otherwise.} \end{cases}$$

and

$$\overline{g}_i(X) := \sum_{j=0}^{r_i - 1} \gamma_{i,j} X^{q^j}.$$

Since

$$\mathrm{lc}_T(f_i(X)^{q^j}) = \lambda_i^{q^j} h_i(X)^{q^j},$$

taking the coefficient of T^D in $\sum_i g_i \circ f_i = 0$ gives

$$\sum_{i=1}^{m} \overline{g}_i \circ h_i = 0. \tag{12}$$

At least one $\gamma_{i,j}$ is nonzero by the definition of D, so the polynomials $\overline{g}_i$ are not all zero. Moreover,

$$\deg_q(\overline{g}_i) \leq r_i - 1 \qquad \text{for every } i \in [m].$$

For $i < m$,

$$\deg_q(h_i) = k' - r_i = k - 1 - r_i,$$

so

$$\deg_q(\overline{g}_i \circ h_i) \leq k - 2. \tag{13}$$

If $r_m > 1$, then

$$\deg_q(h_m) = k' - r'_m = k - r_m.$$

Consequently, if $\deg_q(\overline{g}_m) = r_m - 1$, the term $\overline{g}_m \circ h_m$ has q-degree $k - 1$, contradicting (12) and (13). Hence

$$\deg_q(\overline{g}_m) \leq r_m - 2 = r'_m - 1.$$

Thus (12) is a nontrivial relation of the form forbidden by (9).

If $r_m = 1$, then a nonzero $\overline{g}_m \circ f_m$ would have q-degree $k - 1$, whereas all other terms have q-degree at most $k - 2$. Therefore $\overline{g}_m = 0$, and (12) restricts to a nontrivial relation for the tuple indexed by $[m - 1]$, again contradicting (9).

This completes the induction and the proof. $\square$

3 A New Direct Proof of Proposition 5.1

Proposition 5.1 of [GXYZ24], which states that a generic linear code attains every generic kernel pattern, remains valid over every finite field. Its proof should be replaced by the following direct argument.

Proposition 3.1 (Proposition 5.1 of [GXYZ24], unchanged)**.** *Let $W = (Z_{a,b})_{a\in[k],b\in[n]}$ be the generic $k \times n$ matrix over*

$$K := \mathbb{F}_q(Z_{a,b} : a \in [k], b \in [n]).$$

Then the $[n,k]_K$ code generated by W attains every generic kernel pattern. Consequently, it is $\mathrm{GKP}(\ell)$ *for every $\ell \geq 1$.*

Proof. Let $(V_1, \dots, V_k)$ be a generic kernel pattern. As in the original proof, the vector-space Hall theorem allows us to enlarge the V_i while preserving genericity, so we may assume

$$\dim(V_i) = k - 1 \qquad \text{for } i \in [k].$$

Set $E := \mathbb{F}_q^n$ and $U_i := V_i^{\perp}$, so $\dim(U_i) = n - k + 1$. For fixed i, let

$$\pi_i : E \longrightarrow E/U_i$$

be the quotient map. For every $\Omega \subseteq [k] \setminus \{i\}$,

$$\begin{aligned} \dim\left(\sum_{j\in\Omega} \pi_i(U_j)\right) &= \dim\left(U_i + \sum_{j\in\Omega} U_j\right) - \dim(U_i) \\ &= k - 1 - \dim\left(\bigcap_{j\in\Omega\cup\{i\}} V_j\right) \\ &\geq |\Omega|. \end{aligned} \tag{14}$$

The last inequality is precisely the generic-kernel-pattern condition. Hence, by the vector-space Hall theorem, for each fixed i one can choose a vector from every U_j, $j \neq i$, whose images under π_i are linearly independent.

Choose a basis $(b_{j,a})_a$ of each U_j, introduce algebraically independent variables $T_{j,a}$, and let

$$u_j := \sum_a T_{j,a} b_{j,a} \in U_j \otimes_{\mathbb{F}_q} K_0, \qquad K_0 := \mathbb{F}_q(T_{j,a} : j, a).$$

For fixed i, the determinant expressing the linear independence of $(\pi_i(u_j))_{j\neq i}$ is a nonzero polynomial by (14). The product of these k determinant polynomials is therefore nonzero. Thus, over K_0, the generic choices $u_1, \dots, u_k$ simultaneously satisfy

$$\operatorname{span}_{K_0}\{u_j : j \neq i\} \cap (U_i \otimes_{\mathbb{F}_q} K_0) = \{0\} \qquad \text{for } i \in [k]. \tag{15}$$

Let $B \in K_0^{k\times n}$ be the matrix whose i-th row is u_i. The matrix B has full row rank: indeed, each u_i is nonzero and lies in U_i, while (15) implies that the span of the other rows meets U_i trivially, and hence u_i is not in that span.

For each i, choose $A_i \in \mathbb{F}_q^{n\times(k-1)}$ with column space V_i. Since $u_i \in V_i^{\perp}$, the i-th row of BA_i is zero. On the other hand, deleting this row gives an invertible $(k-1) \times (k-1)$ matrix: a linear dependence among the remaining rows after restriction to V_i would give a nonzero vector in

$$\operatorname{span}_{K_0}\{u_j : j \neq i\} \cap (U_i \otimes_{\mathbb{F}_q} K_0),$$

contrary to (15).

For the generic matrix W, define a row vector $m_i(W)$ by the signed maximal minors of WA_i:

$$(m_i(W))_r := (-1)^{r+1}\det\big((WA_i)_{\widehat{r}}\big), \qquad r \in [k],$$

where $(WA_i)_{\widehat{r}}$ denotes the matrix obtained by deleting row r. The cofactor identity gives

$$m_i(W)WA_i = 0.$$

Let $M(W)$ be the $k \times k$ matrix whose i-th row is $m_i(W)$. At the specialization $W = B$, the preceding paragraph shows that

$$m_i(B) = c_i e_i \qquad \text{for some } c_i \in K_0^{\times}.$$

Therefore

$$\det M(B) = \prod_{i=1}^{k} c_i \neq 0.$$

It follows that $\det M(W)$ is a nonzero polynomial, so $M(W)$ is invertible over K and the code generated by W attains $(V_1, \ldots, V_k)$. The generic code is also MRD, as established independently in Section 2 of the original paper. This proves the proposition. $\square$

Consequently, in [GXYZ24], Proposition 5.1 and all results derived from it remain valid without any restriction on q. In particular, Theorem 1.16, Theorem 1.13, Theorem 1.14, Corollary 1.15, and all intermediate results in Sections 5 and 6 are unchanged.

References

[GXYZ24] Zeyu Guo, Chaoping Xing, Chen Yuan, and Zihan Zhang. Random Gabidulin codes achieve list decoding capacity in the rank metric. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1846–1873. IEEE, 2024.

[GXYZ25] Zeyu Guo, Chaoping Xing, Chen Yuan, and Zihan Zhang. Gabidulin codes achieve list decoding capacity with an order-optimal column-to-row ratio. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2025)*, pages 43–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2025.