Electronic Colloquium on Computational Complexity, Report No. 152 (2024)

THE COMMUNICATION COMPLEXITY OF APPROXIMATING MATRIX RANK

ALEXANDER A. SHERSTOV AND ANDREY A. STOROZHENKO

Abstract. We fully determine the communication complexity of approximating matrix rank, over any finite field $\mathbb{F}$. We study the most general version of this problem, where $0 \leqslant r < R \leqslant n$ are given integers, Alice and Bob's inputs are matrices $A, B \in \mathbb{F}^{n\times n}$, respectively, and they need to distinguish between the cases $\mathrm{rk}(A+B) = r$ and $\mathrm{rk}(A+B) = R$. We show that this problem has randomized communication complexity $\Omega(1 + r^2 \log|\mathbb{F}|)$. This is optimal in a strong sense because $O(1 + r^2 \log|\mathbb{F}|)$ communication is sufficient to determine, for arbitrary A, B, whether $\mathrm{rk}(A+B) \leqslant r$. Prior to our work, lower bounds were known only for *consecutive* integers r and R, with no implication for the approximation of matrix rank. Our lower bound holds even for quantum protocols and even for error probability $\frac{1}{2} - \frac{1}{4}|\mathbb{F}|^{-r/3}$, which too is virtually optimal because the problem has a two-bit classical protocol with error $\frac{1}{2} - \Theta(|\mathbb{F}|^{-r})$.

As an application, we obtain an $\Omega(\frac{1}{k} \cdot n^2 \log|\mathbb{F}|)$ space lower bound for any streaming algorithm with k passes that approximates the rank of an input matrix $M \in \mathbb{F}^{n\times n}$ within a factor of $\sqrt{2} - \delta$, for any $\delta > 0$. Our result is an exponential improvement in k over previous work.

We also settle the randomized and quantum communication complexity of several other linear-algebraic problems, for all settings of parameters. This includes the *determinant problem* (given matrices A and B, distinguish between the cases $\det(A+B) = a$ and $\det(A+B) = b$, for fixed field elements $a \neq b$) and the *subspace sum* and *subspace intersection problem* (given subspaces S and T of known dimensions m and ℓ, respectively, approximate the dimensions of $S+T$ and $S \cap T$).

* Computer Science Department, UCLA, Los Angeles, CA 90095. Supported by NSF grant CCF-2220232.

✉ {sherstov,storozhenko}@cs.ucla.edu .

ISSN 1433-8092

Contents

1. Introduction

The exact and approximate computation of matrix rank is a fundamental problem in theoretical computer science, studied for its intrinsic importance as well as its connections to other algorithmic and complexity-theoretic questions. In particular, a large body of research has focused on the communication complexity of the matrix rank problem in Yao's two-party model [29, 30], with both classical and quantum communication. In this problem, the two parties Alice and Bob receive matrices $A, B \in \mathbb{F}^{n\times n}$, respectively, over a finite field $\mathbb{F}$ and are tasked with determining the rank of $A + B$ using minimal communication. The first result in this line of research was obtained three decades ago by Chu and Schnitger [6], who proved a lower bound of $\Omega(kn^2)$ for the deterministic communication complexity of computing the rank of $A + B$ when the matrix entries are k-bit integers. Several years later, Chu and Schnitger [7] further showed that this communication problem has deterministic complexity $\Omega(n^2 \log p)$ when the matrix entries are in $\mathbb{F}_p$, the finite field with p elements. The first result on the *randomized* communication complexity of the matrix rank problem was obtained by Sun and Wang [27], who proved that determining whether $A+B$ is singular requires $\Omega(n^2 \log p)$ bits of communication for matrices A, B over the finite field $\mathbb{F}_p$ for prime p. In a follow-up paper, Li, Sun, Wang, and Woodruff [16] showed that this $\Omega(n^2 \log p)$ lower bound holds even for a promise version of the matrix rank problem, where the matrix $A + B$ is guaranteed to have rank either $n - 1$ or n. The lower bounds of [27, 16] further apply to quantum communication.

Despite these exciting developments, no progress has been made on lower bounds for *approximating* matrix rank. Our main contribution is the complete resolution of the approximate matrix rank problem. In what follows, we state our results for matrix rank and several other approximation problems, and present applications of our work to streaming complexity.

1.1. Matrix rank problem.

We study the problem of approximating matrix rank in its most general form. Specifically, let $\mathbb{F}$ be any finite field. For integer parameters n, m, R, r such that $\min\{n, m\} \geqslant R > r \geqslant 0$, we consider the promise communication problem defined on pairs of matrices $A, B \in \mathbb{F}^{n\times m}$ by

$$\mathrm{RANK}_{r,R}^{\mathbb{F},n,m}(A, B) = \begin{cases} -1 & \text{if } \mathrm{rk}(A + B) = r, \\ 1 & \text{if } \mathrm{rk}(A + B) = R, \\ * & \text{otherwise,} \end{cases}$$

where the asterisk indicates that the communication protocol is allowed to exhibit arbitrary behavior when $\mathrm{rk}(A + B) \notin \{r, R\}$. In words, the problem amounts to distinguishing input pairs with $\mathrm{rk}(A+B) = r$ from those with $\mathrm{rk}(A+B) = R$. The corresponding *total* communication problem is given by

$$\mathrm{RANK}_{r}^{\mathbb{F},n,m}(A, B) = \begin{cases} -1 & \text{if } \mathrm{rk}(A + B) \leqslant r, \\ 1 & \text{otherwise.} \end{cases}$$

Clearly, the total problem $\mathrm{RANK}_{r}^{\mathbb{F},n,m}$ is more challenging than the promise problem $\mathrm{RANK}_{r,R}^{\mathbb{F},n,m}$. Prior to our work, the strongest known result was the $\Omega(n^2 \log p)$ lower bound of [16] on the bounded-error quantum communication complexity of $\mathrm{RANK}_{n-1,n}^{\mathbb{F}_p,n,n}$ for fields $\mathbb{F}_p$ of prime order. Unfortunately, this lower bound has no implications for the approximation of matrix rank because the ratio $(n-1)/n$ rapidly tends to 1. We resolve this question in full in the following theorem.

Theorem 1.1 (Lower bound for rank problem). *There is an absolute constant $c > 0$ such that for all finite fields $\mathbb{F}$ and all integers n, m, R, r with $\min\{n, m\} \geqslant R > r \geqslant 0$,*

$$Q^*_{\frac{1}{2}-\frac{1}{4|\mathbb{F}|^{r/3}}}(\mathrm{RANK}_{r,R}^{\mathbb{F},n,m}) \geqslant c(1 + r^2 \log |\mathbb{F}|).$$

In particular,

$$Q^*_{1/4}(\mathrm{RANK}^{\mathbb{F},n,m}_{r,R}) \geqslant c(1 + r^2 \log |\mathbb{F}|).$$

In the statement above, Q^*_ε denotes ε-error quantum communication complexity with arbitrary prior entanglement, which is the most powerful model of probabilistic computation. Clearly, all our lower bounds apply to the randomized (classical) model as well. Two other remarks are in order. Even in the special case of $r = n - 1$ and $R = n$, our result is a significant improvement on previous work because our theorem is proved in the *large-error regime,* with the error probability exponentially close to $1/2$. This should be contrasted with the communication lower bounds of [27, 16], which were proved for error probability $1/3$. Moreover, Theorem 1.1 is the first result of its kind because it allows for an arbitrary gap between r and R. In particular, Theorem 1.1 shows for the first time that approximating the matrix rank to any constant factor requires $\Omega(n^2 \log |\mathbb{F}|)$ bits of communication, even for protocols that succeed with exponentially small probability (take $R = n$ and $r = cn$ for a small constant $c > 0$).

Theorem 1.1 is optimal in a strong sense. Specifically, we have the following matching upper bound, which we prove by adapting Clarkson and Woodruff's streaming algorithm for matrix rank [9]. In the statement below, R_ε denotes randomized (classical) communication complexity with error ε.

THEOREM 1.2 (Upper bound for rank problem). *There is an absolute constant $c > 0$ such that for all finite fields $\mathbb{F}$ and all integers n, m, r with $\min\{n, m\} > r \geqslant 0$,*

$$R_{1/3}(\mathrm{RANK}^{\mathbb{F},n,m}_r) \leqslant c(1 + r^2 \log |\mathbb{F}|),$$
$$R_{\frac{1}{2} - \frac{1}{32|\mathbb{F}|^r}}(\mathrm{RANK}^{\mathbb{F},n,m}_r) \leqslant 2.$$

This result shows that the lower bound of Theorem 1.1 is tight not only for quantum protocols solving the partial problem $\mathrm{RANK}^{\mathbb{F},n,m}_{r,R}$ but even for *classical*, *bounded-error* protocols solving the *total* problem $\mathrm{RANK}^{\mathbb{F},n,m}_r$. Moreover, Theorem 1.2 shows that the error regime for which we prove our lower bound in Theorem 1.1 is also optimal, in that the total rank problem has a classical protocol with cost only 2 bits and error probability $\frac{1}{2} - |\mathbb{F}|^{-\Theta(r)}$.

Theorem 1.1 generalizes to multiparty communication, as we discuss below in Section 1.5.

1.2. Streaming complexity. The streaming complexity of matrix rank has received extensive attention in the literature [9, 27, 16, 4, 1, 2, 5]. In this model, an algorithm with limited space is presented with a matrix M of order n over a given field, in row-major order. The objective is to compute or approximate the rank of M, using either a single pass or multiple passes over M. Via standard reductions, our Theorem 1.1 implies an essentially optimal lower bound on the streaming complexity of approximating matrix rank. Unlike previous work, our result remains valid even for polynomially many passes and even for correctness probability exponentially close to $1/2$. Stated in its most general form, our result is as follows.

THEOREM 1.3. *Let n, r, R be nonnegative integers with $n/2 \leqslant r < R \leqslant n$, and let $\mathbb{F}$ be a finite field. Define $f\colon \mathbb{F}^{n\times n} \to \{-1, 1, *\}$ by*

$$f(M) = \begin{cases} -1 & \text{if } \operatorname{rk} M = r, \\ 1 & \text{if } \operatorname{rk} M = R, \\ * & \text{otherwise.} \end{cases}$$

Let $\mathscr{A}$ be any randomized streaming algorithm for f with error probability $\frac{1}{2} - \frac{1}{4}|\mathbb{F}|^{-(r-\lceil n/2 \rceil)/3}$ that uses k passes and space s. Then

$$sk = \Omega\left(\left(r - \left\lceil \frac{n}{2} \right\rceil\right)^2 \log|\mathbb{F}|\right).$$

By way of notation, recall that f in the above statement is a *partial* function, and $\mathscr{A}$ is allowed to exhibit arbitrary behavior on matrices M where $f(M) = *$.

COROLLARY 1.4. *Let $\mathbb{F}$ be a finite field, and let $\delta \in (1/2, 1)$ be any constant. Let $\mathscr{A}$ be a k-pass streaming algorithm that takes as input a matrix $M \in \mathbb{F}^{n \times n}$ (for any $n \geqslant \frac{5}{\delta - 0.5}$) such that either $\operatorname{rk} M = n$ or $\operatorname{rk} M = \lfloor \delta n \rfloor$, and determines which is the case with probability of correctness at least $\frac{1}{2} + |\mathbb{F}|^{-(\delta - 0.5)n/5}$. Then $\mathscr{A}$ uses $\Omega(\frac{1}{k} \cdot n^2 \log|\mathbb{F}|)$ space.*

Proof. Take $R = n$ and $r = \lfloor \delta n \rfloor$ in Theorem 1.3. ∎

The space lower bound in Corollary 1.4 is essentially optimal since the rank of a matrix $M \in \mathbb{F}^{n \times n}$ can be computed exactly by a trivial, single-pass algorithm with space $O(n^2 \log|\mathbb{F}|)$. Prior to our work, the strongest streaming lower bound for approximating matrix rank was due to Chen et al. [5]. For any constants $\varepsilon > 0$ and $\delta > 0$, they proved that no $o(\sqrt{\log n})$-pass algorithm with space $n^{2-\varepsilon}$ can distinguish between the cases $\operatorname{rk} M = n$ and $\operatorname{rk} M \leqslant \delta n$ with probability $2/3$, where M is an input matrix of order n over a finite field of size $\omega(n)$. Our Corollary 1.4 shows that distinguishing between the cases $\operatorname{rk} M = n$ and $\operatorname{rk} M = \lfloor \delta n \rfloor$ requires $n^{2-\varepsilon} \log|\mathbb{F}|$ space even with $k = \Theta(n^\varepsilon)$ passes, an exponential improvement on [5]. Moreover, Corollary 1.4 is valid for all finite fields regardless of size, and holds even when the correctness probability is exponentially close to $1/2$.

We now restate our streaming lower bound in more standard terminology. Recall that an algorithm $\mathscr{A}$ with input $M \in \mathbb{F}^{n \times n}$ approximates, with probability p, the rank of M within a factor of $c \in [1, \infty)$ if for every input matrix M, the output of $\mathscr{A}$ is in the range $[\frac{1}{c} \operatorname{rk} M, c \operatorname{rk} M]$ with probability at least p. We have:

COROLLARY 1.5. *Let $\mathbb{F}$ be a finite field, and let $c \in [1, \sqrt{2})$ be any constant. Let $\mathscr{A}$ be a k-pass streaming algorithm with input $M \in \mathbb{F}^{n \times n}$ (for any $n \geqslant \frac{40}{2 - c^2}$) that approximates, with probability at least $\frac{1}{2} + |\mathbb{F}|^{-(2-c^2)n/40}$, the rank of M within a factor of c. Then $\mathscr{A}$ uses $\Omega(\frac{1}{k} \cdot n^2 \log|\mathbb{F}|)$ space.*

Proof. Define $\delta = \frac{1}{2}(\frac{1}{2} + \frac{1}{c^2})$. Since $\delta < 1/c^2$, algorithm $\mathscr{A}$ can be used to distinguish, with correctness probability at least $\frac{1}{2} + |\mathbb{F}|^{-(2-c^2)n/40}$, matrices $M \in \mathbb{F}^{n \times n}$ of rank $\lfloor \delta n \rfloor$ from those of rank n (simply check if $\mathscr{A}$'s output is $< n/c$ or $\geqslant n/c$). The correctness probability of this distinguisher exceeds $\frac{1}{2} + |\mathbb{F}|^{-(\lfloor \delta n \rfloor - \lceil n/2 \rceil)/3}$ due to $n \geqslant 40/(2 - c^2)$. Therefore, it uses $\Omega(\frac{1}{k} \cdot n^2 \log|\mathbb{F}|)$ space by Theorem 1.3. ∎

1.3. Determinant problem. Recall that a square matrix over a field $\mathbb{F}$ has full rank if and only if its determinant is nonzero. As a result, the problem of computing the determinant has received considerable attention in previous work on matrix rank, e.g., [7, 27, 16]. We are interested in the most general form of the determinant problem, where Alice and Bob receive as input matrices $A, B \in \mathbb{F}^{n \times n}$, respectively, and need to determine whether the determinant of $A + B$ equals a or b. The problem parameters a and b are distinct field elements that are fixed in advance. Formally, the determinant problem is the partial communication problem on matrix pairs (A, B) given by

$$\mathrm{DET}_{a,b}^{\mathbb{F},n}(A, B) = \begin{cases} -1 & \text{if } \det(A + B) = a, \\ 1 & \text{if } \det(A + B) = b, \\ * & \text{otherwise.} \end{cases}$$

Prior to our work, the strongest result on the determinant problem was due to Sun and Wang [27], who proved a tight lower bound of $\Omega(n^2 \log |\mathbb{F}|)$ for the randomized and quantum communication complexity of $\mathrm{DET}_{a,b}^{\mathbb{F},n}$ for nonzero a, b over any finite field $\mathbb{F}$ of prime order. They conjectured the same lower bound for the case of arbitrary a, b. To see why the case of nonzero a, b is rather special, observe that the number of matrices with determinant a is always the same as the number of matrices with determinant b, with natural bijections between these two sets; but this is no longer true if one of a, b is zero. This asymmetry suggests that the determinant problem requires a substantially different approach when one of a, b is zero. In this work, we develop sufficiently strong techniques to solve the determinant problem in full, thereby settling Sun and Wang's conjecture in the affirmative.

THEOREM 1.6. *There is an absolute constant $c > 0$ such that for every finite field $\mathbb{F}$, every pair of distinct elements $a, b \in \mathbb{F}$, and all integers $n \geqslant 2$,*

$$Q^*_{\frac{1}{2} - \frac{1}{4|\mathbb{F}|^{(n-1)/3}}}(\mathrm{DET}_{a,b}^{\mathbb{F},n}) \geqslant cn^2 \log |\mathbb{F}|.$$

The communication lower bound of Theorem 1.6 is best possible, up to the multiplicative constant c. It matches the trivial, deterministic protocol where Alice sends her input matrix A to Bob using $n^2 \lceil \log |\mathbb{F}| \rceil$ bits, at which point Bob computes $\det(A+B)$ and announces the output of the protocol. Furthermore, the error regime in Theorem 1.6 is also essentially optimal because, for example, the problem $\mathrm{DET}_{0,b}^{\mathbb{F},n}$ has a randomized protocol with only 2 bits of communication and error probability $\frac{1}{2} - \Theta(|\mathbb{F}|^{n-1})$, by taking $r = n - 1$ and $R = m = n$ in Theorem 1.2. Lastly, we note that the requirement that $n \geqslant 2$ in Theorem 1.6 is also necessary because the determinant problem for 1×1 matrices reduces to the equality problem with domain $\mathbb{F} \times \mathbb{F}$ and therefore has randomized communication complexity $O(1)$.

We prove Theorem 1.6 for all a, b from first principles, without relying on the work of Sun and Wang [27]. In the case of nonzero a, b, we give a new proof that is quite short and uses only basic Fourier analysis, unlike the rather technical proof of [27]. To settle the complementary case where one of a, b is zero, we prove a stronger result of independent interest. Here, we introduce a natural problem that we call $\mathrm{RANKDET}_{r,a}^{\mathbb{F},n}$, which combines features of the matrix rank and determinant problems. It is parameterized by a nonzero field element $a \in \mathbb{F}$ and a nonnegative integer $r < n$, and Alice and Bob's objective is to distinguish input pairs (A, B) with $\mathrm{rk}(A + B) = r$ from those with $\det(A + B) = a$. We prove the following.

THEOREM 1.7. *There is an absolute constant $c > 0$ such that for every finite field $\mathbb{F}$, every field element $a \in \mathbb{F} \setminus \{0\}$, and all integers $n > r \geqslant 0$,*

$$Q^*_{\frac{1}{2} - \frac{1}{4|\mathbb{F}|^{r/3}}}(\mathrm{RANKDET}_{r,a}^{\mathbb{F},n}) \geqslant c(1 + r^2 \log |\mathbb{F}|).$$

Taking $r = n-1$ in this result settles Theorem 1.6 when one of a, b is zero, as desired. Theorem 1.7 is optimal in a strong sense: even the *total* problem $\mathrm{RANK}_{r}^{\mathbb{F},n,n}$, which subsumes $\mathrm{RANKDET}_{r,a}^{\mathbb{F},n}$, has bounded-error classical communication complexity $O(1 + r^2 \log |\mathbb{F}|)$ by Theorem 1.2. Theorem 1.7 for the $\mathrm{RANKDET}_{r,a}^{\mathbb{F},n}$ problem significantly strengthens our main result, Theorem 1.1, for the matrix rank problem $\mathrm{RANK}_{r,n}^{\mathbb{F},n,n}$ (in the former problem, Alice and Bob distinguish rank r from determinant $a \neq 0$; in the latter problem, they distinguish rank r from rank n).

Theorems 1.6 and 1.7 generalize to multiparty communication, as we discuss below in Section 1.5.

1.4. Subspace sum and intersection problems. There are two natural ways to recast the computation of matrix rank as a communication problem. One approach, discussed in detail above, is to assign matrices A and B to Alice and Bob, respectively, and require them to compute the rank of $A + B$. Alternatively, one can require Alice and Bob to compute the rank of the matrix $\begin{bmatrix} A & B \end{bmatrix}$.

This alternative approach is best described in the language of linear subspaces: letting S and T stand for the column space of A and B, respectively, the rank of $\begin{bmatrix} A & B \end{bmatrix}$ is precisely the dimension of the linear subspace $S + T$ generated by S and T. Here, we may assume that the dimensions of S and T are known in advance because this information can be communicated at negligible cost.

In this way, one arrives at the *subspace sum problem* over a finite field $\mathbb{F}$, where Alice receives as input an m-dimensional linear subspace $S \subseteq \mathbb{F}^n$ and Bob receives an ℓ-dimensional linear subspace $T \subseteq \mathbb{F}^n$. The integers m and ℓ are part of the problem specification and are fixed in advance. In the promise version of the subspace sum problem, the objective is to distinguish subspace pairs with $\dim(S + T) = d_1$ from those with $\dim(S + T) = d_2$, for distinct integers d_1, d_2 fixed in advance. This corresponds to the partial function given by

$$\mathrm{SUM}_{d_1,d_2}^{\mathbb{F},n,m,\ell}(S,T) = \begin{cases} -1 & \text{if } \dim(S+T) = d_1, \\ 1 & \text{if } \dim(S+T) = d_2, \\ * & \text{otherwise.} \end{cases}$$

The corresponding total communication problem is that of determining whether $S+T$ has dimension at most d, for an integer d fixed in advance:

$$\mathrm{SUM}_{d}^{\mathbb{F},n,m,\ell}(S,T) = \begin{cases} -1 & \text{if } \dim(S+T) \leqslant d, \\ 1 & \text{otherwise.} \end{cases}$$

The total problem is more challenging than the promise problem in that $\mathrm{SUM}_{d_1,d_2}^{\mathbb{F},n,m,\ell}$ is a restriction of $\mathrm{SUM}_{d_1}^{\mathbb{F},n,m,\ell}$, for any integers $d_1 < d_2$. As noted by many authors, from the standpoint of communication complexity, computing the dimension of the subspace sum $S + T$ is equivalent to computing the dimension of the subspace intersection $S \cap T$. This equivalence follows from the identity $\dim(S + T) = \dim(S) + \dim(T) - \dim(S \cap T)$.

Despite the syntactic similarity between the matrix sum $A + B$ and the corresponding subspace sum $S + T$, the subspace sum problem appears to be significantly more subtle and technical. Previous work has focused on a special case that we call *subspace disjointness* (determining whether Alice and Bob's subspaces have trivial intersection, $\{0\}$) and the dual problem that we call *vector space span* (determining if the sum of Alice and Bob's subspaces is the entire vector space). These two problems were studied in [18, 7], with an optimal lower bound of $\Omega(n^2 \log p)$ on their deterministic communication complexity over a field with p elements. Sun and Wang [27] showed that the $\Omega(n^2 \log p)$ lower bound for subspace disjointness remains valid even for randomized and quantum communication. In follow-up work, Li, Sun, Wang, and Woodruff [16] proved an $\Omega(n^2 \log p)$ quantum lower bound for a promise version of subspace disjointness, where Alice and Bob's inputs are $n/2$-dimensional subspaces that either have trivial intersection or intersect in a one-dimensional subspace. The authors of [19] considered an asymmetric problem where Alice receives an n-bit vector, Bob receives a subspace, and their objective is to determine whether Alice's vector is contained in Bob's subspace. They showed that in any randomized one-way protocol that solves this problem, either Alice sends $\Omega(n)$ bits, or Bob sends $\Omega(n^2)$ bits.

In summary, all previous lower bounds for two-way communication complexity have focused on subspace disjointness or vector space span. The general problem, where Alice and Bob need to distinguish between the cases $\dim(S + T) = d_1$ and $\dim(S + T) = d_2$, is substantially harder and has remained unsolved. The difficulty is that previous results [27, 16] are based on a reduction from the matrix rank problem to subspace disjointness, and this straightforward strategy does not produce optimal results for the subspace sum problem with arbitrary parameters. In this paper, we approach the subspace sum problem from first principles and solve it completely. Our solution settles both the promise version of subspace sum and the corresponding total version. For clarity, we first state our result in the regime of constant error.

THEOREM 1.8. *Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements, and let n, m, ℓ, d, D be nonnegative integers with $\max\{m, \ell\} \leqslant d < D \leqslant \min\{m + \ell, n\}$. If $m = \ell = d$, then*

$$R_{1/3}(\mathrm{SUM}_d^{\mathbb{F},n,m,\ell}) = O(1).$$

If m, ℓ, d are not all equal, then

$$Q^*_{1/3}(\mathrm{SUM}_{d,D}^{\mathbb{F},n,m,\ell}) = \Theta((d - m + 1)(d - \ell + 1) \log q),$$
$$R_{1/3}(\mathrm{SUM}_d^{\mathbb{F},n,m,\ell}) = \Theta((d - m + 1)(d - \ell + 1) \log q).$$

Several remarks are in order. Recall that in $\mathbb{F}^n$, the sum of an m-dimensional subspace and an ℓ-dimensional subspace has dimension between $\max\{m, \ell\}$ and $\min\{m + \ell, n\}$. This justifies the above requirement that $d, D \in [\max\{m, \ell\}, \min\{m + \ell, n\}]$. Theorem 1.8 shows that the promise version of the subspace sum problem has the same communication complexity as the total version, up to a constant factor. Moreover, the theorem shows that this communication complexity is the same, up to a constant factor, for quantum and classical communication protocols. Both the lower and upper bounds in Theorem 1.8 require substantial effort. Lastly, the degenerate case $d = m = \ell$ of the subspace sum problem is easily seen to be equivalent to the equality problem, which explains the $O(1)$ bound in the theorem statement.

In addition to the constant-error regime of Theorem 1.8, we are able to determine the communication complexity of subspace sum for essentially all settings of the error parameter, as follows.

THEOREM 1.9. *Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements, and let n, m, ℓ, d, D be nonnegative integers with $\max\{m, \ell\} \leqslant d < D \leqslant \min\{m + \ell, n\}$. If $m = \ell = d$, then*

$$R_{1/3}(\mathrm{SUM}_d^{\mathbb{F},n,m,\ell}) = O(1).$$

If m, ℓ, d are not all equal, then for all $\gamma \in [\frac{1}{3} q^{-(2d-m-\ell)/5}, \frac{1}{3}]$,

$$Q^*_{\frac{1-\gamma}{2}}(\mathrm{SUM}_{d,D}^{\mathbb{F},n,m,\ell}) = \Theta((\log_q \lceil q^{d-m}\gamma \rceil + 1)(\log_q \lceil q^{d-\ell}\gamma \rceil + 1) \log q),$$
$$R_{\frac{1-\gamma}{2}}(\mathrm{SUM}_d^{\mathbb{F},n,m,\ell}) = \Theta((\log_q \lceil q^{d-m}\gamma \rceil + 1)(\log_q \lceil q^{d-\ell}\gamma \rceil + 1) \log q)$$

and moreover

$$R_{\frac{1}{2} - \frac{1}{16q^{2d-m-\ell+16}}}(\mathrm{SUM}_d^{\mathbb{F},n,m,\ell}) \leqslant 2. \tag{1.1}$$

Theorem 1.9 determines the communication complexity of subspace sum for every error probability in $[\frac{1}{3}, \frac{1}{2} - \Theta(|\mathbb{F}|^{-(2d-m-\ell)/5})]$. This is essentially the complete range of interest because by (1.1), the communication cost drops to 2 bits when the error probability is set to $\frac{1}{2} - |\mathbb{F}|^{-(2d-m-\ell)-\Theta(1)}$. Analogous to the constant-error regime, Theorem 1.9 shows that the communication complexity of subspace sum for any error in $[\frac{1}{3}, \frac{1}{2} - \Theta(|\mathbb{F}|^{-(2d-m-\ell)/5})]$ is the same, up to a constant factor, for both the partial and total versions of the problem, and for both quantum and classical communication. Theorems 1.8 and 1.9 reveal a rather subtle dependence of the communication complexity on the problem parameters d, m, ℓ, particularly as one additionally varies the error parameter. This explains why we were not able to obtain these theorems via a reduction from the matrix rank problem, as was done in previous work [27, 16] in the special case of subspace disjointness.

In view of the aforementioned identity $\dim(S+T) = \dim(S)+\dim(T)-\dim(S\cap T)$, our results for subspace sum can be equivalently stated in terms of subspace intersection. Formally, the *subspace intersection problem* requires Alice and Bob to distinguish subspace pairs (S, T) with $\dim(S \cap T) = d_1$ from those with $\dim(S \cap T) = d_2$, where S is an m-dimensional subspace given as input to Alice, T is an ℓ-dimensional subspace given to Bob, and d_1, d_2 are distinct integers fixed in advance. This

corresponds to the partial function

$$\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{d_1,d_2}(S,T) = \begin{cases} -1 & \text{if } \dim(S \cap T) = d_1, \\ 1 & \text{if } \dim(S \cap T) = d_2, \\ * & \text{otherwise.} \end{cases}$$

The total version of the subspace intersection problem is given by

$$\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{d}(S,T) = \begin{cases} -1 & \text{if } \dim(S \cap T) \geqslant d, \\ 1 & \text{otherwise,} \end{cases}$$

where d is a problem parameter fixed in advance. Theorem 1.9 fully settles the complexity of the subspace intersection problem, as follows.

THEOREM 1.10. *Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements, and let n, m, ℓ, r, R be nonnegative integers with $\max\{0, m+\ell-n\} \leqslant r < R \leqslant \min\{m, \ell\}$. If $m = \ell = R$, then*

$$R_{1/3}(\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{R}) = O(1).$$

If m, ℓ, R are not all equal, then for all $\gamma \in [\frac{1}{3}q^{-(m+\ell-2R)/5}, \frac{1}{3}]$,

$$Q^{*}_{\frac{1-\gamma}{2}}(\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{r,R}) = \Theta((\log_q \lceil q^{m-R}\gamma \rceil + 1)(\log_q \lceil q^{\ell-R}\gamma \rceil + 1)\log q),$$

$$R_{\frac{1-\gamma}{2}}(\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{R}) = \Theta((\log_q \lceil q^{m-R}\gamma \rceil + 1)(\log_q \lceil q^{\ell-R}\gamma \rceil + 1)\log q)$$

and moreover

$$R_{\frac{1}{2}-\frac{1}{16q^{m+\ell-2R+16}}}(\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{R}) \leqslant 2.$$

A moment's reflection (see Proposition 2.25) shows that in $\mathbb{F}^n$, the intersection of an m-dimensional subspace and an ℓ-dimensional subspace is a subspace of dimension between $\max\{0, m+\ell-n\}$ and $\min\{m, \ell\}$, hence the requirement that $r, R \in [\max\{0, m+\ell-n\}, \min\{m, \ell\}]$. Remarks analogous to those for subspace sum apply to Theorem 1.10 as well. Specifically, Theorem 1.10 determines the ε-error communication complexity of subspace intersection for all $\varepsilon \in [\frac{1}{3}, \frac{1}{2} - \Theta(|\mathbb{F}|^{-(m+\ell-2R)/5})]$, which is essentially the complete range of interest because the communication cost drops to 2 bits when the error probability is set to $\frac{1}{2} - |\mathbb{F}|^{-(m+\ell-2R)-\Theta(1)}$. Also, Theorem 1.10 shows that in this range of interest, the ε-error communication complexity of subspace intersection is the same (up to a constant factor) for both the partial and total versions of the problem, and for both quantum and classical communication.

1.5. Multiparty lower bounds. Via a blackbox reduction which we will now describe, our lower bounds for the matrix rank and determinant problems scale to multiparty communication. We adopt the standard multiparty model known as the *number-in-hand blackboard model*, which features t communicating players and a (possibly partial) function $F\colon X_1 \times X_2 \times \cdots \times X_t \to \{-1, 1, *\}$ with t arguments. An input $(x_1, x_2, \ldots, x_t)$ is partitioned among the t players by assigning x_i to the i-th player. The players communicate by writing on a shared blackboard. They also have access to an unbounded supply of shared random bits, which they can use in deciding what to do at any given point in the protocol. In the end, they must all agree on a bit (-1 or 1) that represents the output of the protocol. The *cost* of a communication protocol is the maximum number of bits written on the blackboard in the worst-case execution. The *ε-error randomized communication complexity* $R_\varepsilon(F)$ of a given function F is the least cost of a protocol that computes F with probability of error at most ε on every input. As usual, the standard setting of the error parameter is $\varepsilon = 1/3$, which can be replaced with any other constant in $(0, 1/2)$ at the expense of a constant-factor change in communication complexity. This model subsumes Yao's two-party randomized model as a special case, which justifies our continued use of the notation $R_\varepsilon(F)$. We note that there are alternative

number-in-hand models, where instead of a shared blackboard, the parties communicate via private channels (the *message-passing model*) or through an intermediary (the *coordinator model*). The blackboard model is more powerful than these alternative models, and lower bounds in it are more widely applicable.

Phillips, Verbin, and Zhang [20] developed a symmetrization technique that transforms two-party communication lower bounds for a class of problems into multiparty lower bounds. Our communication problems have a large symmetry group and are particularly well-suited for the methods of [20]. Using their technique, we prove the following.

PROPOSITION 1.11. *Let $(X, +)$ be a finite Abelian group, and let $f\colon X \to \{-1, 1, *\}$ be a given function. For $t \geqslant 2$, let $F_t\colon X^t \to \{-1, 1, *\}$ be the t-party communication problem given by $F_t(x_1, x_2, \ldots, x_t) = f(x_1 + x_2 + \cdots + x_t)$. Then for all $t \geqslant 2$,*

$$R_{1/6}(F_t) \geqslant \frac{1}{12} t R_{1/3}(F_2).$$

In other words, as one transitions from two parties to t parties, the communication complexity scales by a factor of $\Omega(t)$. This proposition, proved in Appendix B, simplifies and generalizes an earlier result due to Li, Sun, Wang, and Woodruff [16, Theorem 7]. The matrix rank problem, determinant problem, and rank versus determinant problem all admit multiparty generalizations that fit perfectly into the framework of Proposition 1.11, with the Abelian group in all cases being the group of matrices under addition. To begin with, the *t-party matrix rank problem* is given by $\mathrm{RANK}^{\mathbb{F},n,m,t}_{r,R}(M_1, M_2, \ldots, M_t) = \mathrm{rank}^{\mathbb{F},n,m}_{r,R}(\sum M_i)$, where the matrix function $\mathrm{rank}^{\mathbb{F},n,m}_{r,R}\colon \mathbb{F}^{n\times m} \to \{-1, 1, *\}$ outputs -1 on matrices of rank r, outputs 1 on matrices of rank R, and outputs $*$ in all other cases. Theorem 1.1 and Proposition 1.11 imply the following.

THEOREM 1.12. *For all finite fields $\mathbb{F}$, all integers n, m, R, r with $\min\{n, m\} \geqslant R > r \geqslant 0$, and all $t \geqslant 2$,*

$$R_{1/3}(\mathrm{RANK}^{\mathbb{F},n,m,t}_{r,R}) = \Omega(t + tr^2 \log |\mathbb{F}|).$$

Continuing, the *t-party determinant problem* is given by $\mathrm{DET}^{\mathbb{F},n,t}_{a,b}(M_1, M_2, \ldots, M_t) = \det^{\mathbb{F},n}_{a,b}(\sum M_i)$, where the matrix function $\det^{\mathbb{F},n}_{a,b}\colon \mathbb{F}^{n\times n} \to \{-1, 1, *\}$ outputs -1 on matrices with determinant a, outputs 1 on matrices with determinant b, and outputs $*$ in all other cases. Theorem 1.6 and Proposition 1.11 yield:

THEOREM 1.13. *For every finite field $\mathbb{F}$, every pair of distinct elements $a, b \in \mathbb{F}$, and all integers $n \geqslant 2$ and $t \geqslant 2$,*

$$R_{1/3}(\mathrm{DET}^{\mathbb{F},n,t}_{a,b}) = \Omega(tn^2 \log |\mathbb{F}|).$$

Finally, the *t-party rank versus determinant problem* is given by $\mathrm{RANKDET}^{\mathbb{F},n,t}_{r,a}(M_1, M_2, \ldots, M_t) = \mathrm{rankdet}^{\mathbb{F},n}_{r,a}(\sum M_i)$, where the matrix function $\mathrm{rankdet}^{\mathbb{F},n}_{r,a}\colon \mathbb{F}^{n\times n} \to \{-1, 1, *\}$ outputs -1 on matrices of rank r, outputs 1 on matrices with determinant a, and outputs $*$ in all other cases. The following multiparty result is immediate from Theorem 1.7 and Proposition 1.11.

THEOREM 1.14. *For every finite field $\mathbb{F}$, every field element $a \in \mathbb{F} \setminus \{0\}$, and all integers $n > r \geqslant 0$ and $t \geqslant 2$,*

$$R_{1/3}(\mathrm{RANKDET}^{\mathbb{F},n,t}_{r,a}) = \Omega(t + tr^2 \log |\mathbb{F}|).$$

Theorems 1.12 and 1.14 are tight for every $r \geqslant 1$ in a very strong sense: we give a t-party protocol with error $1/3$ and communication cost $O(t(r^2 + 1) \log |\mathbb{F}|)$ for checking whether the sum

of the players' matrices has rank at most r (see Corollary 3.17 in Section 3.7). Theorem 1.13 is tight because the stated lower bound matches the trivial, deterministic protocol where each party announces their input. Since the blackboard model is more powerful than the message-passing and coordinator models, Theorems 1.12–1.14 are valid in those alternative models as well.

1.6. Bilinear query complexity. Our communication lower bounds additionally imply new results in query complexity. We adopt the *bilinear query model* due to Rashtchian, Woodruff, and Zhu [21], which subsumes a large number of other query models and is particularly well-suited for linear-algebraic problems. Formally, let $f\colon \mathbb{F}^{n\times m} \to \{-1, 1, *\}$ be a (possibly partial) Boolean function on matrices over a field $\mathbb{F}$. In the bilinear query model, the query algorithm accesses the input $X \in \mathbb{F}^{n\times m}$ in an adaptive manner with *bilinear queries*. Each such query reveals the value $u^{\mathsf{T}}Xv \in \mathbb{F}$ for a pair of vectors $u \in \mathbb{F}^n$, $v \in \mathbb{F}^m$ of the algorithm's choosing. As usual, a randomized query algorithm is a probability distribution on deterministic query algorithms. The *cost* of a query algorithm is the maximum number of queries in the worst-case execution. The *ε-error bilinear query complexity of f*, which we denote by $\mathrm{BLQ}_\varepsilon(f)$, is the minimum cost of a bilinear query algorithm that computes f with probability of error at most ε on every input. As always, the algorithm may exhibit arbitrary behavior on inputs X with $f(X) = *$.

Recall the matrix functions $\mathrm{rank}_{r,R}^{\mathbb{F},n,m}, \det_{a,b}^{\mathbb{F},n}, \mathrm{rankdet}_{r,a}^{\mathbb{F},n}$ that correspond to the matrix rank problem, determinant problem, and rank versus determinant problem and were formally defined in Section 1.5. Our next result settles their bilinear query complexity for all settings of the parameters n, m, r, R, a, b.

THEOREM 1.15. *Let $\mathbb{F}$ be a finite field. Then:*

(i) *for all integers n, m, R, r with $\min\{n, m\} \geqslant R > r \geqslant 0$,*
$$\mathrm{BLQ}_{\frac{1}{2}-\frac{1}{4|\mathbb{F}|^{r/3}}}(\mathrm{rank}_{r,R}^{\mathbb{F},n,m}) = \Omega(r^2 + 1);$$

(ii) *for every pair of distinct elements $a, b \in \mathbb{F}$ and all integers $n \geqslant 1$,*
$$\mathrm{BLQ}_{\frac{1}{2}-\frac{1}{4|\mathbb{F}|^{(n-1)/3}}}(\det_{a,b}^{\mathbb{F},n}) = \Omega(n^2);$$

(iii) *for every field element $a \in \mathbb{F} \setminus \{0\}$ and all integers $n > r \geqslant 0$,*
$$\mathrm{BLQ}_{\frac{1}{2}-\frac{1}{4|\mathbb{F}|^{r/3}}}(\mathrm{rankdet}_{r,a}^{\mathbb{F},n}) = \Omega(r^2 + 1).$$

Proof. For a matrix function $f\colon \mathbb{F}^{n\times m} \to \{-1, 1, *\}$, consider the associated communication problem $F\colon \mathbb{F}^{n\times m} \times \mathbb{F}^{n\times m} \to \{-1, 1, *\}$ given by $F(A, B) = f(A + B)$. As observed by the authors of [21], a cost-c randomized algorithm for f in the bilinear query model gives a randomized communication protocol for F of cost $2\lceil \log |\mathbb{F}| \rceil c$. Specifically, on input A for Alice and B for Bob, they simulate the query algorithm on $A + B$. Computing a query $u^{\mathsf{T}}(A + B)v$ for given vectors u, v amounts to exchanging the field elements $u^{\mathsf{T}}Av$ and $u^{\mathsf{T}}Bv$. In summary,
$$R_\varepsilon(F) \leqslant 2\lceil \log |\mathbb{F}| \rceil \, \mathrm{BLQ}_\varepsilon(f).$$
Now the claimed query lower bounds in (i)–(iii)are immediate from our corresponding communication complexity results (Theorems 1.1, 1.6, and 1.7) as well as the trivial query lower bound of 1 for any nonconstant function. □

Every lower bound in Theorem 1.15 is tight, even for computation with error probability 1/3. To prove the tightness of Theorem 1.15(i) and 1.15(iii), we give a query algorithm with error probability 1/3 and cost $O(r^2+1)$ for checking whether the input matrix has rank at most r (see Theorem 3.18 in Section 3.7). Finally, the lower bound in Theorem 1.15(ii) matches the trivial, deterministic upper bound of n^2 queries.

The strongest result prior to our work was an $\Omega(n^2)$ query lower bound due to Rashtchian, Woodruff, and Zhu [21] for distinguishing, with probability $2/3$, matrices of rank $n-1$ from those of rank n. Theorem 1.15(i) shows that the $\Omega(n^2)$ query lower bound remains valid even for distinguishing matrices of rank cn (for any constant $c > 0$) from those of rank n, and even for correctness probability exponentially close to $1/2$. In particular, Theorem 1.15(i) shows that $\Omega(n^2)$ bilinear queries are needed to approximate the rank of a matrix to any constant factor.

1.7. Previous approaches. A powerful tool for proving lower bounds on randomized and quantum communication complexity is the *approximate trace norm* [30, 13, 22, 17, 24]. In more detail, let $F\colon X \times Y \to \{-1,1\}$ be a given communication problem, and let $M = [F(x,y)]_{x,y}$ be its characteristic matrix. The *δ-approximate trace norm of M*, denoted $\|M\|_{\Sigma,\delta}$, is the minimum trace norm of a real matrix $\widetilde{M}$ that approximates M entrywise within δ. The approximate trace norm bound states that

$$Q^*_\varepsilon(F) \geqslant \frac{1}{2}\log\left(\frac{\|M\|_{\Sigma,2\varepsilon}}{3\sqrt{|X||Y|}}\right) \tag{1.2}$$

for all $\varepsilon \geqslant 0$, making it possible to prove communication lower bounds by analyzing the approximate trace norm of M. To bound the approximate trace norm from below, it is useful to appeal to its dual formulation as a maximization problem, whereby

$$\|M\|_{\Sigma,2\varepsilon} \geqslant \frac{\langle M, \Phi\rangle - 2\varepsilon\|\Phi\|_1}{\|\Phi\|} \tag{1.3}$$

for every nonzero real matrix Φ. As a result, proving a communication lower bound reduces to constructing a matrix Φ whose spectral norm and ℓ_1 norm are small relative to the inner product of Φ with the communication matrix M. The matrix Φ is often referred to as a *dual matrix* or a *witness.* The lower bound (1.2) remains valid for partial functions $F\colon X \times Y \to \{-1,1,*\}$ and their characteristic matrices M, in which case the dual characterization of the approximate trace norm is given by

$$\|M\|_{\Sigma,2\varepsilon} \geqslant \frac{1}{\|\Phi\|}\left(\sum_{\operatorname{dom} F} M_{x,y}\Phi_{x,y} - 2\varepsilon\|\Phi\|_1 - \sum_{\overline{\operatorname{dom} F}} |\Phi_{x,y}|\right) \tag{1.4}$$

for all $\Phi \neq 0$. In this equation, $\operatorname{dom} F = \{(x,y) : F(x,y) \neq *\}$ denotes the domain of the partial function F. Comparing this dual characterization with the original one (1.3) for total functions, we notice that the inner product is now restricted to the domain of F, and there is an additional penalty term for any weight placed by Φ outside the domain of F. For more background on the use of duality in proving communication lower bounds, we refer the reader to the surveys [23, 15].

Main idea in [27], [16]. Constructing a good witness Φ can be very challenging. Sun and Wang [27] studied the *nonsingularity problem* over fields $\mathbb{F}_p$ of prime order p, where Alice and Bob's inputs are matrices $A, B \in \mathbb{F}_p^{n\times n}$, respectively, and they are required to output 1 if $A+B$ is nonsingular and -1 otherwise. Let M be the characteristic matrix of this communication problem. To analyze the approximate trace norm of M, the authors of [27] use the witness $\Phi = [(-1)^n\widehat{g}(A+B)]_{A,B}$, where $\widehat{g}$ is the Fourier transform of the function $g\colon \mathbb{F}_p^{n\times n} \to \{0,1\}$ given by $g(X) = 1$ if and only if X is nonsingular. The calculations in [27] reveal the following, where $C \geqslant 6$ is an absolute constant:

(i) $\|\Phi\| = 1$;
(ii) $\langle M, \Phi\rangle = 2p^{n^2-n}\prod_{i=1}^n (p^i - 1)$;
(iii) $\|\Phi\|_1 \leqslant Cp^{n^2-n}\prod_{i=1}^n (p^i - 1)$.

Using this witness Φ in (1.3) with a sufficiently small error parameter ε, Sun and Wang obtain $\|M\|_{\Sigma,2\varepsilon} = \Omega(p^{n^2}p^{n(n-1)/2})$, which in view of (1.2) gives an $\Omega(n^2\log p)$ lower bound on the bounded-error communication complexity of the nonsingularity problem.

In follow-up work, Li, Sun, Wang, and Woodruff [16] studied the partial communication problem $F = \mathrm{RANK}_{n-1,n}^{\mathbb{F}_p,n,n}$. Let M' denote its characteristic matrix. The authors of [16] used the same witness Φ as Sun and Wang [27] and proved the following:

(i) $\|\Phi\| = 1$;
(ii) $\sum_{\mathrm{dom}\, F} M'_{A,B}\Phi_{A,B} = p^{n^2-n}(1 + \frac{p-p^{-n+1}}{p-1}) \prod_{i=1}^{n}(p^i - 1)$;
(iii) $\|\Phi\|_1 = p^{n^2-n} \prod_{i=0}^{n-1}(1 + p^{-i}) \cdot \prod_{i=1}^{n}(p^i - 1)$;
(iv) $\sum_{\overline{\mathrm{dom}\, F}} |\Phi_{A,B}| = \|\Phi\|_1 - \sum_{\mathrm{dom}\, F} M'_{A,B}\Phi_{A,B}$.

Making these substitutions in (1.4) and setting ε to a sufficiently small constant, the authors of [16] obtain $\|M'\|_{\Sigma,2\varepsilon} = \Omega(p^{n^2} p^{n(n-1)/2})$, which along with (1.2) results in an $\Omega(n^2 \log p)$ lower bound on the quantum communication complexity of $F = \mathrm{RANK}_{n-1,n}^{\mathbb{F}_p,n,n}$. We note that we have described the work of [27, 16] in the framework that we adopt in our paper, which differs somewhat from the original presentation in [27, 16]. These differences do not affect any of the ideas or bounds in question.

Unfortunately, the above analyses rely heavily on ε being set to a small constant. This is because $\|\Phi\|_1$ is too large compared to the inner product $\langle M, \Phi \rangle$ and the correlation $\sum_{\mathrm{dom}\, F} M'_{A,B}\Phi_{A,B}$, which makes setting ε close to $1/2$ impossible. Since the authors of [16] determined $\|\Phi\|_1$ and $\sum_{\mathrm{dom}\, F} M'_{A,B}\Phi_{A,B}$ exactly, with equality, there is no room for improved analysis and no possibility of setting ε close to $1/2$ with this choice of witness Φ. This rules out the use of Φ for proving Theorem 1.1 even in the special case of $\mathrm{RANK}_{n-1,n}^{\mathbb{F},n,n}$.

When it comes to the general problem $\mathrm{RANK}_{r,n}^{\mathbb{F},n,n}$, the witness Φ produces no meaningful results at all for any $r \leqslant n - 3$, regardless of the error parameter ε. The issue is that the ℓ_1 norm of Φ is concentrated on matrix pairs (A, B) for which $A + B$ has rank n or $n - 1$, whereas the domain of $\mathrm{RANK}_{r,n}^{\mathbb{F},n,n}$ consists of matrix pairs whose sum has rank n or r. Quantitatively, the domain of $\mathrm{RANK}_{r,n}^{\mathbb{F},n,n}$ supports less than half of the ℓ_1 norm of Φ, which causes the lower bound in (1.4) to be negative for every ε. Our attempts at simple modifications to Φ were not successful.

1.8. Our approach. Our techniques depart substantially from the previous work in [27, 16]. Instead of attempting to guess a good witness Φ and analyzing its metric and analytic properties, we determine how exactly those properties depend on the choice of a witness. In this way, we are able to construct essentially optimal witnesses for the matrix rank, determinant, subspace sum, and subspace intersection problems. We first discuss the matrix rank problem, over an arbitrary finite field $\mathbb{F}$. In this overview, we focus on the canonical case $F = \mathrm{RANK}_{k,n}^{\mathbb{F},n,n}$, where Alice and Bob receive square matrices $A, B \in \mathbb{F}^{n\times n}$, respectively, and need to decide whether $\mathrm{rk}(A + B) = k$ or $\mathrm{rk}(A + B) = n$. This special case captures the matrix rank problem in its full generality via straightforward reductions.

Reducing the degrees of freedom. We will call a witness Φ *symmetric* if each entry $\Phi_{A,B}$ is fully determined by the rank of $A + B$. In searching for a good witness for the matrix rank problem, we will only consider symmetric witnesses Φ. This restriction is without loss of generality: since $F(A, B)$ depends only on the rank of $A + B$, it is not hard to verify that any witness for F can be "symmetrized" without harming the corresponding value of the approximate trace norm bound, (1.4). The resulting witness matrix Φ has only $n + 1$ degrees of freedom, corresponding to every possible value of the rank of $A + B$.

Let $i \in \{0, 1, \ldots, n\}$ be given. Consider the matrix whose rows and columns are indexed by elements of $\mathbb{F}^{n\times n}$, and whose (A, B) entry is defined to be 1 if $\mathrm{rk}(A + B) = i$ and zero otherwise. Normalize this matrix to have ℓ_1 norm 1, and call the resulting matrix E_i. Then any symmetric witness matrix is a linear combination of $E_0, E_1, \ldots, E_n$. With this in mind, for any real function

$\varphi\colon \{0,1,\dots,n\} \to \mathbb{R}$, we define

$$E_\varphi = \varphi(0)E_0 + \varphi(1)E_1 + \cdots + \varphi(n)E_n.$$

Taking $\Phi = E_\varphi$ in the approximate trace norm bound (1.4) and simplifying, we arrive at the following bound for the characteristic matrix M of F:

$$\|M\|_{\Sigma,2\varepsilon} \geqslant \frac{1}{\|E_\varphi\|} \left(\varphi(n) - \varphi(k) - 2\varepsilon\|\varphi\|_1 - \sum_{i \notin \{k,n\}} |\varphi(i)| \right). \tag{1.5}$$

Our challenge now is to understand how φ affects the spectral norm of E_φ. For matrices with a large symmetry group, it is reasonable to expect algebraic structure in the spectrum. For example, the so-called *combinatorial matrices,* studied by Knuth [12] and used for communication lower bounds by Razborov [22], have all eigenvalues described in terms of Hahn polynomials. We will similarly see that the spectrum of each E_φ has strong algebraic structure and is described in terms of what we call *hyperpolynomials*.

By analyzing the singular values of E_φ, we prove that

$$\|E_\varphi\| = q^{-n^2} \max_{s=0,1,\dots,n} \left| \sum_{t=0}^{n} \varphi(t)\Gamma_n(s,t) \right|, \tag{1.6}$$

where q is the order of the finite field $\mathbb{F}$, and Γ_n is an auxiliary function. In more detail, we define

$$\Gamma_n(s,t) = \mathop{\mathbf{E}}_{\substack{\operatorname{rk} A = s \\ \operatorname{rk} B = t}} \omega^{\langle A,B \rangle},$$

where ω is a primitive root of unity of order equal to the characteristic of $\mathbb{F}$, with the operation $x \mapsto \omega^x$ for field elements $x \in \mathbb{F}$ deferred to Section 2.4. An exact expression for $\Gamma_n(n,t)$ can be obtained from the analysis of the Fourier spectrum of the nonsingularity function in [27]. Understanding $\Gamma_n(s,t)$ for general s,t, however, is rather nontrivial. To this end, we derive the representation

$$\Gamma_n(s,t) = \sum_{r=0}^{n} P_n(s,t,r)\Gamma_n(n,r),$$

where $P_n(s,t,r)$ is the probability that the upper-left $s \times t$ quadrant of a uniformly random nonsingular matrix of order n has rank r. By explicitly calculating the probabilities $P_n(s,t,r)$ and combining them with the closed-form expression for $\Gamma_n(n,r)$, we obtain the upper bound $|\Gamma_n(s,t)| \leqslant cq^{-st/2}$ for an absolute constant c. In addition to this *analytic* property, we establish the following *algebraic* result: for n,s fixed, $\Gamma_n(s,t)$ as a function of $t \in \{0,1,\dots,n\}$ is a polynomial in q^{-t} of degree at most s. These two properties play a central role in our analysis. In what follows, we will refer to a polynomial in q^{-t} as a *hyperpolynomial in* t.

Univariate object for the rank problem. Since (1.5) is invariant under multiplication of φ by a positive factor, we will normalize φ such that $\varphi(n) = 1$. To achieve a large value on the right-hand side of (1.5), we will construct a function φ that is negative at k, has ℓ_1 norm concentrated on $\{k,n\}$, and results in E_φ having a small spectral norm. In view of (1.6), the spectral norm requirement amounts to a bound on $\max_s |\sum_{t=0}^{n} \varphi(t)\Gamma_n(s,t)|$. Quantitatively speaking, to obtain an asymptotically optimal lower bound for the matrix rank problem, we need φ to satisfy the following constraints:

(i) $\varphi(n) = 1$;
(ii) $\varphi(k) < 0$;
(iii) $\sum_{i \notin \{k,n\}} |\varphi(i)| = q^{-\Omega(k)}$;
(iv) $|\sum_{t=0}^{n} \varphi(t)\Gamma_n(s,t)| = q^{-\Omega(k^2)}$ for every $s \in \{0,1,\dots,n\}$.

The last requirement states that φ needs to be almost orthogonal to each $\Gamma_n(s,t)$, viewed as a function of t with fixed s. Recall from our earlier discussion that for s and n fixed, $\Gamma_n(s,t)$ is a hyperpolynomial of low degree, namely, a polynomial in q^{-t} of degree at most s. To achieve orthogonality to hyperpolynomials of low degree, we leverage the *Cauchy binomial theorem* [26, eqn. (1.87)], which implies that

$$\sum_{t=0}^{n} \binom{n}{t}_q (-1)^t q^{\binom{t}{2}} g(q^{-t}) = 0 \tag{1.7}$$

for every polynomial g of degree less than n. In particular, defining $\varphi(t) = \binom{n}{t}_q (-1)^t q^{\binom{t}{2}}$ for $t = 0, 1, \ldots, n$ ensures that φ is exactly orthogonal to each hyperpolynomial $\Gamma_n(s,t)$ for $s < n$. Unfortunately, this choice of φ does not satisfy our constraint on the distribution of the ℓ_1 norm because most of it would be concentrated on the values $\varphi(t)$ at points $t \approx n$. To overcome this difficulty, we apply a hyperpolynomial of low degree to achieve the desired distribution of the ℓ_1 norm. Specifically, we set

$$\varphi(t) = \binom{n}{t}_q (-1)^{t-n} q^{\binom{t}{2} - \binom{n}{2}} \zeta(q^{-t})$$

for a carefully constructed polynomial ζ; the factor $(-1)^{-n} q^{-\binom{n}{2}}$ in this formula serves to normalize φ and ensure the proper signs. As we increase the degree of ζ, we improve the distribution of the ℓ_1 norm of φ at the expense of a weaker orthogonality guarantee, for now φ is orthogonal only to hyperpolynomials of degree less than $n - \deg \zeta$. With an appropriate choice of ζ, we are able to ensure all four desiderata (i)–(iv) for the univariate function φ. The most technical part of the analysis is the upper bound in (iv). For s small, our construction guarantees (iv) as a consequence of the Cauchy binomial theorem, with $\sum_{t=0}^{n} \varphi(t) \Gamma_n(s,t) = 0$. For s large, we use the pointwise bounds for φ and Γ_n and show that $\sum_{t=0}^{n} |\varphi(t)| \, |\Gamma_n(s,t)| = q^{-\Omega(k^2)}$.

By combining equations (1.5) and (1.6) with the properties (i)–(iv) of the univariate function φ, we derive the following bound on the approximate trace norm: $\|M\|_{\Sigma, 2\varepsilon} \geqslant (1 - 2\varepsilon - q^{-\Omega(k)}) q^{n^2} q^{\Omega(k^2)}$. Applying the approximate trace norm method (1.2), we obtain the sought lower bound of $\Omega(k^2 \log q)$ on the quantum communication complexity of F for error $\varepsilon = \frac{1}{2} - q^{-\Theta(k)}$. To achieve the error probability as stated in Theorem 1.1, we derive bounds for φ with explicit constants, which we did not discuss in this proof sketch.

The determinant problem. To solve the determinant problem $\mathrm{DET}_{a,b}^{\mathbb{F},n}$ for all field elements a, b, we combine our approach to the matrix rank problem presented above with additional Fourier-theoretic ideas. Recall that we tackle the determinant problem from first principles, without relying on the partial solution for nonzero a, b due to Sun and Wang [27]. With this in mind, we will first discuss the case of nonzero a, b. Consider the function $g_{a,b} \colon \mathbb{F}^{n \times n} \to \{-1, 1, 0\}$ given by

$$g_{a,b}(X) = \begin{cases} -1 & \text{if } \det X = a, \\ 1 & \text{if } \det X = b, \\ 0 & \text{otherwise.} \end{cases}$$

A simple argument reveals that the Fourier coefficients of $g_{a,b}$ corresponding to singular matrices are zero, whereas those corresponding to nonsingular matrices M depend only on $\det(M)$. By applying Parseval's identity, we obtain a strong upper bound on the absolute value of every Fourier coefficient of $g_{a,b}$:

$$\|\widehat{g_{a,b}}\|_\infty \leqslant \frac{1}{\sqrt{|\mathrm{SL}(\mathbb{F}, n)|}},$$

where $\mathrm{SL}(\mathbb{F}, n)$ denotes the special linear group of order-n matrices over $\mathbb{F}$. Consider now the matrix $\Phi_{a,b}$ whose rows and columns are indexed by elements of $\mathbb{F}^{n\times n}$ and whose entries are given by $\Phi_{a,b}(A, B) = g_{a,b}(A + B)$. The spectral norm of $\Phi_{a,b}$ is governed by the Fourier coefficients of $g_{a,b}$, with

$$\|\Phi_{a,b}\| = q^{n^2}\|\widehat{g_{a,b}}\|_\infty \leqslant \frac{q^{n^2}}{\sqrt{|\mathrm{SL}(\mathbb{F}, n)|}}.$$

Observe that $\Phi_{a,b}$ is precisely the characteristic matrix of $\mathrm{DET}^{\mathbb{F},n}_{a,b}$ with the $*$ entries replaced with zeroes. Using $\Phi_{a,b}$ as a witness in the approximate trace norm method, we immediately obtain Theorem 1.6 for nonzero a, b.

Consider now the complementary case when one of a, b is zero, say, $a \neq 0$ and $b = 0$. Here, we study the rank versus determinant problem $\mathrm{RANKDET}^{\mathbb{F},n}_{k,a}$, which in this case is a subproblem of the determinant problem. Its parameters are an integer $k \in \{0, 1, \ldots, n-1\}$ and a nonzero field element $a \in \mathbb{F}$. Recall that in this problem, Alice and Bob are given matrices $A, B \in \mathbb{F}^{n\times n}$, respectively, and are called upon to distinguish between the cases $\mathrm{rk}(A + B) = k$ and $\det(A + B) = a$. To construct a witness for $\mathrm{RANKDET}^{\mathbb{F},n}_{k,a}$, we combine our solutions to the matrix rank problem and the determinant problem for nonzero field elements. In more detail, consider the witness Φ for the problem $\mathrm{RANK}^{\mathbb{F},n,n}_{k,n}$ that we sketched above. Recall that $\Phi_{A,B}$ depends only on the rank of $A + B$, and moreover the ℓ_1 norm of Φ is concentrated on matrix pairs (A, B) with $\mathrm{rk}(A + B) \in \{k, n\}$. To turn Φ into a witness for $\mathrm{RANKDET}^{\mathbb{F},n}_{k,a}$, we form a *linear combination* of Φ with the matrices $\Phi_{a,b}$ for all $b \in \mathbb{F} \setminus \{0, a\}$, constructed in the previous paragraph for the determinant problem with nonzero field elements. The coefficients in this linear combination are chosen so as to transfer the ℓ_1 weight placed by Φ on matrix pairs with $\det(A+B) \notin \{0, a\}$ to the matrix pairs with $\det(A+B) = a$, without affecting any other entries of Φ. The resulting dual witness has low spectral norm (being the sum of matrices with low spectral norm) and has its ℓ_1 norm concentrated on matrix pairs (A, B) for which $A + B$ has rank k or determinant a, ensuring strong correlation with the partial function $\mathrm{RANKDET}^{\mathbb{F},n}_{k,a}$. By applying the approximate trace norm method, we obtain the claimed communication lower bounds for $\mathrm{RANKDET}^{\mathbb{F},n}_{k,a}$.

Subspace sum and intersection. We now present the main ideas in our solution to the subspace sum and subspace intersection problems. Since these problems are equivalent, we will discuss the intersection problem alone. As before, we work with an arbitrary finite field $\mathbb{F}$, whose order we denote by q. Also by way of notation, recall that m and ℓ stand for the dimensions of Alice's subspace S and Bob's subspace T, respectively. For simplicity, we will assume in this overview that the dimension n of the ambient vector space satisfies $n \geqslant m+\ell$, which ensures that $\dim(S\cap T)$ takes on every possible value in $\{0, 1, 2, \ldots, \min\{m, \ell\}\}$ as one varies the subspaces S, T. We will focus on the canonical case of the subspace intersection problem where Alice and Bob need to distinguish subspace pairs with $\dim(S \cap T) = 0$ from those with $\dim(S \cap T) = R$, for an integer R with $0 < R \leqslant \min\{m, \ell\}$. In what follows, we let $F = \mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{0,R}$ stand for this communication problem of interest. The general case of the subspace intersection problem, which we will not discuss in this overview, reduces to this canonical case.

As before, the challenge is to construct a dual matrix Φ that witnesses a strong lower bound on the approximate trace norm of the characteristic matrix M of F. Note that the rows of Φ are indexed by m-dimensional subspaces, and the columns are indexed by ℓ-dimensional subspaces. Analogous to the matrix rank problem, we start with the methodological observation that the symmetry of F greatly reduces the number of degrees of freedom in Φ. Specifically, $F(S, T)$ by definition depends only on $\dim(S \cap T)$. A moment's thought now shows that any dual matrix Φ for the subspace intersection problem can be "symmetrized" such that its (S, T) entry depends only on $\dim(S \cap T)$,

and this symmetrization can only improve the resulting lower bound on the approximate trace norm in (1.4).

For $r = 0, 1, \ldots, \min\{m, \ell\}$, let $J_r^{n,m,\ell}$ stand for the matrix whose rows are indexed by m-dimensional subspaces of $\mathbb{F}^n$, whose columns are indexed by ℓ-dimensional subspaces of $\mathbb{F}^n$, and whose (S, T) entry is 1 if $\dim(S \cap T) = r$ and zero otherwise. Put another way, $J_r^{n,m,\ell}$ is the characteristic matrix of subspace pairs whose intersection has dimension r. For an arbitrary function $\psi\colon \{0, 1, \ldots, \min\{m, \ell\}\} \to \mathbb{R}$, we define

$$J_\psi^{n,m,\ell} = \sum_{r=0}^{\min\{m,\ell\}} \psi(r) J_r^{n,m,\ell}.$$

We refer to this family of matrices, whose (S, T) entry depends only on $\dim(S \cap T)$, as *subspace matrices.* It will also be helpful to have notation for normalized versions of these matrices, as follows:

$$\overline{J}_r^{n,m,\ell} = \frac{1}{\|J_r^{n,m,\ell}\|_1} J_r^{n,m,\ell}, \qquad \overline{J}_\psi^{n,m,\ell} = \sum_{r=0}^{\min\{m,\ell\}} \frac{\psi(r)}{\|J_r^{n,m,\ell}\|_1} J_r^{n,m,\ell}.$$

In this notation, we are looking to construct a dual witness of the form $\Phi = \overline{J}_\psi^{n,m,\ell}$ for some function ψ. This matrix has $\min\{m, \ell\} + 1$ degrees of freedom, corresponding to every possible value that $\dim(S \cap T)$ can take. Setting $\Phi = \overline{J}_\psi^{n,m,\ell}$ in the approximate trace norm bound (1.4) and simplifying, one obtains the following bound for the characteristic matrix M of F:

$$\|M\|_{\Sigma,2\varepsilon} \geqslant \frac{1}{\|\overline{J}_\psi^{n,m,\ell}\|} \left(-\psi(0) + \psi(R) - 2\varepsilon\|\psi\|_1 - \sum_{i \notin \{0,R\}} |\psi(i)| \right). \tag{1.8}$$

At first glance, this equation looks similar to the corresponding equation (1.5) for the matrix rank problem. However, there is a major difference: the spectral norm of E_φ is now replaced with the spectral norm of $\overline{J}_\psi^{n,m,\ell}$, and there is no reason to expect that these quantities depend on their corresponding univariate objects φ and ψ in a similar way. Indeed, our spectral analysis of $\overline{J}_\psi^{n,m,\ell}$ is quite different and significantly more technical than that of E_φ.

Analyzing the spectrum of subspace matrices. Symmetric subspace matrices $J_\psi^{n,m,m}$ are classical objects whose eigenvectors and eigenvalues have been studied in numerous works, e.g., [10, 11, 3, 8]. However, these previous analyses do not seem to apply to the general, asymmetric case of interest to us, namely, that of subspace matrices $J_\psi^{n,m,\ell}$ for arbitrary m, ℓ. One way to reduce the analysis of the spectral norm of $J_\psi^{n,m,\ell}$ to the symmetric case is to express the product $J_\psi^{n,m,\ell}(J_\psi^{n,m,\ell})^{\mathsf{T}} = J_\psi^{n,m,\ell} J_\psi^{n,\ell,m}$ as the sum of symmetric subspace matrices and then apply known results for the symmetric case. Unfortunately, multiplying these subspace matrices leads to expressions so unwieldy and complicated that this is clearly not the method of choice.

Instead, our analysis is inspired by a result of Knuth [12] on what he called *combinatorial matrices*, which we briefly mentioned above. Specifically, Knuth investigated the eigenvalues of symmetric matrices of order $\binom{n}{t}$ whose rows and columns are indexed by t-element subsets of $\{1, 2, \ldots, n\}$ and whose (A, B) entry depends only on $|A \cap B|$. To determine the eigenvectors of a combinatorial matrix, Knuth studied certain homogeneous linear systems with variables indexed by subsets of a fixed cardinality s, and the equations themselves corresponding to sets of cardinality $s - 1$. He showed that any solution to such a system for $s \in \{1, 2, \ldots, t\}$ is an eigenvector for every combinatorial matrix of order $\binom{n}{t}$. Knuth also proved that for any given s, the space of solutions has a basis supported on the variables indexed by what he called *basic sets.* These sets have a simple combinatorial description, which the author of [12] used to prove that the eigenvectors arising from the homogeneous systems for $s = 1, 2, \ldots, t$, together with the all-ones vector, form an exhaustive

description of the eigenvectors of each combinatorial matrix. Once the eigenvectors are determined, one readily calculates their associated eigenvalues and in particular the spectral norm.

With some effort, we are able to adapt Knuth's ideas to the context of subspaces. Along the way, we encounter several obstacles. To begin with, counting problems that are straightforward for sets become challenging for subspaces, and some intuitive combinatorial principles no longer work. For example, the inclusion-exclusion formula $\dim(S+T) = \dim(S) + \dim(T) - \dim(S \cap T)$ has no analogue for three or more subspaces. Another obstacle is that Knuth's notion of a basic set does not seem to have a meaningful analogue for subspaces. For this reason, we reformulate Knuth's ideas in a purely linear-algebraic way and sidestep much of the combinatorial machinery in [12]. The final hurdle is extending Knuth's analysis to the asymmetric case. Ultimately, we are able to determine the singular values and spectral norm of every subspace matrix $J_\psi^{n,m,\ell}$ and in particular its normalized version $\overline{J}_\psi^{n,m,\ell}$. We prove that

$$\|\overline{J}_\psi^{n,m,\ell}\| = \max_{s=0,1,\ldots,\min\{m,\ell\}} \left| \sum_{r=0}^{\min\{m,\ell\}} \psi(r) \overline{\Lambda}_r^{n,m,\ell}(s) \right|^{1/2} \left| \sum_{r=0}^{\min\{m,\ell\}} \psi(r) \overline{\Lambda}_r^{n,\ell,m}(s) \right|^{1/2}, \tag{1.9}$$

where $\overline{\Lambda}_r^{n,m,\ell}$ and $\overline{\Lambda}_r^{n,\ell,m}$ are functions with algebraic and analytic properties analogous to those of the Γ_n function in our solution to the matrix rank problem. Specifically, we have:

(i) for n, m, ℓ, s fixed, $\overline{\Lambda}_r^{n,m,\ell}(s)$ as a function of $r \in \{0, 1, \ldots, \min\{m,\ell\}\}$ is a polynomial in q^r of degree at most s;

(ii) $|\overline{\Lambda}_r^{n,m,\ell}(s)| \leqslant 8\binom{n}{m}_q^{-1} q^{-s(m-r)/2}$ for $r = 0, 1, \ldots, \min\{m,\ell\}$.

By swapping the roles of m and ℓ, one obtains analogous properties for $\overline{\Lambda}_r^{n,\ell,m}(s)$.

This spectral result gives us fine-grained control over the spectrum of $J_\psi^{n,m,\ell}$ via the univariate function ψ. Our construction of ψ is based on the Cauchy binomial theorem and is conceptually similar to our univariate function φ in the matrix rank problem. In particular, we use the algebraic property (i) to bound the product in (1.9) for small s, and the analytic property (ii) to bound it for large s. We further ensure that the ℓ_1 norm of ψ is highly concentrated on $\{0, R\}$, with $\psi(0) < 0$ and $\psi(R) > 0$. This results in a strong lower bound in (1.8), which in turn leads to an optimal lower bound on the communication complexity of F by virtue of the approximate trace norm method.

2. Preliminaries

2.1. General notation. We view Boolean functions as mappings $X \to \{-1, 1\}$, where X is a nonempty finite set and the range elements $-1, 1$ correspond to "true" and "false," respectively. A *partial* Boolean function is a mapping $f\colon X \to \{-1, 1, *\}$, whose *domain* is defined as $\operatorname{dom} f = \{x \in X : f(x) \neq *\}$. Recall that for an arbitrary function $f\colon X \to Y$, the restriction of f to a subset $X' \subseteq X$ is defined to be the mapping $f|_{X'}\colon X' \to Y$ given by $(f|_{X'})(x) = f(x)$.

We adopt the shorthand $[n] = \{1, 2, \ldots, n\}$. We use the letters p and q throughout this manuscript to refer to a prime number and a prime power, respectively. As usual, $\mathbb{F}_q$ stands for the Galois field $\mathrm{GF}(q)$, the q-element field which is unique up to isomorphism. For a given set X, the *Kronecker delta* $\delta_{x,y}$ is defined for $x, y \in X$ by

$$\delta_{x,y} = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{otherwise.} \end{cases}$$

For a function $f\colon X \to \mathbb{C}$, we use the familiar norms $\|f\|_1 = \sum_{x \in X} |f(x)|$ and $\|f\|_\infty = \max_{x \in X} |f(x)|$. Similarly, for a real or complex matrix M, one defines $\|M\|_1 = \sum |M_{i,j}|$ and $\|M\|_\infty = \max |M_{i,j}|$. The norms $\|v\|_1$ and $\|v\|_\infty$ for a real or complex vector v are defined analogously. The Euclidean

norm is given by $\|v\|_2 = \sqrt{\sum |v_i|^2}$. We denote the base-$q$ logarithm of x by $\log_q x$. In the special case of the binary logarithm, we write simply $\log x$ rather than $\log_2 x$.

2.2. Linear-algebraic preliminaries. Let $\mathbb{F}$ be a given field. We denote the set of $n \times m$ matrices over $\mathbb{F}$ by $\mathbb{F}^{n\times m}$. We use the standard notation $\operatorname{rk} A$, $\ker A$, and A^{T} for the rank, null space, and transpose of the matrix A. As usual, the determinant of $A \in \mathbb{F}^{n\times n}$ is denoted $\det A$. The trace of a matrix $A \in \mathbb{F}^{n\times n}$ is denoted $\operatorname{tr} A$ and defined as the sum of the diagonal elements of A. The commutativity of the trace operator is often helpful: $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ for square matrices A, B. We let $\operatorname{diag}(a_1, a_2, \ldots, a_n)$ denote the diagonal matrix of order n with diagonal entries $a_1, a_2, \ldots, a_n$. Recall that I_n normally denotes the identity matrix of order n, whereas I denotes the identity matrix whose order is to be inferred from the context. We generalize the meaning of I_n somewhat by defining

$$I_n = \operatorname{diag}(\underbrace{1, 1, \ldots 1}_{n}, 0, \ldots 0),$$

where the order of the matrix (and hence the number of zeroes on the diagonal) will be clear from the context. We let J and $\mathbf{1}$ denote the all-ones matrix and all-ones vector, respectively, whose dimensions will be clear from the context.

FACT 2.1. *For square matrices A, B of order n over a given field $\mathbb{F}$,*

$$\operatorname{rk} AB \geqslant \operatorname{rk} A + \operatorname{rk} B - n.$$

Proof. Recall that the dimension of $\ker AB$ is at most the sum of the dimensions of $\ker A$ and $\ker B$. By the rank-nullity theorem, this is equivalent to the claimed inequality. □

For $\mathbb{F}$ a finite field or the field of real numbers, the inner product operation on vectors and matrices is defined as usual by $\langle x, y\rangle = \sum x_i y_i$ and $\langle A, B\rangle = \sum A_{i,j} B_{i,j}$. For $\mathbb{F} = \mathbb{C}$, the modified definitions $\langle x, y\rangle = \sum x_i \overline{y_i}$ and $\langle A, B\rangle = \sum A_{i,j}\overline{B_{i,j}}$ are used instead. For complex-valued functions $f, g\colon X \to \mathbb{C}$, we write $\langle f, g\rangle = \sum_{x\in X} f(x)\overline{g(x)}$. Again for $\mathbb{F} = \mathbb{C}$, the conjugate transpose of a matrix $A = [A_{i,j}]_{i,j}$ is denoted by $A^* = [\overline{A_{j,i}}]_{i,j}$, and a matrix $A \in \mathbb{C}^{n\times n}$ is called *unitary* if $A^*A = AA^* = I$. The following useful fact relates the inner product and trace operators.

FACT 2.2. *Let A, B, C, D be matrices of order n over $\mathbb{R}$ or a finite field. Then:*

(i) $\langle A, B\rangle = \operatorname{tr}(AB^{\mathsf{T}}) = \operatorname{tr}(A^{\mathsf{T}}B)$,
(ii) $\langle A, C_1 B C_2\rangle = \langle C_1^{\mathsf{T}} A C_2^{\mathsf{T}}, B\rangle$.

Proof. Item (i) is immediate from the definition of matrix multiplication, whereas (ii) follows from (i) and the commutativity of the trace operator: $\langle A, C_1BC_2\rangle = \operatorname{tr}(AC_2^{\mathsf{T}}B^{\mathsf{T}}C_1^{\mathsf{T}}) = \operatorname{tr}(C_1^{\mathsf{T}}AC_2^{\mathsf{T}}B^{\mathsf{T}}) = \langle C_1^{\mathsf{T}}AC_2^{\mathsf{T}}, B\rangle$. □

Over any field $\mathbb{F}$, we let $e_1, e_2, \ldots, e_n$ denote as usual the vectors of the standard basis for $\mathbb{F}^n$. For any subset $S \subseteq \mathbb{F}^n$, recall that its span over $\mathbb{F}$ is denoted $\operatorname{span} S$. For a linear subspace S, the symbols $\dim S$ and $S^{\perp}$ refer as usual to the dimension of S and the orthogonal complement of S, respectively. For a linear transformation M, we let $M(S) = \{Mx : x \in S\}$ denote the image of S under M. Recall that the *sum* of linear subspaces S and T is defined as $S + T = \{x + y : x \in S, y \in T\}$ and is the smallest subspace that contains both S and T. In expressions involving subspaces, we adopt the convention that the union $\cup$ and intersection $\cap$ operators have higher precedence than the subspace sum operator $+$. For a vector space V and an integer k, we adopt the notation $\mathscr{S}(V, k)$ for the set of all subspaces of V of dimension k. For arbitrary subspaces S, T in a finite-dimensional vector space, the following identity is well-known, and we use it extensively in our proofs without further

mention:

$$\dim(S+T) = \dim(S) + \dim(T) - \dim(S \cap T). \tag{2.1}$$

This equation is one of the few instances when subspaces behave in ways analogous to sets. Such instances are rare. For example, unlike sets, general subspaces S, T, U need not satisfy $S \cap (T+U) = S \cap T + S \cap U$. The equality requires additional hypotheses, as recorded below.

FACT 2.3. *For any linear subspaces S, S', T with $S' \subseteq S$,*

$$S \cap (S' + T) = S' + S \cap T.$$

Proof. It is clear that $S' + S \cap T$ is a subspace of both S and $S' + T$. It remains to prove the opposite inclusion, $S \cap (S' + T) \subseteq S' + S \cap T$. For this, consider an arbitrary vector $u + v \in S$ with $u \in S'$ and $v \in T$. Then $v \in S + u = S$. As a result, $v \in S \cap T$ and therefore $u + v \in S' + S \cap T$ as claimed. □

We continue with a fact that relates the dimension of $S \cap T$ to that of $S^\perp \cap T^\perp$.

FACT 2.4. *Let $S, T \subseteq \mathbb{F}^n$ be subspaces over a given field $\mathbb{F}$. Then*

$$(S+T)^\perp = S^\perp \cap T^\perp, \tag{2.2}$$

$$(S \cap T)^\perp = S^\perp + T^\perp, \tag{2.3}$$

$$\dim(S \cap T) = \dim(S) + \dim(T) + \dim(S^\perp \cap T^\perp) - n. \tag{2.4}$$

Proof. To begin with,

$$\begin{aligned} S^\perp \cap T^\perp &= \{x : \langle x, y\rangle = 0 \text{ for all } y \in S\} \cap \{x : \langle x, y\rangle = 0 \text{ for all } y \in T\} \\ &= \{x : \langle x, y\rangle = 0 \text{ for all } y \in S \cup T\} \\ &= \{x : \langle x, y\rangle = 0 \text{ for all } y \in S + T\} \\ &= (S+T)^\perp, \end{aligned}$$

where the third step uses the linearity of inner product. This settles (2.2). Applying (2.2) to the orthogonal complements of S and T results in $(S^\perp + T^\perp)^\perp = S \cap T$, which upon orthogonal complementation of both sides yields (2.3). Equation (2.4) is also a straightforward consequence of (2.2), as follows:

$$\begin{aligned} \dim(S^\perp \cap T^\perp) &= \dim((S+T)^\perp) \\ &= n - \dim(S+T) \\ &= n - \dim(S) - \dim(T) + \dim(S \cap T). \end{aligned}$$

□

It is well-known that for a symmetric real matrix, any pair of eigenvectors corresponding to distinct eigenvalues are orthogonal. For completeness, we state this simple fact with a proof below.

FACT 2.5. *Let M be a symmetric real matrix. Let u, v be eigenvectors of M corresponding to different eigenvalues. Then $\langle u, v\rangle = 0$.*

Proof. Suppose that $Mu = \alpha u$ and $Mv = \beta v$, where $\alpha \neq \beta$. Then $(\alpha - \beta)\langle u, v\rangle = \langle \alpha u, v\rangle - \langle u, \beta v\rangle = \langle Mu, v\rangle - \langle u, Mv\rangle = 0$, where the last step uses $M = M^{\mathsf{T}}$. This forces $\langle u, v\rangle = 0$, as claimed. □

2.3. Matrix norms. Associated with every matrix $A \in \mathbb{C}^{n \times m}$ are $\min\{n, m\}$ nonnegative reals that are called the *singular values of A*, denoted $\sigma_1(A) \geqslant \sigma_2(A) \geqslant \cdots \geqslant \sigma_{\min\{n,m\}}(A)$. Every matrix $A \in \mathbb{C}^{n \times m}$ has a *singular value decomposition* $A = U\Sigma V^*$, where U and V are unitary matrices of order n and m, respectively, and Σ is a rectangular diagonal matrix whose diagonal entries are $\sigma_1(A), \sigma_2(A), \ldots, \sigma_{\min\{n,m\}}(A)$. In the case of real matrices A, the matrices U and V in the singular

value decomposition can be taken to be real. An alternative characterization of the singular values is given by

FACT 2.6. *Let $A \in \mathbb{C}^{n\times m}$ be given, with $n \leqslant m$. Then the singular values of A are precisely the square roots of the eigenvalues of AA^*, counting multiplicities.*

The spectral norm, trace norm, and Frobenius norm of A are defined in terms of the singular values as follows:

$$\|A\| = \sigma_1(A), \tag{2.5}$$

$$\|A\|_\Sigma = \sum \sigma_i(A), \tag{2.6}$$

$$\|A\|_{\mathrm{F}} = \sqrt{\sum \sigma_i(A)^2}. \tag{2.7}$$

Equivalently,

$$\|A\| = \max_{x:\|x\|_2=1} \|Ax\|_2, \tag{2.8}$$

$$\|A\|_{\mathrm{F}} = \sqrt{\sum |A_{ij}|^2}. \tag{2.9}$$

These equations agree with (2.5) and (2.7) because the Euclidean norm on vectors is invariant under unitary transformations.

FACT 2.7. *For any matrices $A, B \in \mathbb{C}^{n\times m}$,*

$$|\langle A, B\rangle| \leqslant \|A\|\, \|B\|_\Sigma.$$

Fact 2.7 follows directly from (2.8) and the singular value decomposition of B. We now recall a relationship between the trace norm and Frobenius norm; see, e.g., [24, Prop. 2.4].

FACT 2.8. *For all matrices A and B of compatible dimensions,*

$$\|AB\|_\Sigma \leqslant \|A\|_{\mathrm{F}}\, \|B\|_{\mathrm{F}}.$$

Recall that a *sign matrix* is a real matrix with entries in $\{-1, 1\}$. A *partial* sign matrix, then, is a matrix with entries in $\{-1, 1, *\}$. We define the *domain* of a partial sign matrix F by $\operatorname{dom} F = \{(i, j) : F_{ij} \neq *\}$. The *$\varepsilon$-approximate trace norm of F*, denoted $\|F\|_{\Sigma,\varepsilon}$, is the least trace norm of a real matrix $\widetilde{F}$ that satisfies

$$|F_{ij} - \widetilde{F}_{ij}| \leqslant \varepsilon \qquad \text{if } F_{ij} \in \{-1, 1\}, \tag{2.10}$$

$$|\widetilde{F}_{ij}| \leqslant 1 + \varepsilon \qquad \text{if } F_{ij} = *. \tag{2.11}$$

The following lower bound on the approximate trace norm is well known [15, 24, 25]. For reader's convenience, we include a proof.

PROPOSITION 2.9. *For any partial sign matrix F and $\varepsilon \geqslant 0$,*

$$\|F\|_{\Sigma,\varepsilon} \geqslant \sup_{\Phi\neq 0} \frac{1}{\|\Phi\|} \left(\sum_{(i,j)\in \operatorname{dom} F} F_{ij}\Phi_{ij} - \varepsilon\|\Phi\|_1 - \sum_{(i,j)\notin \operatorname{dom} F} |\Phi_{ij}| \right).$$

Proof. Let $\widetilde{F}$ be a real matrix that approximates F in the sense of (2.10) and (2.11). Then for any $\Phi \neq 0$,

$$\begin{aligned}
\langle \widetilde{F}, \Phi \rangle &= \sum_{\operatorname{dom} F} F_{ij}\Phi_{ij} + \sum_{\operatorname{dom} F} (\widetilde{F}_{ij} - F_{ij})\Phi_{ij} + \sum_{\overline{\operatorname{dom} F}} \widetilde{F}_{ij}\Phi_{ij} \\
&\geqslant \sum_{\operatorname{dom} F} F_{ij}\Phi_{ij} - \sum_{\operatorname{dom} F} |\widetilde{F}_{ij} - F_{ij}|\,|\Phi_{ij}| - \sum_{\overline{\operatorname{dom} F}} |\widetilde{F}_{ij}|\,|\Phi_{ij}| \\
&\geqslant \sum_{\operatorname{dom} F} F_{ij}\Phi_{ij} - \sum_{\operatorname{dom} F} \varepsilon|\Phi_{ij}| - \sum_{\overline{\operatorname{dom} F}} (1+\varepsilon)|\Phi_{ij}| \\
&= \sum_{\operatorname{dom} F} F_{ij}\Phi_{ij} - \varepsilon\|\Phi\|_1 - \sum_{\overline{\operatorname{dom} F}} |\Phi_{ij}|.
\end{aligned}$$

On the other hand, Fact 2.7 shows that $\langle \widetilde{F}, \Phi \rangle \leqslant \|\widetilde{F}\|_\Sigma \, \|\Phi\|$. Combining these two bounds for $\langle \widetilde{F}, \Phi \rangle$ gives

$$\|\widetilde{F}\|_\Sigma \geqslant \frac{1}{\|\Phi\|} \left(\sum_{\operatorname{dom} F} F_{ij}\Phi_{ij} - \varepsilon\|\Phi\|_1 - \sum_{\overline{\operatorname{dom} F}} |\Phi_{ij}| \right).$$

Taking the supremum over $\Phi \neq 0$ completes the proof. □

2.4. Fourier transform. Consider a prime power $q = p^k$, with p a prime and k a positive integer. Recall that the additive group of $\mathbb{F}_q$ is isomorphic to the Abelian group $\mathbb{Z}_p^k$. Fix any such isomorphism ψ. Let $\omega = e^{2\pi i/p}$, a primitive p-th root of unity. For $x \in \mathbb{F}_q$, define $\omega^x = \omega^{x_1}\omega^{x_2}\cdots\omega^{x_k}$, where $(x_1, x_2, \ldots, x_k)$ is the image of x under ψ. Then for all $x, y \in \mathbb{F}_q$,

$$\omega^{x+y} = \omega^x \omega^y, \tag{2.12}$$

$$\omega^{-x} = \overline{\omega^x}. \tag{2.13}$$

One further calculates $\sum_{x\in\mathbb{F}_q} \omega^x = \prod_{i=1}^k (1 + \omega + \omega^2 + \cdots + \omega^{p-1}) = 0$, which in turn generalizes to

$$\sum_{x\in\mathbb{F}_q} \omega^{ax} = 0, \qquad a \in \mathbb{F}_q \setminus \{0\} \tag{2.14}$$

since $x \mapsto ax$ is a permutation on $\mathbb{F}_q$.

Let n be a positive integer. For $A \in \mathbb{F}_q^{n\times n}$, define a corresponding character $\chi_A : \mathbb{F}_q^{n\times n} \to \mathbb{C}$ by

$$\chi_A(X) = \omega^{\langle A, X\rangle}.$$

It follows from (2.12) that

$$\chi_A(X+Y) = \chi_A(X)\chi_A(Y), \tag{2.15}$$

making χ_A a homomorphism of the additive group $\mathbb{F}_q^{n\times n}$ into the multiplicative group of $\mathbb{C}$. Using (2.12) and (2.13), one obtains $\langle \chi_A, \chi_B \rangle = \sum_X \omega^{\langle A,X\rangle}\overline{\omega^{\langle B,X\rangle}} = \sum_X \omega^{\langle A,X\rangle - \langle B,X\rangle} = \sum_X \omega^{\langle A-B,X\rangle}$, which along with (2.14) leads to

$$\langle \chi_A, \chi_B \rangle = \begin{cases} q^{n^2} & \text{if } A = B, \\ 0 & \text{otherwise.} \end{cases} \tag{2.16}$$

Hence, the characters χ_A for $A \in \mathbb{F}_q^{n\times n}$ form an orthogonal basis for the complex vector space of functions $\mathbb{F}_q^{n\times n} \to \mathbb{C}$. In particular, every function $f\colon \mathbb{F}_q^{n\times n} \to \mathbb{C}$ has a unique representation as a

linear combination of the characters:

$$f(X) = \sum_{A \in \mathbb{F}_q^{n \times n}} \widehat{f}(A)\chi_A(X). \tag{2.17}$$

The numbers $\widehat{f}(A)$ are called the *Fourier coefficients of* f. They are given by

$$\widehat{f}(A) = q^{-n^2}\langle f, \chi_A \rangle = \mathop{\mathbf{E}}_{X \in \mathbb{F}_q^{n \times n}} f(X)\omega^{-\langle A, X \rangle}. \tag{2.18}$$

where the first step is justified by (2.16), and the second step uses (2.13). An immediate consequence of (2.16) and (2.17) is that $\langle f, f \rangle = q^{n^2} \sum_A |\widehat{f}(A)|^2$. This result is known as *Parseval's identity,* and it is typically written in the form

$$\mathop{\mathbf{E}}_{X \in \mathbb{F}_q^{n \times n}}[|f(X)|^2] = \sum_{A \in \mathbb{F}_q^{n \times n}} |\widehat{f}(A)|^2. \tag{2.19}$$

With $\widehat{f}$ viewed as a complex-valued function on $\mathbb{F}_q^{n \times n}$, the linear transformation that sends $f \mapsto \widehat{f}$ is called the *Fourier transform.* Its matrix representation is easy to describe. Specifically, define

$$H_n = q^{-n^2/2}[\omega^{\langle A, B \rangle}]_{A,B},$$

where the row and column indices range over all matrices in $\mathbb{F}_q^{n \times n}$. Analogous to (2.16), one shows that H_n is unitary:

$$H_n H_n^* = H_n^* H_n = I. \tag{2.20}$$

Then the Fourier transform $f \mapsto \widehat{f}$, given by (2.18), corresponds to the linear transformation $q^{-n^2/2}H_n^*$. Analogously, the inverse transformation $\widehat{f} \mapsto f$ of (2.17) corresponds to $q^{n^2/2}H_n$.

The following well-known fact relates the singular values of a matrix $[\varphi(A+B)]_{A,B}$ to the Fourier spectrum of the outer function φ. We include a proof adapted from [16] and generalized to the case of $\mathbb{F}_q$.

Fact 2.10 (adapted from Li et al., Lemma 20). *Let* $\varphi : \mathbb{F}_q^{n \times n} \to \mathbb{C}$ *be given. Define*

$$\Phi = [\varphi(X + Y)]_{X,Y \in \mathbb{F}_q^{n \times n}}.$$

Then

$$\Phi = H_n D H_n,$$

where D *is the diagonal matrix given by* $D_{A,A} = q^{n^2}\widehat{\varphi}(A)$. *In particular, the singular values of* Φ *are* $q^{n^2}|\widehat{\varphi}(A)|$ *for* $A \in \mathbb{F}_q^{n \times n}$.

Proof. Using the homomorphic property (2.15) of the characters,

$$\begin{aligned}\varphi(X + Y) &= \sum_{A \in \mathbb{F}_q^{n \times n}} \widehat{\varphi}(A)\chi_A(X + Y) \\ &= \sum_{A \in \mathbb{F}_q^{n \times n}} \widehat{\varphi}(A)\chi_A(X)\chi_A(Y).\end{aligned}$$

Restated in matrix form, this equation becomes $\Phi = [\chi_A(X)]_{X,A}\ \mathrm{diag}(\ldots, \widehat{\varphi}(A), \ldots)\,[\chi_A(Y)]_{A,Y} = H_n D H_n$, as desired. ∎

2.5. Gaussian binomial coefficients. *Gaussian binomial coefficients*, also known as *q-binomial coefficients*, are defined by

$$\binom{n}{m}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{m-1})}{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})} \tag{2.21}$$

$$= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-m+1}-1)}{(q^m-1)(q^{m-1}-1)\cdots(q-1)} \tag{2.22}$$

for all nonnegative integers n, m and real numbers $q > 1$. Observe that $\binom{n}{0}_q = 1$ since the above product is empty for $m = 0$. Note further that $\binom{n}{m}_q = 0$ whenever $m > n$. One recovers standard binomial coefficients from this definition via

$$\lim_{q \searrow 1} \binom{n}{m}_q = \binom{n}{m}.$$

As a matter of convenience, one generalizes Gaussian binomial coefficients to arbitrary integers n, m by defining

$$\binom{n}{m}_q = 0 \qquad \text{if } \min\{n, m\} < 0.$$

With this convention, one has the familiar identity

$$\binom{n}{m}_q = \binom{n}{n-m}_q, \qquad n, m \in \mathbb{Z}. \tag{2.23}$$

Gaussian binomial coefficients play an important role in enumerative combinatorics. In particular, we recall the following classical fact.

FACT 2.11. *Fix a prime power q and integers $n \geqslant m \geqslant 0$. Then the number of m-dimensional subspaces of $\mathbb{F}_q^n$ is exactly $\binom{n}{m}_q$.*

Proof. This result is clearly true for $m = 0$. For $m \geqslant 1$, there are $(q^n-1)(q^n-q)\cdots(q^n-q^{m-1})$ ordered bases $(v_1, v_2, \ldots, v_m)$ of vectors in $\mathbb{F}_q^n$. Each such basis defines an m-dimensional subspace. Conversely, every m-dimensional subspace has exactly $(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})$ ordered bases. Thus, the number of m-dimensional subspaces is (2.21), as claimed. □

The following monotonicity property of q-binomial coefficients is well-known. We provide a proof for convenience.

FACT 2.12. *Let $n \geqslant m \geqslant 0$ be given integers. Then for all integers $\ell \in [m, n-m]$ and reals $q > 1$,*

$$\binom{n}{m}_q \leqslant \binom{n}{\ell}_q. \tag{2.24}$$

Proof. The defining equation (2.22) gives

$$\binom{n}{\ell}_q = \binom{n}{m}_q \cdot \prod_{i=m+1}^{\ell} \frac{q^{n-i+1}-1}{q^i-1}.$$

If $\ell \leqslant n/2$, then every fraction in the above product is greater than 1. As a result, (2.24) holds in this case. In the complementary case $\ell > n/2$, we have $n - \ell \in [m, n/2]$ and therefore

$$\binom{n}{m}_q \leqslant \binom{n}{n-\ell}_q$$

by the first part of the proof. Since $\binom{n}{n-\ell}_q = \binom{n}{\ell}_q$, we again arrive at (2.24). □

We will use the next proposition to accurately estimate Gaussian binomial coefficients.

PROPOSITION 2.13. *For any set I of positive integers, and any real number $x \geqslant 2$,*

$$\frac{1}{4} \leqslant \prod_{i \in I} \left(1 - \frac{1}{x^i}\right) \leqslant 1.$$

Proof. The upper bound is trivial. For the lower bound, we may clearly assume that $I = \{1, 2, 3 \ldots\}$. A simple inductive argument shows that $(1-a_1)\cdots(1-a_n) \geqslant 1 - a_1 - \cdots - a_n$ for any $a_1, \ldots, a_n \in (0,1)$. It follows that

$$\prod_{i=2}^{\infty} \left(1 - \frac{1}{x^i}\right) \geqslant 1 - \frac{1}{x^2} - \frac{1}{x^3} - \ldots = 1 - \frac{1}{x(x-1)}$$

and therefore

$$\prod_{i=1}^{\infty} \left(1 - \frac{1}{x^i}\right) \geqslant \left(1 - \frac{1}{x}\right)\left(1 - \frac{1}{x(x-1)}\right) \geqslant \frac{1}{4},$$

where the last step uses $x \geqslant 2$. ∎

COROLLARY 2.14. *For any integers $n \geqslant m \geqslant 0$ and any real number $q \geqslant 2$,*

$$q^{m(n-m)} \leqslant \binom{n}{m}_q \leqslant 4q^{m(n-m)}.$$

Proof. The lower bound follows directly from the fact that $(q^n - q^i)/(q^m - q^i) \geqslant q^n/q^m$ for $n \geqslant m$. The upper bound can be verified as follows:

$$\binom{n}{m}_q = \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{m-1})}{(q^m-1)(q^m-q)\ldots(q^m-q^{m-1})} \leqslant \frac{q^{nm}}{q^{m^2}\prod_{i=1}^{m}(1-q^{-i})} \leqslant 4q^{m(n-m)},$$

where the last step applies Proposition 2.13. ∎

We now recall a classical result known as the *Cauchy binomial theorem*, see, e.g., [26, eqn. (1.87)].

FACT 2.15. *For any integer $n \geqslant 1$ and real number $q > 1$, the following identity holds in $\mathbb{R}[t]$:*

$$(1+t)(1+qt)\ldots(1+q^{n-1}t) = \sum_{i=0}^{n} q^{\binom{i}{2}} \binom{n}{i}_q t^i. \tag{2.25}$$

COROLLARY 2.16. *For any integer $n \geqslant 1$ and real number $q > 1$, and any real polynomial g of degree less than n,*

$$\sum_{i=0}^{n} (-1)^i q^{\binom{i}{2}} \binom{n}{i}_q g(q^{-i}) = 0. \tag{2.26}$$

Proof. For $d = 0, 1, \ldots, n-1$, take $t = -1/q^d$ in (2.25) to obtain

$$\sum_{i=0}^{n} (-1)^i q^{\binom{i}{2}} \binom{n}{i}_q (q^{-i})^d = 0. \tag{2.27}$$

This establishes (2.26) when g is a *monomial* of degree less than n. The general case follows by linearity: multiply (2.27) by the degree-d coefficient in g and sum over d.

∎

2.6. Counting and generating matrices of given rank. For a field $\mathbb{F}$, we let $\mathscr{M}_r^{\mathbb{F},n,m}$ denote the set of matrices in $\mathbb{F}^{n\times m}$ of rank r. Since we mostly use $\mathbb{F} = \mathbb{F}_q$ in this work, we will usually omit the reference to the field and write simply $\mathscr{M}_r^{n,m}$. As a matter of convenience, we adopt the convention that for any $n \geqslant 0$ there is exactly one "matrix" of size $0 \times n$ and exactly one "matrix" of size $n \times 0$, both of rank 0. The role of these empty matrices is to ensure that

$$|\mathscr{M}_0^{0,n}| = |\mathscr{M}_0^{n,0}| = 1, \qquad n \geqslant 0,$$

which simplifies the statement of several lemmas in this paper. Analogously, we define

$$\mathscr{M}_r^{n,m} = \varnothing \qquad \text{if } \min\{n,m,r\} < 0. \tag{2.28}$$

For nonsingular matrices of order $n \geqslant 1$, we adopt the shorthand $\mathscr{M}_n = \mathscr{M}_n^{n,n}$.

PROPOSITION 2.17. *Let n, m, r be nonnegative integers with $r \leqslant \min\{n,m\}$. Then*

$$|\mathscr{M}_r^{n,m}| = \binom{n}{r}_q (q^m - 1)(q^m - q)\dots(q^m - q^{r-1}). \tag{2.29}$$

Proof. If $r = 0$, then the right-hand side of (2.29) evaluates to 1. This is consistent with our convention that $|\mathscr{M}_0^{n,m}| = 1$ for all $n, m \geqslant 0$.

We now consider the complementary case $r \geqslant 1$, which forces n and m to be positive. Fix an arbitrary r-dimensional subspace $S \subseteq \mathbb{F}_q^n$ and consider the subset $\mathscr{M}_S \subseteq \mathscr{M}_r^{n,m}$ of matrices whose column space is S. Fix an $n \times r$ matrix A with column space S. Since the columns of A are linearly independent, every matrix in $\mathscr{M}_S$ has a unique representation of the form AB for some $B \in \mathscr{M}_r^{r,m}$. Conversely, any product AB with $B \in \mathscr{M}_r^{r,m}$ is a matrix in $\mathscr{M}_S$. Therefore,

$$|\mathscr{M}_S| = |\mathscr{M}_r^{r,m}|. \tag{2.30}$$

Recall that $\mathscr{M}_r^{n,m}$ is the disjoint union of $\mathscr{M}_S$ over r-dimensional subspaces $S \subseteq \mathbb{F}_q^n$, and there are precisely $\binom{n}{r}_q$ such subspaces (Fact 2.11). With this in mind, (2.30) leads to

$$|\mathscr{M}_r^{n,m}| = \binom{n}{r}_q |\mathscr{M}_r^{r,m}|. \tag{2.31}$$

Finally, the number of $r \times m$ matrices of rank r is precisely the number of bases $(v_1, v_2, \dots, v_r)$ of row vectors in $\mathbb{F}_q^m$, whence $|\mathscr{M}_r^{r,m}| = (q^m - 1)(q^m - q)\cdots(q^m - q^{r-1})$. Making this substitution in (2.31) completes the proof. □

Using Proposition 2.13 and Corollary 2.14 to estimate the right-hand side of (2.29), we obtain:

COROLLARY 2.18. *Let m, n, r be nonnegative integers with $r \leqslant \min\{n,m\}$. Then*

$$\frac{1}{4} q^{r(n+m-r)} \leqslant |\mathscr{M}_r^{n,m}| \leqslant 4q^{r(n+m-r)}.$$

The following fact is well-known; cf. [16].

PROPOSITION 2.19. *Let $n \geqslant 1$ be a given integer. Let X, Y be random matrices distributed independently and uniformly on $\mathscr{M}_n$. Then:*

(i) *for any fixed $A \in \mathscr{M}_n$, the matrices XA and AX are distributed uniformly on $\mathscr{M}_n$;*
(ii) *for any $r \in \{0, 1, \dots, n\}$ and fixed $A \in \mathscr{M}_r^{n,n}$, the matrix XAY is distributed uniformly on $\mathscr{M}_r^{n,n}$.*

Proof. (i) For any $B \in \mathscr{M}_n$, we have $\mathbf{P}[XA = B] = \mathbf{P}[X = BA^{-1}] = 1/|\mathscr{M}_n|$. Therefore, XA is distributed uniformly on $\mathscr{M}_n$. The argument for AX is analogous.

(ii) Fix $B \in \mathscr{M}_r^{n,n}$ arbitrarily. Then B can be obtained from A by a series of elementary row and column operations, so that $B = M_1 A M_2$ for nonsingular M_1, M_2. As a result,

$$\mathbf{P}[XAY = B] = \mathbf{P}[M_1^{-1} XAY M_2^{-1} = A] = \mathbf{P}[XAYM_2^{-1} = A] = \mathbf{P}[XAY = A],$$

where the last two steps are valid by part (i). To summarize, XAY takes on every value in $\mathscr{M}_r^{n,n}$ with the same probability. Since $XAY \in \mathscr{M}_r^{n,n}$, the proof is complete. □

2.7. Random projections. Given a collection of subspaces $S_1, S_2, \ldots, S_m$ in a vector space, we use random projections to reduce the dimension of the ambient space while preserving algebraic relationships among the S_i. This is done by choosing a uniformly random matrix X and replacing $S_1, S_2, \ldots, S_m$ with the subspaces $X(S_1), X(S_2), \ldots, X(S_m)$, respectively. The following lemma provides quantitative details.

LEMMA 2.20. *Let n and d be positive integers, $\mathbb{F}$ a finite field with $q = |\mathbb{F}|$ elements, and $S \subseteq \mathbb{F}^n$ a subspace. Then for every integer $t \leqslant \min\{\dim(S), d\}$,*

$$\mathop{\mathbf{P}}_{X \in \mathbb{F}^{d\times n}}[\dim(X(S)) \leqslant t] \leqslant 4q^{-(\dim(S)-t)(d-t)}. \tag{2.32}$$

In particular, for every integer $T \leqslant \min\{\dim(S), d\}$,

$$\mathop{\mathbf{E}}_{X \in \mathbb{F}^{d\times n}} q^{T-\min\{T,\dim(X(S))\}} \leqslant 1 + 8q^{-(\dim(S)-T+1)(d-T+1)+1}. \tag{2.33}$$

Proof. Equations (2.32) and (2.33) hold trivially for negative t and T, respectively. As a result, we may assume that $t \geqslant 0$ and $T \geqslant 0$. Abbreviate $k = \dim(S)$. Fix a basis $v_1, v_2, \ldots, v_k$ for S and extend it to a basis $v_1, v_2, \ldots, v_n$ for $\mathbb{F}^n$. Let $A \in \mathbb{F}^{n\times n}$ be the unique matrix such that $Av_i = e_i$ for each $i = 1, 2, \ldots, n$. In particular, $A(S) = \operatorname{span}\{e_1, e_2, \ldots, e_k\}$. Now, let $X \in \mathbb{F}^{d\times n}$ be uniformly random. Then the rows of XA are independent random variables, each a uniformly random linear combination of the rows of A. Since A is nonsingular of order n, it follows that the rows of XA are independent random vectors in $\mathbb{F}^n$. Put another way, $XA \in \mathbb{F}^{d\times n}$ has the same distribution as X. As a result,

$$\begin{aligned}
\mathbf{P}[\dim(X(S)) \leqslant t] &= \mathbf{P}[\dim(XA(S)) \leqslant t] \\
&= \mathbf{P}[\dim(X(A(S))) \leqslant t] \\
&= \mathbf{P}[\dim(\operatorname{span}\{Xe_1, Xe_2, \ldots, Xe_k\}) \leqslant t] \\
&= \mathbf{P}[\exists B \in \mathscr{S}(\mathbb{F}^d, t) \text{ such that } Xe_1, Xe_2, \ldots, Xe_k \in B] \\
&\leqslant \sum_{B \in \mathscr{S}(\mathbb{F}^d,t)} \mathbf{P}[Xe_1, Xe_2, \ldots, Xe_k \in B],
\end{aligned} \tag{2.34}$$

where the third step uses $A(S) = \operatorname{span}\{e_1, e_2, \ldots, e_k\}$, and the last step applies a union bound. Now

$$\mathbf{P}[\dim(X(S)) \leqslant t] \leqslant \sum_{\mathscr{S}(\mathbb{F}^d,t)} \left(\frac{q^t}{q^d}\right)^k = \binom{d}{t}_q q^{-k(d-t)} \leqslant 4q^{t(d-t)} q^{-k(d-t)} = 4q^{-(k-t)(d-t)},$$

where the first step is justified by (2.34) and the fact that $Xe_1, Xe_2, \ldots, Xe_k$ are independent and uniformly random vectors in $\mathbb{F}^d$; the second step applies Fact 2.11; and the third step uses Corollary 2.14. This settles (2.32). Now (2.33) can be verified as follows:

$$\begin{aligned}
\mathbf{E}\, q^{T-\min\{T,\dim(X(S))\}} &\leqslant 1 + \sum_{t=0}^{T-1} q^{T-t}\, \mathbf{P}[\dim(X(S)) = t] \\
&\leqslant 1 + \sum_{t=0}^{T-1} q^{T-t} \cdot 4q^{-(k-t)(d-t)} \\
&= 1 + \sum_{t=1}^{T} q^{t} \cdot 4q^{-(k-T+t)(d-T+t)} \\
&= 1 + \sum_{t=1}^{T} q^{t} \cdot 4q^{-(k-T+1)(d-T+1)-(t-1)(d+k+t-2T+1)} \\
&\leqslant 1 + \sum_{t=1}^{\infty} q^{t} \cdot 4q^{-(k-T+1)(d-T+1)-(t^2-1)} \\
&\leqslant 1 + 4q^{-(k-T+1)(d-T+1)+1} \cdot \frac{q}{q-1} \\
&\leqslant 1 + 8q^{-(k-T+1)(d-T+1)+1},
\end{aligned}$$

where the third step is a change of variable, the next-to-last step bounds the series by a geometric series, and the last step is valid due to $q \geqslant 2$. □

The previous lemma yields an analogous results for matrices:

LEMMA 2.21. *Let n, m, d be positive integers, $\mathbb{F}$ a finite field with $q = |\mathbb{F}|$ elements, and $M \in \mathbb{F}^{n\times m}$ a given matrix. Then for every integer $t \leqslant \min\{\operatorname{rk} M, d\}$:*

(i) $\mathbf{P}[\operatorname{rk}(XM) \leqslant t] \leqslant 4q^{-(\operatorname{rk}(M)-t)(d-t)}$ *for a uniformly random matrix $X \in \mathbb{F}^{d\times n}$;*
(ii) $\mathbf{P}[\operatorname{rk}(MY) \leqslant t] \leqslant 4q^{-(\operatorname{rk}(M)-t)(d-t)}$ *for a uniformly random matrix $Y \in \mathbb{F}^{m\times d}$.*

Proof. Let S be the column span of M. Then $\operatorname{rk}(XM) = \dim(X(S))$, and (i) follows from Lemma 2.20. For (ii), rewrite the probability of interest as $\mathbf{P}[\operatorname{rk}(Y^{\mathsf{T}}M^{\mathsf{T}}) \leqslant t]$ and apply (i). □

2.8. Communication complexity. An excellent reference on communication complexity is the monograph by Kushilevitz and Nisan [14]. In this overview, we will limit ourselves to key definitions and notation. The *public-coin randomized model*, due to Yao [29], features two players Alice and Bob and a (possibly partial) Boolean function $F\colon X \times Y \to \{-1, 1, *\}$ for finite sets X and Y. Alice is given as input an element $x \in X$, Bob is given $y \in Y$, and their objective is to evaluate $F(x, y)$. To this end, Alice and Bob communicate by sending bits according to a protocol agreed upon in advance. Moreover, they have an unlimited supply of shared random bits which they can use when deciding what message to send at any given point in the protocol. Eventually, they must agree on a bit (-1 or 1) that represents the output of the protocol. An *ε-error protocol* for F is one which, on every input $(x, y) \in \operatorname{dom} F$, produces the correct answer $F(x, y)$ with probability at least $1 - \varepsilon$. The protocol's behavior on inputs outside $\operatorname{dom} F$ can be arbitrary. The *cost* of a protocol is the total bit length of the messages exchanged by Alice and Bob in the worst-case execution of the protocol. The *ε-error randomized communication complexity of F*, denoted $R_\varepsilon(F)$, is the least cost of an ε-error randomized protocol for F. The standard setting of the error parameter is $\varepsilon = 1/3$, which can be replaced by any other constant in $(0, 1/2)$ with only a constant-factor change in communication cost.

A far-reaching generalization of the randomized model is Yao's *quantum model* [30], where Alice and Bob exchange *quantum* messages. As before, their objective is to evaluate a fixed function $F\colon X \times Y \to \{-1, 1, *\}$ on any given input pair (x, y), where Alice receives as input x and Bob receives y. We allow arbitrary *prior entanglement* at the start of the communication, which is the quantum analogue of shared randomness. A measurement at the end of the protocol produces a one-bit answer, which is interpreted as the protocol output. An *ε-error protocol for F* is required to output, on every input $(x, y) \in \operatorname{dom} F$, the correct value $F(x, y)$ with probability at least $1 - \varepsilon$. As before, the protocol can exhibit arbitrary behavior on inputs outside $\operatorname{dom} F$. The *cost* of a quantum protocol is the total number of quantum bits exchanged in the worst-case execution. The *ε-error quantum communication complexity of F*, denoted $Q^*_\varepsilon(F)$, is the least cost of an ε-error quantum protocol for F. The asterisk in $Q^*_\varepsilon(F)$ indicates that the parties can share arbitrary prior entanglement. As before, the standard setting of the error parameter is $\varepsilon = 1/3$. For a detailed formal description of the quantum model, we refer the reader to [28, 22, 24]. For any protocol Π, quantum or otherwise, we write $\operatorname{cost}(\Pi)$ for the communication cost of Π.

The following theorem, due to Linial and Shraibman [17, Lem. 10], states that the matrix of the acceptance probabilities of a quantum protocol has an efficient factorization with respect to the Frobenius norm. Closely analogous statements were established earlier by Yao [30], Kremer [13], and Razborov [22].

THEOREM 2.22. *Let X, Y be finite sets. Let P be a quantum protocol (with or without prior entanglement) with cost C qubits and input sets X and Y. Then*

$$\Big[\, \mathbf{P}[P(x, y) = 1] \Big]_{x \in X, y \in Y} = AB$$

for some real matrices A, B with $\|A\|_{\mathrm{F}} \leqslant 2^C \sqrt{|X|}$ and $\|B\|_{\mathrm{F}} \leqslant 2^C \sqrt{|Y|}$.

Theorem 2.22 provides a transition from quantum protocols to matrix factorization, which is by now a standard technique that has been used by various authors in various contexts. Among other things, Theorem 2.22 gives the following *approximate trace norm method* for quantum lower bounds; see, e.g., [22, Thm. 5.5]. For the reader's convenience, we state and prove this result in the generality that we require.

THEOREM 2.23 (Approximate trace norm method). *Let $F\colon X \times Y \to \{-1, 1, *\}$ be a (possibly partial) communication problem. Then*

$$4^{Q^*_\varepsilon(F)} \geqslant \frac{\|M\|_{\Sigma, 2\varepsilon}}{3\sqrt{|X|\,|Y|}},$$

where $M = [F(x, y)]_{x \in X, y \in Y}$ is the characteristic matrix of F.

Proof. Let P be a quantum protocol with prior entanglement that computes F with error ε and cost C. Put

$$\Pi = \Big[\, \mathbf{P}[P(x, y) = 1] \Big]_{x \in X,\, y \in Y}.$$

Then the matrix $\widetilde{M} = 2\Pi - J$ satisfies $|\widetilde{M}_{x,y}| \leqslant 1$ for all $(x, y) \in X \times Y$ and $|M_{x,y} - \widetilde{M}_{x,y}| \leqslant 2\varepsilon$ for all $(x, y) \in \operatorname{dom} M$. In particular,

$$\|M\|_{\Sigma, 2\varepsilon} \leqslant \|\widetilde{M}\|_{\Sigma}. \tag{2.35}$$

On the other hand, Theorem 2.22 guarantees the existence of matrices A and B with $AB = \Pi$ and $\|A\|_{\mathrm{F}}\,\|B\|_{\mathrm{F}} \leqslant 4^C\sqrt{|X|\,|Y|}$. Therefore,

$$\begin{aligned}\|\widetilde{M}\|_\Sigma &= \|2AB - J\|_\Sigma \\ &\leqslant 2\|AB\|_\Sigma + \|J\|_\Sigma \\ &\leqslant 2\|A\|_{\mathrm{F}}\|B\|_{\mathrm{F}} + \|J\|_\Sigma \\ &\leqslant 2\cdot 4^C\sqrt{|X|\,|Y|} + \|J\|_\Sigma \\ &= 2\cdot 4^C\sqrt{|X|\,|Y|} + \sqrt{|X|\,|Y|}, \end{aligned} \tag{2.36}$$

where the third step uses Fact 2.8. Equations (2.35) and (2.36) give $\|M\|_{\Sigma,2\varepsilon} \leqslant (2\cdot 4^C+1)\sqrt{|X|\,|Y|}$, which implies the claimed lower bound on 4^C. □

A *distinguisher* for a communication problem $F\colon X\times Y \to \{-1,1,*\}$ is a communication protocol Π for which the expected output on every input in $F^{-1}(-1)$ is less than the expected output on every input in $F^{-1}(1)$. We will use the following proposition to convert any distinguisher for F into a communication protocol that computes F.

Proposition 2.24. *Let $F\colon X \times Y \to \{-1,1,*\}$ be a (possibly partial) communication problem. Suppose that Π is a cost-c randomized protocol with output ± 1 such that*

$$\mathbf{E}[\Pi(x,y)] \leqslant \alpha \qquad \text{for all } (x,y) \in F^{-1}(-1), \tag{2.37}$$

$$\mathbf{E}[\Pi(x,y)] \geqslant \beta \qquad \text{for all } (x,y) \in F^{-1}(1), \tag{2.38}$$

where α,β are reals with $-1 \leqslant \alpha \leqslant \beta \leqslant 1$. Then

$$R_{\frac{1}{2}-\frac{1}{8}(\beta-\alpha)}(F) \leqslant c.$$

Proof. For a real number t, define $\widetilde{\operatorname{sgn}}\,t$ to be 1 if $t \geqslant 0$ and -1 if $t < 0$. Set $p = |\alpha+\beta|/(2+|\alpha+\beta|)$ and consider the following randomized protocol Π' with input $(x,y) \in X\times Y$: with probability p, Alice and Bob output $-\widetilde{\operatorname{sgn}}(\alpha+\beta)$ without any communication; with the complementary probability $1-p$, they execute the original protocol Π on (x,y) and output its answer. Clearly, Π' has the same cost as Π. On every $(x,y) \in F^{-1}(-1)$,

$$\mathbf{E}[\Pi'(x,y)] \leqslant -p\,\widetilde{\operatorname{sgn}}(\alpha+\beta) + (1-p)\alpha = \frac{-(\alpha+\beta)+2\alpha}{2+|\alpha+\beta|} = \frac{\alpha-\beta}{2+|\alpha+\beta|} \leqslant -\frac{\beta-\alpha}{4},$$

where the first step uses (2.37), and the last step uses $-1 \leqslant \alpha \leqslant \beta \leqslant 1$. Analogously, on every $(x,y) \in F^{-1}(1)$,

$$\mathbf{E}[\Pi'(x,y)] \geqslant -p\,\widetilde{\operatorname{sgn}}(\alpha+\beta) + (1-p)\beta = \frac{-(\alpha+\beta)+2\beta}{2+|\alpha+\beta|} = \frac{\beta-\alpha}{2+|\alpha+\beta|} \geqslant \frac{\beta-\alpha}{4},$$

where the first step uses (2.38). We have shown that $\mathbf{E}[\Pi'(x,y)F(x,y)] \geqslant (\beta-\alpha)/4$ on the domain of F, which is another way of saying that Π' computes F with error at most $\frac{1}{2} - \frac{1}{8}(\beta-\alpha)$. □

2.9. Communication problems defined. Let $\mathbb{F}$ be a given field. For nonnegative integers n, m, r with $r \leqslant \min\{n,m\}$, the *rank problem* is the communication problem in which Alice and Bob are given matrices $A, B \in \mathbb{F}^{n\times m}$, respectively, and their objective is to determine whether $\operatorname{rk}(A+B) \leqslant r$. Formally, this problem corresponds to the Boolean function $\mathrm{RANK}_r^{\mathbb{F},n,m}\colon \mathbb{F}^{n\times m}\times\mathbb{F}^{n\times m} \to \{-1,1\}$ given by

$$\mathrm{RANK}_r^{\mathbb{F},n,m}(A+B) = -1 \qquad \Leftrightarrow \qquad \operatorname{rk}(A+B) \leqslant r.$$

We also study the corresponding partial problem $\mathrm{RANK}_{r,R}^{\mathbb{F},n,m}$ for nonnegative integers n, m, r, R with $r < R \leqslant \min\{n, m\}$, defined on $\mathbb{F}^{n\times m} \times \mathbb{F}^{n\times m}$ by

$$\mathrm{RANK}_{r,R}^{\mathbb{F},n,m}(A,B) = \begin{cases} -1 & \text{if } \mathrm{rk}(A+B) = r, \\ 1 & \text{if } \mathrm{rk}(A+B) = R, \\ * & \text{otherwise.} \end{cases}$$

For a positive integer n and a pair of distinct field elements $a, b \in \mathbb{F}$, the *determinant problem* $\mathrm{DET}_{a,b}^{\mathbb{F},n} \colon \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times n} \to \{-1, 1, *\}$ is given by

$$\mathrm{DET}_{a,b}^{\mathbb{F},n}(A,B) = \begin{cases} -1 & \text{if } \det(A+B) = a, \\ 1 & \text{if } \det(A+B) = b, \\ * & \text{otherwise.} \end{cases}$$

The *rank versus determinant problem* is a hybrid inspired by the previous two problems. Specifically, for a number $r \in \{0, 1, \ldots, n-1\}$ and a nonzero field element $a \in \mathbb{F} \setminus \{0\}$, we define $\mathrm{RANKDET}_{r,a}^{\mathbb{F},n} \colon \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times n} \to \{-1, 1, *\}$ by

$$\mathrm{RANKDET}_{r,a}^{\mathbb{F},n}(A,B) = \begin{cases} -1 & \text{if } \mathrm{rk}(A+B) = r, \\ 1 & \text{if } \det(A+B) = a, \\ * & \text{otherwise.} \end{cases}$$

Note that $\mathrm{RANKDET}_{r,a}^{\mathbb{F},n}$ is a *subproblem* of both $\mathrm{RANK}_{r,n}^{\mathbb{F},n,n}$ and $\mathrm{DET}_{0,a}^{\mathbb{F},n}$, in the sense that the domain of $\mathrm{RANKDET}_{r,a}^{\mathbb{F},n}$ is a subset of the domain of each of these other two problems and it agrees on its domain with those problems.

Consider now the setting where Alice is given an m-dimensional subspace $S \subseteq \mathbb{F}^n$ and Bob is given an ℓ-dimensional subspace $T \subseteq \mathbb{F}^n$, for some nonnegative integers n, m, ℓ with $\max\{m, \ell\} \leqslant n$. In the *subspace intersection problem* with parameter d, Alice and Bob need to determine whether $S \cap T$ has dimension at least d. In the *subspace sum problem*, they need to determine whether $S + T$ has dimension at most d. Formally, these problems correspond to the Boolean functions $\mathrm{INTERSECT}_d^{\mathbb{F},n,m,\ell}$ and $\mathrm{SUM}_d^{\mathbb{F},n,m,\ell}$ that are defined on $\mathscr{S}(\mathbb{F}^n, m) \times \mathscr{S}(\mathbb{F}^n, \ell)$ by

$$\begin{aligned} \mathrm{INTERSECT}_d^{\mathbb{F},n,m,\ell}(S,T) = -1 \quad &\Leftrightarrow \quad \dim(S \cap T) \geqslant d, \\ \mathrm{SUM}_d^{\mathbb{F},n,m,\ell}(S,T) = -1 \quad &\Leftrightarrow \quad \dim(S + T) \leqslant d. \end{aligned}$$

Their partial counterparts $\mathrm{INTERSECT}_{d_1,d_2}^{\mathbb{F},n,m,\ell}$ and $\mathrm{SUM}_{d_1,d_2}^{\mathbb{F},n,m,\ell}$, for any pair of distinct integers d_1, d_2, are defined on $\mathscr{S}(\mathbb{F}^n, m) \times \mathscr{S}(\mathbb{F}^n, \ell)$ by

$$\mathrm{INTERSECT}_{d_1,d_2}^{\mathbb{F},n,m,\ell}(S,T) = \begin{cases} -1 & \text{if } \dim(S \cap T) = d_1, \\ 1 & \text{if } \dim(S \cap T) = d_2, \\ * & \text{otherwise,} \end{cases}$$

$$\mathrm{SUM}_{d_1,d_2}^{\mathbb{F},n,m,\ell}(S,T) = \begin{cases} -1 & \text{if } \dim(S + T) = d_1, \\ 1 & \text{if } \dim(S + T) = d_2, \\ * & \text{otherwise.} \end{cases}$$

These partial functions are well-defined for any d_1, d_2 with $d_1 \neq d_2$. Their communication complexity, however, is zero unless both d_1 and d_2 have meaningful values for the problem in question. Specifically, one must have $d_1, d_2 \in [\max\{m, \ell\}, \min\{m + \ell, n\}]$ for the subspace sum problem and $d_1, d_2 \in [\max\{0, m+\ell-n\}, \min\{m, \ell\}]$ for the subspace intersection problem. We record this simple fact as a proposition below.

PROPOSITION 2.25. *Let $\mathbb{F}$ be a field. Let n, m, ℓ be nonnegative integers with $\max\{m,\ell\} \leqslant n$. Then:*

(i) *there exist $S \in \mathscr{S}(\mathbb{F}^n, m)$ and $T \in \mathscr{S}(\mathbb{F}^n, \ell)$ with $\dim(S+T) = d$ if and only if d is an integer with $\max\{m,\ell\} \leqslant d \leqslant \min\{m+\ell, n\}$;*

(ii) *there exist $S \in \mathscr{S}(\mathbb{F}^n, m)$ and $T \in \mathscr{S}(\mathbb{F}^n, \ell)$ with $\dim(S \cap T) = d$ if and only if d is an integer with $\max\{0, m+\ell-n\} \leqslant d \leqslant \min\{m,\ell\}$.*

Proof. (i) For any subspaces $S, T \subseteq \mathbb{F}^n$, we have the trivial bounds $\max\{\dim(S), \dim(T)\} \leqslant \dim(S+T) \leqslant \min\{\dim(S) + \dim(T), n\}$. This proves the "only if" part of (i). For the converse, let d be any integer with $\max\{m,\ell\} \leqslant d \leqslant \min\{m+\ell, n\}$. Then the sets $A = \{1, 2, \ldots, m\}$ and $B = \{d-\ell+1, \ldots, d-1, d\}$ satisfy $A, B \subseteq \{1, 2, \ldots, n\}$ (because $\ell \leqslant d \leqslant n$) and $A \cup B = \{1, 2, \ldots, d\}$ (because $m \leqslant d \leqslant m+\ell$). As a result, $\operatorname{span}\{e_1, e_2, \ldots, e_m\}$ and $\operatorname{span}\{e_{d-\ell+1}, \ldots, e_{d-1}, e_d\}$ are a pair of subspaces in $\mathbb{F}^n$ of dimension m and ℓ, respectively, whose sum has dimension d.

(ii) Recall that $\dim(S \cap T) = \dim(S) + \dim(T) - \dim(S+T)$ for any subspaces S, T. As a result,

$$\begin{aligned}
&\{\dim(S \cap T) : S \in \mathscr{S}(\mathbb{F}^n, m), T \in \mathscr{S}(\mathbb{F}^n, \ell)\} \\
&\qquad = \{m + \ell - \dim(S+T) : S \in \mathscr{S}(\mathbb{F}^n, m), T \in \mathscr{S}(\mathbb{F}^n, \ell)\} \\
&\qquad = \{m + \ell - d : d \in \mathbb{Z} \text{ with } \max\{m,\ell\} \leqslant d \leqslant \min\{m+\ell, n\}\} \\
&\qquad = \{\max\{0, m+\ell-n\}, \ldots, \min\{m,\ell\} - 1, \min\{m,\ell\}\},
\end{aligned}$$

where the second step uses (i). □

Let $F\colon X \times Y \to \{-1, 1, *\}$ and $F'\colon X' \times Y' \to \{-1, 1, *\}$ be (possibly partial) communication problems. A *communication-free reduction from F to F'* is a pair of mappings $\alpha\colon X \to X'$ and $\beta\colon Y \to Y'$ such that $F(x,y) = F'(\alpha(x), \beta(y))$ for all $(x,y) \in \operatorname{dom} F$. We indicate the existence of a communication-free reduction from F to F' by writing $F' \succeq F$. In this case, it is clear that the communication complexity of F' in any given model is bounded from below by the communication complexity of F in the same model.

PROPOSITION 2.26. *Let n, m, ℓ, r, R be integers with $0 \leqslant r < R \leqslant \min\{m,\ell\}$ and $\max\{m,\ell\} \leqslant n$. Then*

$$\mathrm{INTERSECT}_{r,R}^{\mathbb{F},n,m,\ell} \succeq \mathrm{INTERSECT}_{0,R-r}^{\mathbb{F},n-r,m-r,\ell-r}.$$

Proof. Consider the injective linear map $\varphi\colon \mathbb{F}^{n-r} \to \mathbb{F}^n$ that takes any vector and extends it with r zero components to obtain a vector in $\mathbb{F}^n$. Given arbitrary subspaces $S, T \subseteq \mathbb{F}^{n-r}$ of dimension $m-r$ and $\ell-r$, respectively, define $S' = \operatorname{span}(\varphi(S) \cup \{e_{n-r+1}, \ldots, e_{n-1}, e_n\})$ and $T' = \operatorname{span}(\varphi(T) \cup \{e_{n-r+1}, \ldots, e_{n-1}, e_n\})$. Then clearly

$$\begin{aligned}
\dim(S' \cap T') &= \dim(S') + \dim(T') - \dim(S'+T') \\
&= \dim(S) + r + \dim(T) + r - \dim(S+T) - r \\
&= \dim(S) + \dim(T) - \dim(S+T) + r \\
&= \dim(S \cap T) + r,
\end{aligned}$$

whence the reduction $\mathrm{INTERSECT}_{0,R-r}^{\mathbb{F},n-r,m-r,\ell-r}(S,T) = \mathrm{INTERSECT}_{r,R}^{\mathbb{F},n,m,\ell}(S',T')$. □

3. The matrix rank problem

In this section, we prove a tight lower bound on the randomized and quantum communication complexity of the rank problem. As discussed in the introduction, we obtain this lower bound by constructing a dual matrix Φ with certain properties, namely, low spectral norm, low ℓ_1 norm, and high correlation with the characteristic matrix of the rank problem. We start in Section 3.1 by analyzing the probabilities P_n that arise in the recurrence relation for the Γ_n function. The latter plays an important role in our proof and is studied in Section 3.2. Section 3.3 constructs a univariate

dual object φ defined on $\{0, 1, \ldots, n\}$ and studies its analytic and metric properties. We build on φ to construct a dual matrix E_φ in Section 3.4, and discuss how the properties of φ give rise to analogous properties of E_φ. Sections 3.5 and 3.6 establish lower bounds for the approximate trace norm of the characteristic matrix and the communication complexity of the rank problem, with $\Phi = E_\varphi$ used as the dual witness. We prove a matching communication upper bound in Section 3.7. Section 3.8 concludes our study of the rank problem with an application to streaming complexity.

Throughout this section, the underlying field is $\mathbb{F}_q$ for an arbitrary prime power q. The root of unity ω and the notation ω^x for $x \in \mathbb{F}_q$ are as defined in Section 2.4.

3.1. The P_n function. The P_n function, defined next, conveys useful information about random nonsingular matrices of order n over a given field.

DEFINITION 3.1. Let $n \geqslant 1$ be a given integer. For nonnegative integers $s, t, r \in \{0, 1, \ldots, n\}$, define $P_n(s, t, r)$ to be the probability that the upper-left $s \times t$ quadrant of a uniformly random nonsingular matrix in $\mathbb{F}_q^{n \times n}$ has rank r:

$$P_n(s, t, r) = \mathop{\mathbf{P}}_{X \in \mathscr{M}_n} [\operatorname{rk}(I_s X I_t) = r]. \tag{3.1}$$

To derive a closed-form expression for P_n, we essentially need to count the number of ways to complete a given $s \times t$ matrix of rank r to a nonsingular matrix of order n. We break this counting task into two steps, where the first step is to count the number of completions of an $s \times t$ matrix of rank r to an $s \times n$ matrix of rank s.

LEMMA 3.2. *Let s, t, r, m be nonnegative integers with $r \leqslant \min\{s, t\}$. Let $A \in \mathscr{M}_r^{s,t}$ be given. Then the number of matrices $B \in \mathbb{F}_q^{s \times m}$ for which $\operatorname{rk} \begin{bmatrix} A & B \end{bmatrix} = s$ is*

$$q^{rm} \, |\mathscr{M}_{s-r}^{s-r,m}|.$$

Proof. If $r = 0$, then $\operatorname{rk} \begin{bmatrix} A & B \end{bmatrix} = \operatorname{rk} B$. As a result, $\operatorname{rk} \begin{bmatrix} A & B \end{bmatrix} = s$ if and only if $B \in \mathscr{M}_s^{s,m}$. Therefore, the lemma holds in this case. In what follows, we consider $r \geqslant 1$, which forces s and t to be positive integers.

Define the matrices A' and A'' to be the top r rows of A and the bottom $s - r$ rows of A, respectively. We first consider the possibility when A'' is zero or empty. Here, the column span of A' is necessarily all of $\mathbb{F}_q^r$. Given an $s \times m$ matrix B, partition it into B' and B'' conformably with the partition of A. Then

$$\operatorname{rk} \begin{bmatrix} A & B \end{bmatrix} = \operatorname{rk} \begin{bmatrix} A' & B' \\ 0 & B'' \end{bmatrix} = \operatorname{rk} \begin{bmatrix} A' & 0 \\ 0 & B'' \end{bmatrix} = \operatorname{rk}(A') + \operatorname{rk}(B'') = r + \operatorname{rk}(B'').$$

Thus, $\begin{bmatrix} A & B \end{bmatrix}$ has rank s if and only if $\operatorname{rk}(B'') = s - r$. This means that there are $|\mathscr{M}_{s-r}^{s-r,m}|$ ways to choose B'', and independently q^{rm} ways to choose B', such that $\operatorname{rk} \begin{bmatrix} A & B \end{bmatrix} = s$.

It remains to examine the case of a general matrix A of rank $r \geqslant 1$. Let V be an invertible matrix such that the bottom $s - r$ rows of VA are zero. Let $\mathscr{M}$ be the set of $s \times m$ matrices M for which $\operatorname{rk} \begin{bmatrix} VA & M \end{bmatrix} = s$. Then $\operatorname{rk} \begin{bmatrix} A & B \end{bmatrix} = s$ if and only if $VB \in \mathscr{M}$. In particular, the number of matrices B for which $\operatorname{rk} \begin{bmatrix} A & B \end{bmatrix} = s$ is $|\mathscr{M}|$. Since $|\mathscr{M}| = q^{rm} \, |\mathscr{M}_{s-r}^{s-r,m}|$ by the previous paragraph, we are done. ∎

We now derive an exact expression for P_n and establish its relevant algebraic and analytic properties.

LEMMA 3.3. *Let $n \geqslant 1$ be a given integer. Then for all $s, t, r \in \{0, 1, \ldots, n\}$:*

(i) $P_n(s, t, r) = 0$ if $r > \min\{s, t\}$ or $r < s + t - n$;
(ii) $P_n(s, t, r) = q^{r(n-t)} |\mathscr{M}_r^{s,t}| \, |\mathscr{M}_{s-r}^{s-r,n-t}| / ((q^n - 1)(q^n - q) \cdots (q^n - q^{s-1}))$;

(iii) for any fixed values of n, s, r, the quantity $P_n(s,t,r)$ as a function of $t \in \{0,1,\ldots,n\}$ is a polynomial in q^{-t} of degree at most s;
(iv) $P_n(s,t,r) \leqslant 16q^{-(s-r)(t-r)}$.

Proof. (i) Since the quadrant of interest is an $s \times t$ matrix, the first inequality is trivial. For the second inequality, observe that the matrix $I_s X I_t$ in the defining equation (3.1) satisfies $\operatorname{rk}(I_s X I_t) \geqslant \operatorname{rk} I_s + \operatorname{rk}(X I_t) - n = s + t - n$ by Fact 2.1.

(ii) If $r > \min\{s,t\}$, then the left-hand side and right-hand side of (ii) both vanish due to (i) and the definition of $\mathscr{M}_r^{s,t}$. We now treat the case $r \leqslant \min\{s,t\}$. Letting $\mathscr{M}$ stand for the set of nonsingular matrices of order n whose upper-left $s \times t$ quadrant has rank r, we have

$$P_n(s,t,r) = \frac{|\mathscr{M}|}{|\mathscr{M}_n|}. \tag{3.2}$$

A matrix in $\mathscr{M}$ can be chosen by the following three-step process: choose a matrix in $\mathscr{M}_r^{s,t}$ for the upper-left quadrant; extend the quadrant to a matrix in $\mathscr{M}_s^{s,n}$, which by Lemma 3.2 can be done in $q^{r(n-t)}\,|\mathscr{M}_{s-r}^{s-r,n-t}|$ ways; and finally add $n-s$ rows to obtain an invertible matrix, which can be done in $(q^n - q^s)(q^n - q^{s+1}) \cdots (q^n - q^{n-1})$ ways. Altogether, we obtain

$$|\mathscr{M}| = |\mathscr{M}_r^{s,t}| \cdot q^{r(n-t)}\,|\mathscr{M}_{s-r}^{s-r,n-t}| \cdot (q^n - q^s)(q^n - q^{s+1}) \cdots (q^n - q^{n-1}),$$

whereas Proposition 2.17 gives

$$|\mathscr{M}_n| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

Making these substitutions in (3.2) completes the proof.

(iii) We claim that for all $s,t,r \in \{0,1,\ldots,n\}$,

$$\begin{aligned} P_n(s,t,r) = q^{r(n-t)} \binom{s}{r}_q (q^t - 1)(q^t - q) \cdots (q^t - q^{r-1}) \\ \times \frac{(q^{n-t} - 1)(q^{n-t} - q) \cdots (q^{n-t} - q^{s-r-1})}{(q^n - 1)(q^n - q) \cdots (q^n - q^{s-1})}. \end{aligned} \tag{3.3}$$

Indeed, in the case when $r > \min\{s,t\}$ or $r < s+t-n$, the right-hand side vanishes and therefore the equality holds due to (i). In the complementary case, Proposition 2.17 gives closed-form expressions for $|\mathscr{M}_r^{s,t}|$ and $|\mathscr{M}_{s-r}^{s-r,n-t}|$ which, when substituted in (ii), result in (3.3). This settles (3.3) for all $s,t,r \in \{0,1,\ldots,n\}$.

Rewrite (3.3) to obtain

$$\begin{aligned} P_n(s,t,r) = q^{rn} \binom{s}{r}_q (1 - q^{-t})(1 - q^{-t+1}) \cdots (1 - q^{-t+r-1}) \\ \times \frac{(q^{n-t} - 1)(q^{n-t} - q) \cdots (q^{n-t} - q^{s-r-1})}{(q^n - 1)(q^n - q) \cdots (q^n - q^{s-1})}. \end{aligned} \tag{3.4}$$

Now, fix n, s, r arbitrarily. If $r \leqslant s$, then (3.4) makes it clear that $P_n(s,t,r)$ is a polynomial in q^{-t} of degree at most $r + (s-r) = s$. If $r > s$, then $P_n(s,t,r)$ is identically zero and thus trivially a polynomial in q^{-t} of degree at most s.

(iv) For $r > s$, we have $P_n(s,t,r) = 0$ by (i) and therefore the claimed upper bound holds trivially. In the complementary case, simplify (3.3) to obtain

$$\begin{aligned} P_n(s,t,r) &\leqslant q^{r(n-t)} \binom{s}{r}_q q^{tr} \cdot \frac{q^{(n-t)(s-r)}}{(q^n-1)(q^n-q)\cdots(q^n-q^{s-1})} \\ &\leqslant q^{r(n-t)} \binom{s}{r}_q q^{tr} \cdot 4q^{(n-t)(s-r)} q^{-ns} \\ &\leqslant q^{r(n-t)} \cdot 4q^{r(s-r)} q^{tr} \cdot 4q^{(n-t)(s-r)} q^{-ns} \\ &= 16q^{-(s-r)(t-r)}, \end{aligned}$$

where the second and third steps apply Proposition 2.13 and Corollary 2.14, respectively. ∎

3.2. The Γ_n function. A basic building block in our construction is the characteristic function of matrices in $\mathbb{F}_q^{n\times n}$ of a given rank. Its Fourier spectrum is best understood in terms of what we call the Γ_n function.

Definition 3.4. Let $n \geqslant 1$ be a given integer. For $s,t \in \{0,1,\ldots,n\}$, define

$$\Gamma_n(s,t) = \mathop{\mathbf{E}}_{\substack{\operatorname{rk} A = s \\ \operatorname{rk} B = t}} \omega^{\langle A,B\rangle},$$

where the expectation is taken with respect to the uniform distribution on $\mathscr{M}_s^{n,n} \times \mathscr{M}_t^{n,n}$.

Sun and Wang [27] studied the Fourier spectrum of the nonsingularity function on $\mathbb{F}_q^{n\times n}$, defined to be 1 on nonsingular matrices and 0 otherwise. In our notation, they established the following result.

Lemma 3.5. *For any integers $n \geqslant 1$ and $r \in \{0,1,\ldots,n\}$,*

$$\Gamma_n(n,r) = \frac{(-1)^r q^{\binom{r}{2}}}{(q^n-1)(q^n-q)\cdots(q^n-q^{r-1})}.$$

The proof of Sun and Wang [27] is stated for fields $\mathbb{F}_p$ with prime p, but their analysis readily extends to fields of cardinality a prime power. In Appendix A, we prove Lemma 3.5 from scratch in our desired generality, using a simpler proof than that of [27].

Our next lemma collects crucial properties of $\Gamma_n(s,t)$ for general values of s,t.

Lemma 3.6. *Let $n \geqslant 1$ be a given integer. Then for all $s,t \in \{0,1,\ldots,n\}$:*

(i) $|\Gamma_n(s,t)| \leqslant 1$;
(ii) $\Gamma_n(s,t) = \Gamma_n(t,s)$;
(iii) $\Gamma_n(s,t) = \sum_{r=0}^{n} P_n(s,t,r)\Gamma_n(n,r)$;
(iv) for n,s fixed, $\Gamma_n(s,t)$ as a function of $t \in \{0,1,\ldots,n\}$ is a polynomial in q^{-t} of degree at most s;
(v) $|\Gamma_n(s,t)| \leqslant 128q^{-st/2}$.

Proof. (i) Using $|\omega| = 1$ and the triangle inequality,

$$|\Gamma_n(s,t)| = \left| \mathop{\mathbf{E}}_{A,B} \omega^{\langle A,B\rangle} \right| \leqslant \mathop{\mathbf{E}}_{A,B} \left| \omega^{\langle A,B\rangle} \right| = 1.$$

(ii) The symmetry of Γ_n follows from the independence of A and B in the defining equation for Γ_n, and the symmetry of the inner product over $\mathbb{F}_q$.

(iii) We have:

$$\begin{aligned}
\Gamma_n(s,t) &= \mathop{\mathbf{E}}_{\substack{A\in\mathscr{M}_s^{n,n}\\ B\in\mathscr{M}_t^{n,n}}} \omega^{\langle A,B\rangle} \\
&= \mathop{\mathbf{E}}_{X,Y,Z_1,Z_2,W\in\mathscr{M}_n} \omega^{\langle XI_sY,Z_1Z_2I_tW\rangle} \\
&= \mathop{\mathbf{E}}_{X,Y,Z_1,Z_2,W\in\mathscr{M}_n} \omega^{\langle XI_sYW^{\mathsf{T}}I_tZ_2^{\mathsf{T}},Z_1\rangle} \\
&= \mathop{\mathbf{E}}_{X,U,Z_1,Z_2\in\mathscr{M}_n} \omega^{\langle X(I_sUI_t)Z_2^{\mathsf{T}},Z_1\rangle} \\
&= \sum_{r=0}^{n} \mathop{\mathbf{P}}_{U\in\mathscr{M}_n}[\operatorname{rk}(I_sUI_t)=r] \mathop{\mathbf{E}}_{X,U,Z_1,Z_2\in\mathscr{M}_n} \left[\omega^{\langle X(I_sUI_t)Z_2^{\mathsf{T}},Z_1\rangle} \;\middle|\; \operatorname{rk}(I_sUI_t)=r\right] \\
&= \sum_{r=0}^{n} \mathop{\mathbf{P}}_{U\in\mathscr{M}_n}[\operatorname{rk}(I_sUI_t)=r] \mathop{\mathbf{E}}_{\substack{B\in\mathscr{M}_r^{n,n}\\ Z_1\in\mathscr{M}_n}} \omega^{\langle B,Z_1\rangle} \\
&= \sum_{r=0}^{n} P_n(s,t,r)\Gamma_n(n,r),
\end{aligned}$$

where the first step restates the definition of Γ_n, the second step uses Proposition 2.19, the third step applies Fact 2.2(ii), the fourth and sixth steps again use Proposition 2.19, and the last step is immediate from the definitions of P_n and Γ_n.

(iv) Immediate from (iii) and Lemma 3.3(iii).

(v) We have:

$$\begin{aligned}
|\Gamma_n(s,t)| &= \left|\sum_{r=0}^{n} P_n(s,t,r)\Gamma_n(n,r)\right| \\
&\leqslant \sum_{r=0}^{n} P_n(s,t,r)|\Gamma_n(n,r)| \\
&= \sum_{r=\max\{0,s+t-n\}}^{n} P_n(s,t,r)\,|\Gamma_n(n,r)| \\
&\leqslant \sum_{r=\max\{0,s+t-n\}}^{n} 16q^{-(s-r)(t-r)} \cdot \frac{q^{\binom{r}{2}}}{(q^n-1)(q^n-q)\cdots(q^n-q^{r-1})} \\
&\leqslant \sum_{r=\max\{0,s+t-n\}}^{n} 64q^{-(s-r)(t-r)+\binom{r}{2}-nr} \\
&\leqslant 128q^{-st/2},
\end{aligned}$$

where the first step appeals to (iii), the third step is valid by Lemma 3.3(i), the fourth step uses Lemma 3.3(iv) and Lemma 3.5, the fifth step applies Proposition 2.13, and the last step which completes the proof is justified by the following claim. □

Claim 3.7. *For any integers $n \geqslant 1$ and $s,t \in \{0,1,\ldots,n\}$,*

$$\sum_{r=\max\{0,s+t-n\}}^{\infty} q^{-(s-r)(t-r)+\binom{r}{2}-nr} \leqslant 2q^{-st/2}. \tag{3.5}$$

Proof. The exponent of q on the left-hand side of (3.5) is given by the function

$$A(r) = -(s-r)(t-r) + \binom{r}{2} - nr \tag{3.6}$$

$$= -st - \frac{1}{2}\left(r + n - s - t + \frac{1}{2}\right)^2 + \frac{1}{2}\left(n - s - t + \frac{1}{2}\right)^2. \tag{3.7}$$

The first equality shows that $A(r)$ is always an integer, whereas the second shows that $A(r)$ is a strictly decreasing function in the variable $r \in [\max\{0, s+t-n\}, \infty)$. These two facts lead to

$$A(\max\{0, s+t-n\} + i) \leqslant A(\max\{0, s+t-n\}) - i, \qquad i = 0, 1, 2, \ldots. \tag{3.8}$$

We will now prove that

$$A(\max\{0, s+t-n\}) \leqslant -\frac{st}{2}. \tag{3.9}$$

There are two cases to consider. If $s + t \leqslant n$, then $A(\max\{0, s+t-n\}) = A(0) = -st$ and therefore (3.9) holds. The complementary case $s + t \geqslant n + 1$ is more challenging. Here, we have

$$A(\max\{0, s+t-n\}) = A(s+t-n) \leqslant -st + \frac{1}{2}\left(n - s - t + \frac{1}{2}\right)^2,$$

where the second step uses (3.7). Thus, the proof of (3.9) will be complete once we show that

$$\left(n - s - t + \frac{1}{2}\right)^2 - st \leqslant 0. \tag{3.10}$$

To prove (3.10), suppose that of all pairs $(s, t) \in \{0, 1, \ldots, n\}^2$ with $s + t \geqslant n + 1$, the left-hand side of (3.10) is maximized at a pair (s^*, t^*). By symmetry, we may assume that $s^* \leqslant t^*$. If we had $t^* \leqslant n - 1$, then it would follow that $s^* \geqslant 2$ (due to the requirement that $s^* + t^* \geqslant n + 1$); as a result, the left-hand side of (3.10) would be larger for the pair $(s, t) = (s^* - 1, t^* + 1)$ than it is for the pair $(s, t) = (s^*, t^*)$, an impossibility. Therefore, $t^* = n$. In addition, we have $s^* \geqslant 1$ (due to the requirement that $s^* + t^* \geqslant n + 1$). Evaluating the right-hand side of (3.10) at this pair $(s^*, t^*) = (s^*, n)$, we obtain $(s^* - \frac{1}{2})^2 - s^* n$, which is clearly negative due to $s^* \in \{1, 2, \ldots, n\}$. This completes the proof of (3.10) and therefore that of (3.9).

Now,

$$\begin{aligned}
\sum_{r=\max\{0,s+t-n\}}^{\infty} q^{-(s-r)(t-r)+\binom{r}{2}-nr} &= \sum_{r=\max\{0,s+t-n\}}^{\infty} q^{A(r)} \\
&= \sum_{i=0}^{\infty} q^{A(\max\{0,s+t-n\}+i)} \\
&\leqslant q^{A(\max\{0,s+t-n\})} \sum_{i=0}^{\infty} q^{-i} \\
&\leqslant q^{-st/2} \cdot \frac{q}{q-1},
\end{aligned}$$

where the first step uses the definition of $A(r)$, the third step applies (3.8), and the final step appeals to (3.9) and a geometric series. Since $q \geqslant 2$, this completes the proof of (3.5). □

3.3. Univariate dual object. Our construction of the univariate dual object is based on the Cauchy binomial theorem along with a certain "correcting" polynomial ζ. The next lemma presents ζ as parametrized by two numbers ℓ and m and gives its basic properties.

LEMMA 3.8. *Let n, k, ℓ, m be nonnegative integers such that $\ell + m \leqslant k < n$. Define a univariate polynomial ζ by*

$$\zeta(t) = \prod_{i=0}^{\ell-1} \frac{t - q^{-i}}{q^{-n} - q^{-i}} \cdot \prod_{i=k-m}^{k-1} \frac{t - q^{-i}}{q^{-n} - q^{-i}} \cdot \prod_{i=k+1}^{n-1} \frac{t - q^{-i}}{q^{-n} - q^{-i}}. \tag{3.11}$$

Then:

(i) $\zeta(q^{-n}) = 1$;
(ii) $\operatorname{sgn} \zeta(q^{-k}) = (-1)^{n-k-1}$;
(iii) $\zeta(q^{-r}) = 0$ for $r \in \{0, 1, \ldots, n\} \setminus (\{\ell, \ell+1, \ldots, k-m-1\} \cup \{k, n\})$;
(iv) $\deg \zeta = n + \ell + m - k - 1$;
(v) $|\zeta(q^{-r})| \leqslant 4q^{-r(n-k+m-1)+\binom{n}{2}-k-\binom{k-m}{2}}$ for $r \in \{\ell, \ell+1, \ldots, k-m-1\}$.

Proof. Items (i), (iii), and (iv) are immediate from the defining equation for ζ. Item (ii) holds because for $t = q^{-k}$, the first and second products in (3.11) contain only positive factors, whereas the third product contains exactly $n - k - 1$ factors all of which are negative. For (v),

$$\begin{aligned}
|\zeta(q^{-r})| &= \left| \prod_{i=0}^{\ell-1} \frac{q^{-r} - q^{-i}}{q^{-n} - q^{-i}} \cdot \prod_{i=k-m}^{k-1} \frac{q^{-r} - q^{-i}}{q^{-n} - q^{-i}} \cdot \prod_{i=k+1}^{n-1} \frac{q^{-r} - q^{-i}}{q^{-n} - q^{-i}} \right| \\
&= \prod_{i=0}^{\ell-1} \frac{1 - q^{i-r}}{1 - q^{-(n-i)}} \cdot \prod_{i=k-m}^{k-1} \frac{q^{i-r} - 1}{1 - q^{-(n-i)}} \cdot \prod_{i=k+1}^{n-1} \frac{q^{i-r} - 1}{1 - q^{-(n-i)}} \\
&\leqslant \prod_{i=0}^{\ell-1} \frac{1}{1 - q^{-(n-i)}} \cdot \prod_{i=k-m}^{k-1} \frac{q^{i-r}}{1 - q^{-(n-i)}} \cdot \prod_{i=k+1}^{n-1} \frac{q^{i-r}}{1 - q^{-(n-i)}}.
\end{aligned}$$

The product of the numerators in the last expression is $q^{-r(n-k+m-1)+\binom{n}{2}-k-\binom{k-m}{2}}$, whereas the product of the denominators is at least $1/4$ by Proposition 2.13. □

With ζ in hand, we are now in a position to construct the promised univariate dual object φ. The properties of φ established in the lemma below will give rise to analogous properties in the dual matrix E_φ.

LEMMA 3.9. *Let n, k, ℓ, m be nonnegative integers such that $\ell + m \leqslant k < n$. Then there is a function $\varphi\colon \{0, 1, \ldots, n\} \to \mathbb{R}$ such that:*

(i) $\varphi(n) = 1$;
(ii) $\varphi(k) < 0$;
(iii) $\varphi(r) = 0$ for $r \in \{0, 1, \ldots, n\} \setminus (\{\ell, \ell+1, \ldots, k-m-1\} \cup \{k, n\})$;
(iv) $\sum_{r=0}^{n} \varphi(r)\xi(q^{-r}) = 0$ for every polynomial ξ of degree at most $k - \ell - m$;
(v) $\sum_{r \in \{0,\ldots,n\} \setminus \{k,n\}} |\varphi(r)| \leqslant 32q^{-m-1}$.

Proof. Define

$$\varphi(r) = \binom{n}{r}_q (-1)^{r-n} q^{\binom{r}{2}-\binom{n}{2}} \zeta(q^{-r}),$$

where ζ is the univariate polynomial from Lemma 3.8. Then items (i)–(iii) are immediate from the corresponding items (i)–(iii) of Lemma 3.8.

For (iv), fix a univariate polynomial ξ of degree at most $k - \ell - m$. In view of Lemma 3.8(iv), the product of ζ and ξ has degree less than n. As a result, the Cauchy binomial theorem (Corollary 2.16)

implies that

$$\sum_{r=0}^{n} \varphi(r)\xi(q^{-r}) = (-1)^{-n} q^{-\binom{n}{2}} \sum_{r=0}^{n} \binom{n}{r}_q (-1)^r q^{\binom{r}{2}} \zeta(q^{-r})\xi(q^{-r}) = 0.$$

For (v), fix any $r \in \{\ell, \ell+1, \dots, k-m-1\}$. Then

$$\begin{aligned} |\varphi(r)| &= \binom{n}{r}_q q^{\binom{r}{2}-\binom{n}{2}} |\zeta(q^{-r})| \\ &\leqslant 4q^{r(n-r)} \cdot q^{\binom{r}{2}-\binom{n}{2}} \cdot 4q^{-r(n-k+m-1)+\binom{n}{2}-k-\binom{k-m}{2}} \\ &= 16q^{-\binom{k-m-r+1}{2}-m}, \end{aligned} \tag{3.12}$$

where in the second step we bound the q-binomial coefficient via Corollary 2.14 and $|\zeta(q^{-r})|$ via Lemma 3.8(v). Now

$$\sum_{r \in \{0,\dots n\} \setminus \{k,n\}} |\varphi(r)| = \sum_{r=\ell}^{k-m-1} |\varphi(r)| \leqslant \sum_{r=\ell}^{k-m-1} 16q^{-\binom{k-m-r+1}{2}-m} \leqslant \sum_{i=2}^{\infty} 16q^{-\binom{i}{2}-m} \leqslant \frac{16q^{-m-1}}{1-\frac{1}{q}},$$

where the first step is valid by (iii), the second step uses (3.12), and the fourth step uses a geometric series along with $\binom{i}{2} \geqslant i-1$ for $i \geqslant 2$. Since $q \geqslant 2$, this completes the proof of (v). ∎

3.4. From univariate dual objects to dual matrices. En route to the main result of this section, we now show how to convert a univariate dual object φ, such as the one constructed in Lemma 3.9, into a dual matrix E_φ.

Definition 3.10. Let $n \geqslant 1$ be a given integer. For $r = 0, 1, \dots, n$, define E_r to be the matrix with rows and columns indexed by matrices in $\mathbb{F}_q^{n\times n}$, and entries given by

$$(E_r)_{A,B} = \begin{cases} q^{-n^2} |\mathscr{M}_r^{n,n}|^{-1} & \text{if } \operatorname{rk}(A+B) = r, \\ 0 & \text{otherwise.} \end{cases}$$

For a function $\varphi\colon \{0, 1, \dots, n\} \to \mathbb{R}$, define

$$E_\varphi = \sum_{r=0}^{n} \varphi(r) E_r.$$

As one would expect, the metric and analytic properties of E_φ are closely related to those of φ.

Lemma 3.11 (Metric properties of E_φ). *Let $n \geqslant 1$ be an integer and $\varphi\colon \{0, 1, \dots, n\} \to \mathbb{R}$ a given function. Then*

$$\sum_{A,B:\operatorname{rk}(A+B)=r} (E_\varphi)_{A,B} = \varphi(r), \qquad r = 0, 1, \dots, n, \tag{3.13}$$

$$\sum_{A,B:\operatorname{rk}(A+B)=r} |(E_\varphi)_{A,B}| = |\varphi(r)|, \qquad r = 0, 1, \dots, n. \tag{3.14}$$

In particular,

$$\|E_\varphi\|_1 = \|\varphi\|_1.$$

Proof. Recall that for any fixed matrix $A \in \mathbb{F}_q^{n\times n}$, the mapping $B \mapsto A + B$ is a permutation on $\mathbb{F}_q^{n\times n}$. As a result, for any fixed matrix A, there are exactly $|\mathscr{M}_r^{n,n}|$ matrices B such that $\operatorname{rk}(A+B) = r$. Altogether, there are $q^{n^2}|\mathscr{M}_r^{n,n}|$ matrix pairs (A, B) with $\operatorname{rk}(A+B) = r$. With this

in mind, Definition 3.10 implies the following for each r:

$$\sum_{\operatorname{rk}(A+B)=r} (E_r)_{A,B} = \sum_{\operatorname{rk}(A+B)=r} |(E_r)_{A,B}| = 1. \tag{3.15}$$

Now for each r,

$$\sum_{\operatorname{rk}(A+B)=r} (E_\varphi)_{A,B} = \sum_{\operatorname{rk}(A+B)=r} \sum_{i=0}^{n} \varphi(i)(E_i)_{A,B} = \sum_{\operatorname{rk}(A+B)=r} \varphi(r)(E_r)_{A,B} = \varphi(r),$$

where the second step uses $(E_i)_{A,B} = 0$ for $i \neq r$, and the final step applies (3.15). Analogously,

$$\sum_{\operatorname{rk}(A+B)=r} |(E_\varphi)_{A,B}| = \sum_{\operatorname{rk}(A+B)=r} \left| \sum_{i=0}^{n} \varphi(i)(E_i)_{A,B} \right| = \sum_{\operatorname{rk}(A+B)=r} |\varphi(r)|\,|(E_r)_{A,B}| = |\varphi(r)|.$$

This establishes (3.13) and (3.14). Summing (3.14) over r gives $\|E_\varphi\|_1 = \|\varphi\|_1$. □

To discuss the spectrum of E_φ, we first describe the Fourier spectrum of the characteristic function of matrices of a given rank. This is where the significance of the Γ_n function becomes evident.

Lemma 3.12. *Let $n \geqslant 1$ be a given integer. For $r \in \{0, 1, \ldots, n\}$, define $f_r \colon \mathbb{F}_q^{n\times n} \to \{0, 1\}$ by $f_r(X) = 1$ if and only if $\operatorname{rk} X = r$. Then for all $M \in \mathbb{F}_q^{n\times n}$,*

$$\widehat{f_r}(M) = \frac{|\mathscr{M}_r^{n,n}|}{q^{n^2}} \cdot \Gamma_n(\operatorname{rk} M, r).$$

Proof. We have

$$\begin{aligned}
\widehat{f_r}(M) &= \mathop{\mathbf{E}}_{X\in\mathbb{F}_q^{n\times n}} \omega^{-\langle M,X\rangle} f_r(X) \\
&= q^{-n^2} \sum_{X\in\mathscr{M}_r^{n,n}} \omega^{-\langle M,X\rangle} \\
&= q^{-n^2} |\mathscr{M}_r^{n,n}| \mathop{\mathbf{E}}_{X\in\mathscr{M}_r^{n,n}} \omega^{-\langle M,X\rangle} \\
&= q^{-n^2} |\mathscr{M}_r^{n,n}| \mathop{\mathbf{E}}_{\substack{X\in\mathscr{M}_r^{n,n} \\ U,V\in\mathscr{M}_n}} \omega^{-\langle M,UXV\rangle} \\
&= q^{-n^2} |\mathscr{M}_r^{n,n}| \mathop{\mathbf{E}}_{\substack{X\in\mathscr{M}_r^{n,n} \\ U,V\in\mathscr{M}_n}} \omega^{\langle -U^{\mathsf{T}}MV^{\mathsf{T}},X\rangle} \\
&= q^{-n^2} |\mathscr{M}_r^{n,n}| \mathop{\mathbf{E}}_{\substack{X\in\mathscr{M}_r^{n,n} \\ Y\in\mathscr{M}_{\operatorname{rk} M}^{n,n}}} \omega^{\langle Y,X\rangle} \\
&= q^{-n^2} |\mathscr{M}_r^{n,n}|\, \Gamma_n(\operatorname{rk} M, r),
\end{aligned}$$

where the second step uses the definition of f_r, the fourth step is valid by Proposition 2.19, the fifth step invokes Fact 2.2(ii), the sixth step uses Proposition 2.19 once more, and the last step applies the definition of Γ_n. □

We are now ready to describe the spectrum of E_φ in terms of φ and the Γ_n function.

LEMMA 3.13 (Singular values of E_φ). *Let $n \geqslant 1$ be an integer and $\varphi\colon \{0,1,\dots,n\} \to \mathbb{R}$ a given function. Then the singular values of E_φ are*

$$q^{-n^2}\left|\sum_{t=0}^{n} \varphi(t)\Gamma_n(s,t)\right|, \qquad s = 0,1,\dots,n,$$

with corresponding multiplicities $|\mathscr{M}_s^{n,n}|$ for $s = 0,1,\dots,n$.

Proof. For $t = 0,1,\dots,n$, define f_t as in Lemma 3.12. In this notation,

$$E_\varphi = \sum_{t=0}^{n} \varphi(t) E_t = \sum_{t=0}^{n} \varphi(t) \left[\frac{1}{q^{n^2}|\mathscr{M}_t^{n,n}|} \cdot f_t(A+B)\right]_{A,B} = [f(A+B)]_{A,B},$$

where

$$f = \sum_{t=0}^{n} \frac{\varphi(t)}{q^{n^2}|\mathscr{M}_t^{n,n}|} \cdot f_t.$$

By Fact 2.10, the singular values of E_φ are $q^{n^2}|\widehat{f}(M)|$ for $M \in \mathbb{F}_q^{n\times n}$. Calculating,

$$\begin{aligned} q^{n^2}|\widehat{f}(M)| &= q^{n^2}\left|\sum_{t=0}^{n} \frac{\varphi(t)}{q^{n^2}|\mathscr{M}_t^{n,n}|} \cdot \widehat{f_t}(M)\right| \\ &= q^{-n^2}\left|\sum_{t=0}^{n} \varphi(t)\Gamma_n(\operatorname{rk} M, t)\right|, \end{aligned}$$

where the first step uses the linearity of the Fourier transform, and the second step applies Lemma 3.12. Grouping these singular values according to $\operatorname{rk} M$ shows that the spectrum of E_φ is as claimed. □

3.5. Approximate trace norm of the rank problem. Using the machinery developed in previous sections, we now prove a lower bound on the approximate trace norm of the characteristic matrix of the rank problem. Combined with the approximate trace norm method, this will allow us to obtain our communication lower bounds for the rank problem.

THEOREM 3.14. *Let $n > k \geqslant 0$ be given integers. Let F be the matrix with rows and columns indexed by elements of $\mathbb{F}_q^{n\times n}$, and entries given by*

$$F_{A,B} = \begin{cases} 1 & \text{if } \operatorname{rk}(A+B) = n, \\ -1 & \text{if } \operatorname{rk}(A+B) = k, \\ * & \text{otherwise.} \end{cases}$$

Then for all reals $\delta \geqslant 0$ and all nonnegative integers ℓ, m with $\ell + m \leqslant k$,

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1}{150}\left(1 - \delta - \frac{64}{q^{m+1}}\right) q^{\ell(k-\ell-m+1)/2}\, q^{n^2}, \tag{3.16}$$

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1-\delta}{150} \cdot q^{k/2}\, q^{n^2}. \tag{3.17}$$

Proof. Let $\varphi\colon \{0,1,\dots,n\} \to \mathbb{R}$ be the function constructed in Lemma 3.9. Then

$$\begin{aligned}
&\sum_{\operatorname{dom} F} F_{A,B}(E_\varphi)_{A,B} - \delta\|E_\varphi\|_1 - \sum_{\overline{\operatorname{dom} F}} |(E_\varphi)_{A,B}| \\
&\qquad = \sum_{\operatorname{rk}(A+B)=n} (E_\varphi)_{A,B} - \sum_{\operatorname{rk}(A+B)=k} (E_\varphi)_{A,B} - \delta\|E_\varphi\|_1 - \sum_{\operatorname{rk}(A+B)\notin\{n,k\}} |(E_\varphi)_{A,B}| \\
&\qquad = \varphi(n) - \varphi(k) - \delta\|\varphi\|_1 - \sum_{r\notin\{n,k\}} |\varphi(r)| \\
&\qquad = |\varphi(n)| + |\varphi(k)| - \delta\|\varphi\|_1 - \sum_{r\notin\{n,k\}} |\varphi(r)| \\
&\qquad = (1-\delta)\|\varphi\|_1 - 2\sum_{r\notin\{n,k\}} |\varphi(r)| \\
&\qquad \geqslant \left(1 - \delta - 2\sum_{r\notin\{n,k\}} |\varphi(r)|\right) \|\varphi\|_1, \qquad (3.18)
\end{aligned}$$

where the second step uses Lemma 3.11, the third step is valid by Lemma 3.9(i)–(ii), and the last step is justified by Lemma 3.9(i).

We now analyze the spectral norm of E_φ. Recall from Lemma 3.6(iv) that for any fixed values of n and s, the quantity $\Gamma_n(s,t)$ as a function of $t \in \{0,1,\dots,n\}$ is a polynomial in q^{-t} of degree at most s. In this light, Lemma 3.9(iv) implies that

$$\max_{s\in\{0,1,\dots,k-\ell-m\}} \left|\sum_{t=0}^{n} \varphi(t)\Gamma_n(s,t)\right| = 0. \qquad (3.19)$$

Continuing,

$$\begin{aligned}
&\max_{s\in\{k-\ell-m+1,\dots,n-1,n\}} \left|\sum_{t=0}^{n} \varphi(t)\Gamma_n(s,t)\right| \\
&\qquad = \max_{s\in\{k-\ell-m+1,\dots,n-1,n\}} \left|\sum_{t=\ell}^{n} \varphi(t)\Gamma_n(s,t)\right| \\
&\qquad \leqslant \max_{s\in\{k-\ell-m+1,\dots,n-1,n\}} \left\{\|\varphi\|_1 \max_{t\in\{\ell,\ell+1,\dots,n\}} |\Gamma_n(s,t)|\right\} \\
&\qquad \leqslant \max_{s\in\{k-\ell-m+1,\dots,n-1,n\}} \left\{\|\varphi\|_1 \max_{t\in\{\ell,\ell+1,\dots,n\}} 128q^{-st/2}\right\} \\
&\qquad = 128\|\varphi\|_1 q^{-\ell(k-\ell-m+1)/2}, \qquad (3.20)
\end{aligned}$$

where the first step uses Lemma 3.9(iii), and the third step applies the bound of Lemma 3.6(v). By (3.19), (3.20), and Lemma 3.13,

$$\|E_\varphi\| \leqslant 128\|\varphi\|_1\, q^{-\ell(k-\ell-m+1)/2}\, q^{-n^2}. \qquad (3.21)$$

Proposition 2.9 with $\Phi = E_\varphi$ implies, in view of (3.18) and (3.21), that

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1}{128} \cdot \left(1 - \delta - 2\sum_{r\notin\{n,k\}} |\varphi(r)|\right) q^{\ell(k-\ell-m+1)/2}\, q^{n^2}. \qquad (3.22)$$

Since $\sum_{r \notin \{n,k\}} |\varphi(r)| \leqslant 32q^{-m-1}$ by Lemma 3.9(v), this settles (3.16). The alternative lower bound (3.17) follows from (3.22) by taking $\ell = k$ and $m = 0$ and noting that $\sum_{r \notin \{n,k\}} |\varphi(r)| = 0$ in this case (by Lemma 3.9(iii)). □

3.6. Communication lower bounds. We will now use our newly obtained lower bound on the approximate trace norm to prove the main result of this section, a tight lower bound on the communication complexity of the rank problem. We will first examine the canonical case of distinguishing rank-k matrices in $\mathbb{F}^{n \times n}$ from full-rank matrices.

THEOREM 3.15. *There is an absolute constant $c > 0$ such that for all finite fields $\mathbb{F}$ and all integers $n > k \geqslant 0$,*

$$Q^*_{\frac{1}{2} - \frac{1}{4|\mathbb{F}|^{k/3}}}(\mathrm{RANK}^{\mathbb{F},n,n}_{k,n}) \geqslant c(1 + k^2 \log |\mathbb{F}|). \tag{3.23}$$

Proof. Abbreviate $q = |\mathbb{F}|$ and $\varepsilon = \frac{1}{2} - \frac{1}{4q^{k/3}}$. Since $\mathrm{RANK}^{\mathbb{F},n,n}_{k,n}$ is a nonconstant function, we have the trivial lower bound

$$Q^*_\varepsilon(\mathrm{RANK}^{\mathbb{F},n,n}_{k,n}) \geqslant 1. \tag{3.24}$$

Let F be the characteristic matrix of this communication problem. We first examine the case $k \leqslant 50$. Here, taking $\delta = 2\varepsilon$ in equation (3.17) of Theorem 3.14 shows that $\|F\|_{\Sigma,2\varepsilon} \geqslant q^{k/6} q^{n^2}/300 \geqslant q^{k^2/300} q^{n^2}/300$, where the last step uses $k \leqslant 50$. It follows from Theorem 2.23 that

$$Q^*_\varepsilon(\mathrm{RANK}^{\mathbb{F},n,n}_{k,n}) \geqslant \frac{1}{2} \log \frac{q^{k^2/300}}{3 \cdot 300} \geqslant \frac{1}{600}\, k^2 \log q - 5.$$

Taking a weighted arithmetic average of this lower bound and (3.24) settles (3.23).

Consider now the complementary case $k > 50$. Taking $\delta = 2\varepsilon$, $\ell = \lceil k/3 \rceil$, and $m = \lfloor k/2 \rfloor$ in equation (3.16) of Theorem 3.14 gives

$$\begin{aligned}
\|F\|_{\Sigma,2\varepsilon} &\geqslant \frac{1}{150} \left(\frac{1}{2q^{k/3}} - \frac{64}{q^{\lfloor k/2 \rfloor + 1}} \right) q^{\lceil k/3 \rceil (k - \lceil k/3 \rceil - \lfloor k/2 \rfloor + 1)/2} q^{n^2} \\
&\geqslant \frac{1}{300} \left(1 - \frac{128}{q^{k/6}} \right) q^{-k/3} q^{\lceil k/3 \rceil k/12} q^{n^2} \\
&\geqslant \frac{1}{600}\, q^{-k/3} q^{\lceil k/3 \rceil k/12} q^{n^2} \\
&\geqslant \frac{1}{600}\, q^{k^2/48} q^{n^2},
\end{aligned}$$

where the last two steps use $k > 50$. As a result, Theorem 2.23 guarantees that

$$Q^*_\varepsilon(\mathrm{RANK}^{\mathbb{F},n,n}_{k,n}) \geqslant \frac{1}{2} \log \frac{q^{k^2/48}}{3 \cdot 600} \geqslant \frac{1}{96}\, k^2 \log q - 6.$$

Taking a weighted arithmetic average of this lower bound and (3.24) settles (3.23). □

We now establish our main lower bound for the rank problem in its full generality.

THEOREM (restatement of Theorem 1.1). *There is an absolute constant $c > 0$ such that for all finite fields $\mathbb{F}$ and all integers n, m, R, r with $\min\{n, m\} \geqslant R > r \geqslant 0$,*

$$Q^*_{\frac{1}{2} - \frac{1}{4|\mathbb{F}|^{r/3}}}(\mathrm{RANK}^{\mathbb{F},n,m}_{r,R}) \geqslant c(1 + r^2 \log |\mathbb{F}|). \tag{3.25}$$

In particular,

$$Q^*_{1/4}(\mathrm{RANK}^{\mathbb{F},n,m}_{r,R}) \geqslant c(1 + r^2 \log |\mathbb{F}|). \tag{3.26}$$

Proof. There is a communication-free reduction from $\mathrm{RANK}^{\mathbb{F},R,R}_{r,R}$ to $\mathrm{RANK}^{\mathbb{F},n,m}_{r,R}$, where Alice and Bob pad their input matrices $A, B \in \mathbb{F}^{R\times R}$ with zeroes to obtain matrices $A', B' \in \mathbb{F}^{n\times m}$ with $\mathrm{rk}(A+B) = \mathrm{rk}(A'+B')$. Therefore, $Q^*_\varepsilon(\mathrm{RANK}^{\mathbb{F},n,m}_{r,R}) \geqslant Q^*_\varepsilon(\mathrm{RANK}^{\mathbb{F},R,R}_{r,R})$ for all ε. Now Theorem 3.15 implies (3.25), which in turn implies (3.26). ∎

3.7. Communication upper bounds. To finalize our study of the rank problem, we will prove a matching upper bound on its communication complexity. We emphasize that our upper bound is achieved by a randomized (classical) protocol, whereas our lower bound is valid even for quantum communication.

THEOREM 3.16. *Let n, m, R be nonnegative integers with $\min\{n, m\} \geqslant R \geqslant 0$. Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements. Then for all $t \geqslant 2$ and $\varepsilon \in (0, 1)$, there is a t-party randomized communication protocol which:*

- *takes as input matrices $A_1, A_2, \ldots, A_t \in \mathbb{F}^{n\times m}$ for players $1, 2, \ldots, t$, respectively;*
- *computes $\min\{\mathrm{rk}(\sum A_i), R\}$ with probability of error at most ε; and*
- *has communication cost $O(t(R + \lceil \log_q(1/\varepsilon)\rceil)^2 \log q)$.*

Proof. We may assume that $n, m \geqslant 1$ since the theorem is trivial otherwise. The communication protocol is based on random projections and is inspired by Clarkson and Woodruff's streaming algorithm [9] for matrix rank. Set $\Delta = \lceil \log_q(8/\varepsilon)\rceil$ and $A = \sum A_i$. The players use their shared randomness to pick a pair of independent and uniformly random matrices $X \in \mathbb{F}^{(R+\Delta)\times n}$ and $Y \in \mathbb{F}^{m\times(R+\Delta)}$. Then each player i sends the matrix $XA_iY \in \mathbb{F}^{(R+\Delta)\times(R+\Delta)}$, and they all output $\min\{\mathrm{rk}(XAY), R\}$. The communication cost is $O(t(R+\Delta)^2 \log q)$ as claimed, due to $XAY = \sum XA_iY$. It is also clear that this protocol always outputs a *lower* bound on the correct value $\min\{\mathrm{rk}\, A, R\}$, due to $\mathrm{rk}(XAY) \leqslant \mathrm{rk}\, A$ for all X, Y. It remains to show that

$$\mathbf{P}[\mathrm{rk}(XAY) \geqslant \min\{\mathrm{rk}\, A, R\}] \geqslant 1 - \varepsilon. \tag{3.27}$$

Conditioned on X, we have $\mathrm{rk}(XAY) \geqslant \min\{\mathrm{rk}(XA), R\}$ with probability at least $1 - 4q^{-\Delta-1} \geqslant 1 - \varepsilon/2$ (apply Lemma 2.21(ii) with $M = XA$ and $t = \min\{\mathrm{rk}(XA), R\} - 1$). Similarly, $\mathrm{rk}(XA) \geqslant \min\{\mathrm{rk}\, A, R\}$ with probability at least $1 - \varepsilon/2$ (apply Lemma 2.21(i) with $M = A$ and $t = \min\{\mathrm{rk}\, A, R\} - 1$). The union bound now gives (3.27). ∎

In the corollary below, $\mathrm{RANK}^{\mathbb{F},n,m,t}_r \colon (\mathbb{F}^{n\times m})^t \to \{-1, 1\}$ denotes the total version of the matrix rank problem for t parties, given by $\mathrm{RANK}^{\mathbb{F},n,m,t}_r(A_1, A_2, \ldots, A_t) = -1$ if and only if $\mathrm{rk}(\sum A_i) \leqslant r$.

COROLLARY 3.17. *Let n, m, r be integers with $\min\{n, m\} > r \geqslant 0$. Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements. Then for all $\varepsilon \in (0, 1/2)$,*

$$R_\varepsilon(\mathrm{RANK}^{\mathbb{F},n,m}_r) = \begin{cases} O(\log(1/\varepsilon)) & \text{if } r = 0, \\ O((r + \lceil \log_q(1/\varepsilon)\rceil)^2 \log q) & \text{otherwise.} \end{cases} \tag{3.28}$$

More generally, for all $t \geqslant 2$,

$$R_\varepsilon(\mathrm{RANK}^{\mathbb{F},n,m,t}_r) = O(t(r + \lceil \log_q(1/\varepsilon)\rceil)^2 \log q). \tag{3.29}$$

Proof. We have $\mathrm{RANK}^{\mathbb{F},n,m,t}_r(A_1, A_2, \ldots, A_t) = -1$ if and only if $\min\{\mathrm{rk}(\sum A_i), r+1\} \leqslant r$. To compute this minimum with error ε, one can use the t-party protocol of Theorem 3.16 with $R = r+1$, with communication cost $O(t(r + \lceil \log_q(1/\varepsilon)\rceil)^2 \log q)$. This settles the multiparty bound (3.29), which in turn implies the two-party bound (3.28) for $r \geqslant 1$.

Lastly, $\mathrm{RANK}^{\mathbb{F},n,m}_0(A, B) = -1$ if and only if $A = -B$. Thus, $\mathrm{RANK}^{\mathbb{F},n,m}_0$ is equivalent to the equality problem with domain $\mathbb{F}^{n\times m} \times \mathbb{F}^{n\times m}$. It is well known [14] that the ε-error randomized communication complexity of equality is $O(\log(1/\varepsilon))$. Therefore, (3.28) holds also for $r = 0$. ∎

Our communication upper bound readily generalizes to the bilinear query model, as follows.

THEOREM 3.18. *Let n, m, r be integers with $\min\{n, m\} > r \geqslant 0$. Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements. Then for all $\varepsilon \in (0, 1/2)$, there is a query algorithm in the bilinear query model with cost $O((r + \lceil \log_q(1/\varepsilon) \rceil)^2)$ that takes as input a matrix $A \in \mathbb{F}^{n \times m}$ and determines whether $\operatorname{rk} A \leqslant r$ with probability of error at most ε.*

Proof. On input $A \in \mathbb{F}^{n \times m}$, choose $X \in \mathbb{F}^{(R+\Delta) \times n}$ and $Y \in \mathbb{F}^{m \times (R+\Delta)}$ uniformly at random, where $\Delta = \lceil \log_q(8/\varepsilon) \rceil$ and $R = r + 1$. Then trivially $\operatorname{rk}(XAY) \leqslant \operatorname{rk} A$. In the opposite direction, we have the bound (3.27), established in the last paragraph of the proof of Theorem 3.16. Therefore, we can determine whether $\operatorname{rk} A \leqslant r$ with probability of error ε by checking whether $\operatorname{rk}(XAY) \leqslant r$. Since the entries of XAY are bilinear forms in A, the entire matrix XAY can be recovered using $(R + \Delta)^2$ queries. ∎

We now prove an alternative communication upper bound, showing that even a two-bit protocol can solve the rank problem with nontrivial advantage. For simplicity, we will only consider the two-party model; a similar statement can be proved for bilinear query complexity.

THEOREM 3.19. *Let n, m, r be integers with $\min\{n, m\} > r \geqslant 0$. Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements. Then*

$$R_{\frac{1}{2} - \frac{1}{32q^r}}(\mathrm{RANK}_r^{\mathbb{F},n,m}) \leqslant 2. \tag{3.30}$$

Proof. Consider the following auxiliary protocol Π. On input $A, B \in \mathbb{F}^{n \times m}$, Alice and Bob use their shared randomness to pick a pair of independent and uniformly random vectors $x \in \mathbb{F}^n$ and $y \in \mathbb{F}^m$, as well as a uniformly random function $H \colon \mathbb{F} \to \{-1, 1\}$. They exchange $H(x^{\mathsf{T}}Ay)$ and $H(-x^{\mathsf{T}}By)$ using 2 bits of communication and output $-H(x^{\mathsf{T}}Ay)H(-x^{\mathsf{T}}By)$.

We now analyze the expected output of $\Pi(A, B)$ on a given matrix pair A, B. To begin with,

$$\mathbf{E}[\Pi(A, B) \mid x, y] = \begin{cases} -1 & \text{if } x^{\mathsf{T}}(A + B)y = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{3.31}$$

Indeed, if $x^{\mathsf{T}}(A + B)y = 0$ then $x^{\mathsf{T}}Ay = -x^{\mathsf{T}}By$ and therefore Π outputs -1. If, on the other hand, $x^{\mathsf{T}}(A + B)y \neq 0$ then $x^{\mathsf{T}}Ay \neq -x^{\mathsf{T}}By$, which means that $H(x^{\mathsf{T}}Ay)$ and $H(-x^{\mathsf{T}}By)$ are independent and their product has expected value 0. Equation (3.31) implies that $\mathbf{E}\,\Pi(A, B) = -\mathbf{P}[x^{\mathsf{T}}(A + B)y = 0]$, which can be expanded as

$$\mathbf{E}\,\Pi(A, B) = -\mathbf{P}[x^{\mathsf{T}}(A+B) = 0] - \mathbf{P}[x^{\mathsf{T}}(A+B) \neq 0]\,\mathbf{P}[x^{\mathsf{T}}(A+B)y = 0 \mid x^{\mathsf{T}}(A+B) \neq 0].$$

The event $x^{\mathsf{T}}(A+B) = 0$ is equivalent to x being in the orthogonal complement of the column span of $A+B$, which happens with probability $q^{n-\operatorname{rk}(A+B)}/q^n = q^{-\operatorname{rk}(A+B)}$. Conditioned on $x^{\mathsf{T}}(A+B) \neq 0$, the field element $x^{\mathsf{T}}(A + B)y$ is uniformly random and in particular is 0 with probability $1/q$. As a result,

$$\mathbf{E}\,\Pi(A, B) = -\frac{1}{q^{\operatorname{rk}(A+B)}} - \left(1 - \frac{1}{q^{\operatorname{rk}(A+B)}}\right) \cdot \frac{1}{q} = -\frac{1}{q} - \frac{q-1}{q^{\operatorname{rk}(A+B)+1}}.$$

Therefore, the expected value of $\Pi(A, B)$ is at most $-1/q - (q-1)/q^{r+1}$ when $\operatorname{rk}(A + B) \leqslant r$ and is at least $-1/q - (q-1)/q^{r+2}$ when $\operatorname{rk}(A + B) > r$. Proposition 2.24 now shows that $\mathrm{RANK}_r^{\mathbb{F},n,m}$ has a communication protocol with the same cost as Π and error at most $\frac{1}{2} - \frac{1}{8}(q-1)^2/q^{r+2}$. This settles (3.30) since $q \geqslant 2$. ∎

Corollary 3.17 (with $\varepsilon = 1/3$) and Theorem 3.19 settle Theorem 1.2 from the introduction.

3.8. Streaming complexity. Fix a finite field $\mathbb{F}$ and a (possibly partial) function $f\colon \mathbb{F}^{n\times n} \to \{-1,1,*\}$. A streaming algorithm for f receives as input a matrix $M \in \mathbb{F}^{n\times n}$ in row-major order. We say that $\mathscr{A}$ *computes* f *with error* ε if for every input in the domain of f, the output of $\mathscr{A}$ agrees with f with probability at least $1-\varepsilon$. We will now use a well-known reduction [16] to transform our communication lower bound for the matrix rank problem into a lower bound on its streaming complexity.

THEOREM (restatement of Theorem 1.3). *Let n, r, R be nonnegative integers with $n/2 \leqslant r < R \leqslant n$, and let $\mathbb{F}$ be a finite field. Define $f\colon \mathbb{F}^{n\times n} \to \{-1,1,*\}$ by*

$$f(M) = \begin{cases} -1 & \text{if } \operatorname{rk} M = r, \\ 1 & \text{if } \operatorname{rk} M = R, \\ * & \text{otherwise.} \end{cases}$$

Let $\mathscr{A}$ be any randomized streaming algorithm for f with error probability $\frac{1}{2} - \frac{1}{4}|\mathbb{F}|^{-(r-\lceil n/2\rceil)/3}$ that uses k passes and space s. Then

$$sk = \Omega\left(\left(r - \left\lceil \frac{n}{2} \right\rceil\right)^2 \log|\mathbb{F}|\right). \tag{3.32}$$

Proof. Abbreviate $m = \lfloor n/2 \rfloor$ and $F = \mathrm{RANK}^{\mathbb{F},m,m}_{r-\lceil n/2\rceil, R-\lceil n/2\rceil}$. We will use a reduction from communication to streaming due to Li, Sun, Wang, and Woodruff [16, Thm. 29]. Specifically, let $A, B \in \mathbb{F}^{m\times m}$ be Alice and Bob's inputs, respectively, for F. Define

$$M = \begin{bmatrix} A & -I_m & 0 \\ B & I_m & 0 \\ 0 & 0 & I_{n-2m} \end{bmatrix},$$

where I_m and I_{n-2m} stand for the identity matrices of order m and $n-2m$, respectively (in particular, I_{n-2m} is empty for even n). We have

$$\operatorname{rk} M = \operatorname{rk} \begin{bmatrix} A+B & 0 & 0 \\ B & I_m & 0 \\ 0 & 0 & I_{n-2m} \end{bmatrix} = \operatorname{rk}(A+B) + n - m = \operatorname{rk}(A+B) + \left\lceil \frac{n}{2} \right\rceil.$$

As a result, for all matrix pairs (A,B) with $\operatorname{rk}(A+B) \in \{r-\lceil n/2\rceil, R-\lceil n/2\rceil\}$, we have $F(A,B) = f(M)$. This makes it possible for Alice and Bob to compute F by simulating $\mathscr{A}$ on M. Alice starts the simulation by running $\mathscr{A}$ on the first m rows of M, which depend only on her input A. She then sends Bob the contents of $\mathscr{A}$'s memory, and Bob runs $\mathscr{A}$ on the remaining $n-m$ rows of M. This completes the first pass. Next, Bob sends Alice the contents of $\mathscr{A}$'s memory, and they continue as before until they simulate all k passes. At the end of the k-th pass, Bob announces the output of $\mathscr{A}$ as the protocol output. The error probability of the described protocol is the same as that of $\mathscr{A}$, and the communication cost is $s(2k-1)+1$ bits. Therefore,

$$R_{\frac{1}{2}-\frac{1}{4}|\mathbb{F}|^{-(r-\lceil n/2\rceil)/3}}(F) \leqslant s(2k-1)+1.$$

Since the left-hand side is at least $\Omega((r-\lceil n/2\rceil)^2 \log|\mathbb{F}| + 1)$ by Theorem 1.1, the claimed trade-off (3.32) follows. ∎

4. The determinant problem

In this section, we establish our lower bound on the communication complexity of the determinant problem. We begin in Section 4.1 with technical results on characteristic functions of matrices with a given determinant value. In Section 4.2, we give our own proof of the lower bound for distinguishing two nonzero values of the determinant, which is simpler and more elementary than the proof in [27].

In Section 4.3, we prove an optimal lower bound for the general case of distinguishing two arbitrary values of the determinant, solving an open problem from [27]. Throughout this section, we use a generic finite field $\mathbb{F}$ with q elements, where q is an arbitrary prime power. The root of unity ω and the notation ω^x for $x \in \mathbb{F}$ are as defined in Section 2.4.

4.1. Auxiliary results. Fix a finite field $\mathbb{F}$ and a positive integer n. Recall that the determinant function on $\mathbb{F}^{n\times n}$ is multiplicative, with $\det(AB) = \det(A)\det(B)$. As a result, the set of matrices in $\mathbb{F}^{n\times n}$ with nonzero determinants form a group under matrix multiplication, called the *general linear group* and denoted by $\mathrm{GL}(\mathbb{F}, n)$. Analogously, the matrices in $\mathbb{F}^{n\times n}$ with determinant 1 also form a group, called the *special linear group* and denoted by $\mathrm{SL}(\mathbb{F}, n)$. The multiplicativity of the determinant further implies that $\mathrm{SL}(\mathbb{F}, n)$ is a normal subgroup of $\mathrm{GL}(\mathbb{F}, n)$, with quotient isomorphic to the multiplicative group of the field: $\mathrm{GL}(\mathbb{F}, n)/\mathrm{SL}(\mathbb{F}, n) \cong \mathbb{F}^\times$. For any given field element $u \neq 0$, the set of matrices with determinant u form a coset of $\mathrm{SL}(\mathbb{F}, n)$ in $\mathrm{GL}(\mathbb{F}, n)$. In particular,

$$|\{X \in \mathbb{F}^{n\times n} : \det X = u\}| = |\mathrm{SL}(\mathbb{F}, n)| = \frac{|\mathscr{M}_n|}{|\mathbb{F}| - 1}, \qquad u \in \mathbb{F} \setminus \{0\}. \tag{4.1}$$

Recall that for each $Y \in \mathbb{F}^{n\times n}$, the mapping $X \mapsto X + Y$ is a permutation on $\mathbb{F}^{n\times n}$. As a result, the previous equation implies that

$$|\{(X, Y) \in \mathbb{F}^{n\times n} \times \mathbb{F}^{n\times n} : \det(X + Y) = u\}| = |\mathbb{F}|^{n^2}|\mathrm{SL}(\mathbb{F}, n)|, \qquad u \in \mathbb{F} \setminus \{0\}. \tag{4.2}$$

To understand the spectral norm of the characteristic matrix of the determinant problem, we now introduce a relevant function on $\mathbb{F}^{n\times n}$ and discuss its Fourier coefficients.

LEMMA 4.1. *Let n be a positive integer, $\mathbb{F}$ a finite field. For a pair of distinct elements $u, v \in \mathbb{F}\setminus\{0\}$, define $g_{u,v} \colon \mathbb{F}^{n\times n} \to \{-1, 1, 0\}$ by*

$$g_{u,v}(X) = \begin{cases} -1 & \text{if } \det X = u, \\ 1 & \text{if } \det X = v, \\ 0 & \text{otherwise.} \end{cases}$$

Then:

(i) $\widehat{g_{u,v}}(A) = 0$ *for every singular matrix* A;
(ii) $\widehat{g_{u,v}}(A) = \widehat{g_{u,v}}(B)$ *whenever* $\det A = \det B$;
(iii) $\|\widehat{g_{u,v}}\|_\infty \leqslant 1/\sqrt{|\mathrm{SL}(\mathbb{F}, n)|}$.

Proof. (i) In view of (4.1), we have

$$\begin{aligned} \widehat{g_{u,v}}(A) &= \mathop{\mathbf{E}}_{X\in\mathbb{F}^{n\times n}} g_{u,v}(X)\omega^{-\langle A,X\rangle} \\ &= |\mathbb{F}|^{-n^2} \cdot \frac{|\mathscr{M}_n|}{|\mathbb{F}| - 1} \left(\mathop{\mathbf{E}}_{X:\det X=v} \omega^{-\langle A,X\rangle} - \mathop{\mathbf{E}}_{X:\det X=u} \omega^{-\langle A,X\rangle} \right). \end{aligned}$$

It remains to show that the expectations in the last expression are equal. Since A is singular, there exist nonsingular matrices P and Q such that $A = PI_sQ$ for $s = \operatorname{rk} A < n$. Consider the order-$n$ diagonal matrix $Z = \mathrm{diag}(1, 1, \ldots, 1, u^{-1}v)$. Using $I_s = I_sZ$, we obtain $A = PI_sZQ = PI_sQQ^{-1}ZQ = AQ^{-1}ZQ$. As a result,

$$\begin{aligned} \mathop{\mathbf{E}}_{X:\det X=u} \omega^{-\langle A,X\rangle} &= \mathop{\mathbf{E}}_{X:\det X=u} \omega^{-\langle AQ^{-1}ZQ,X\rangle} \\ &= \mathop{\mathbf{E}}_{X:\det X=u} \omega^{-\langle A,X(Q^{-1}ZQ)^{\mathsf{T}}\rangle} \\ &= \mathop{\mathbf{E}}_{Y:\det Y=v} \omega^{-\langle A,Y\rangle}, \end{aligned}$$

where the second step uses Fact 2.2(ii), and the last step is valid because the mapping $X \mapsto X(Q^{-1}ZQ)^{\mathsf{T}}$ is a bijection from the set of matrices with determinant u onto the set of matrices with determinant $u \cdot \det((Q^{-1}ZQ)^{\mathsf{T}}) = v$.

(ii) For singular A and B, the claim is immediate from (i). In the complementary case,

$$\begin{aligned}
\widehat{g_{u,v}}(A) &= \mathop{\mathbf{E}}_{X \in \mathbb{F}^{n\times n}} g_{u,v}(X)\omega^{-\langle A,X\rangle} \\
&= \mathop{\mathbf{E}}_{X \in \mathbb{F}^{n\times n}} g_{u,v}((BA^{-1})^{\mathsf{T}}X)\omega^{-\langle A,(BA^{-1})^{\mathsf{T}}X\rangle} \\
&= \mathop{\mathbf{E}}_{X \in \mathbb{F}^{n\times n}} g_{u,v}(X)\omega^{-\langle A,(BA^{-1})^{\mathsf{T}}X\rangle} \\
&= \mathop{\mathbf{E}}_{X \in \mathbb{F}^{n\times n}} g_{u,v}(X)\omega^{-\langle B,X\rangle} \\
&= \widehat{g_{u,v}}(B),
\end{aligned}$$

where the second step is valid because $(BA^{-1})^{\mathsf{T}}$ is invertible and hence $X \mapsto (BA^{-1})^{\mathsf{T}}X$ is a permutation on $\mathbb{F}^{n\times n}$; the third step is justified by $\det((BA^{-1})^{\mathsf{T}}X) = \det(B)\det(X)/\det(A) = \det X$; and the fourth step is an application of Fact 2.2(ii).

(iii) Let M be a matrix with $|\widehat{g_{u,v}}(M)| = \|\widehat{g_{u,v}}\|_\infty$. By (i), we know that $\det M \neq 0$. Now

$$\begin{aligned}
1 &\geqslant \mathop{\mathbf{E}}_{X \in \mathbb{F}^{n\times n}} [|g_{u,v}(X)|^2] \\
&= \sum_{A \in \mathbb{F}^{n\times n}} |\widehat{g_{u,v}}(A)|^2 \\
&\geqslant \sum_{A : \det A = \det M} |\widehat{g_{u,v}}(A)|^2 \\
&= |\{A : \det A = \det M\}|\, |\widehat{g_{u,v}}(M)|^2 \\
&= |\mathrm{SL}(\mathbb{F},n)|\, \|\widehat{g_{u,v}}\|_\infty^2,
\end{aligned}$$

where the second step applies Parseval's inequality (2.19), the fourth step is justified by (ii), and the fifth step uses $\det M \neq 0$ along with (4.1). □

4.2. Determinant problem for nonzero field elements. As an application of the previous lemma, we now prove that the characteristic matrix of the determinant problem $\mathrm{DET}_{a,b}^{\mathbb{F},n}$ for any two nonzero field elements a, b has small spectral norm.

LEMMA 4.2. *Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements. For each $u \in \mathbb{F} \setminus \{0\}$, define G_u to be the matrix with rows and columns indexed by elements of $\mathbb{F}^{n\times n}$, and entries given by*

$$(G_u)_{X,Y} = \begin{cases} q^{-n^2}|\mathrm{SL}(\mathbb{F},n)|^{-1} & \text{if } \det(X+Y) = u, \\ 0 & \text{otherwise.} \end{cases} \tag{4.3}$$

Then

$$\|G_u\|_1 = 1, \qquad u \in \mathbb{F} \setminus \{0\}, \tag{4.4}$$

$$\|G_v - G_u\| \leqslant |\mathrm{SL}(\mathbb{F},n)|^{-3/2} \leqslant 8q^{-3(n^2-1)/2}, \qquad u, v \in \mathbb{F} \setminus \{0\}. \tag{4.5}$$

Proof. Equation (4.4) follows from (4.2). For (4.5), there are two cases to consider. If $u = v$, then $G_v - G_u = 0$ and thus $\|G_v - G_u\| = 0$. If $u \neq v$, write $G_v - G_u = [q^{-n^2}|\mathrm{SL}(\mathbb{F},n)|^{-1} g_{u,v}(X+Y)]_{X,Y}$ with $g_{u,v}$ as defined in Lemma 4.1. Then

$$\|G_v - G_u\| = \frac{\|\widehat{g_{u,v}}\|_\infty}{|\mathrm{SL}(\mathbb{F},n)|} \leqslant \frac{1}{|\mathrm{SL}(\mathbb{F},n)|^{3/2}}, \tag{4.6}$$

where the first step applies Fact 2.10, and the second step uses Lemma 4.1(iii). It remains to simplify the bound of (4.6):

$$\frac{1}{|\mathrm{SL}(\mathbb{F},n)|^{3/2}} = \left(\frac{|\mathscr{M}_n|}{q-1}\right)^{-3/2} = \left(q^{n-1}\prod_{i=0}^{n-2}(q^n-q^i)\right)^{-3/2} \leqslant 8q^{-3(n^2-1)/2},$$

where the first step uses (4.1), the second step applies Proposition 2.17, and the last step is justified by Proposition 2.13. □

Lemma 4.2 was originally obtained by Sun and Wang [27] using a different and rather technical proof. By contrast, the proof presented above is short and uses only basic Fourier analysis. With this newly obtained bound on the spectral norm of the characteristic matrix of $\mathrm{DET}_{a,b}^{\mathbb{F},n}$ for nonzero a, b, we can use the approximate trace norm method to obtain a tight communication lower bound for this special case of the determinant problem.

THEOREM 4.3. *Let $\mathbb{F}$ be a finite field, and n a positive integer. Then for every pair of distinct elements $a, b \in \mathbb{F} \setminus \{0\}$ and every $\gamma \in (0,1)$,*

$$Q^*_{(1-\gamma)/2}(\mathrm{DET}_{a,b}^{\mathbb{F},n}) \geqslant \frac{1}{4}(n^2-3)\log|\mathbb{F}| - \frac{1}{2}\log\frac{12}{\gamma}. \tag{4.7}$$

Proof. Let F be the characteristic matrix of $\mathrm{DET}_{a,b}^{\mathbb{F},n}$. For $u \in \mathbb{F}\setminus\{0\}$, define G_u as in Lemma 4.2. Since G_a and G_b are supported on disjoint sets of entries, (4.4) leads to

$$\|G_b - G_a\|_1 = \|G_b\|_1 + \|G_a\|_1 = 2. \tag{4.8}$$

Taking $\Phi = G_b - G_a$ in Proposition 2.9, we obtain

$$\begin{aligned}
\|F\|_{\Sigma,1-\gamma} &\geqslant \frac{1}{\|G_b-G_a\|}\left(\sum_{\mathrm{dom}\,F} F_{A,B}(G_b-G_a)_{A,B} - (1-\gamma)\|G_b-G_a\|_1 - \sum_{\overline{\mathrm{dom}\,F}}|(G_b-G_a)_{A,B}|\right)\\
&= \frac{1}{\|G_b-G_a\|}\left(\sum_{\mathrm{dom}\,F}|(G_b-G_a)_{A,B}| - (1-\gamma)\|G_b-G_a\|_1\right)\\
&= \frac{\gamma\|G_b-G_a\|_1}{\|G_b-G_a\|}\\
&\geqslant \frac{1}{4}\,\gamma|\mathbb{F}|^{3(n^2-1)/2},
\end{aligned} \tag{4.9}$$

where the second and third steps are valid because $G_b - G_a$ by definition coincides in sign with F on $\mathrm{dom}\,F$ and vanishes on $\overline{\mathrm{dom}\,F}$; and the last step uses (4.5) and (4.8). Now (4.7) follows from (4.9) in view of Theorem 2.23. □

We remind the reader that Theorem 4.3 was obtained with different techniques by Sun and Wang [27], who settled the determinant problem $\mathrm{DET}_{a,b}^{\mathbb{F},n}$ for nonzero a, b and left open the complementary case when one of a, b is zero.

4.3. Determinant problem for arbitrary field elements. Recall that the *rank versus determinant problem,* $\mathrm{RANKDET}_{k,a}^{\mathbb{F},n}$, is a hybrid problem that naturally generalizes the matrix rank problem $\mathrm{RANK}_{k,n}^{\mathbb{F},n,n}$ and the determinant problem $\mathrm{DET}_{0,a}^{\mathbb{F},n}$. Specifically, the rank versus determinant problem requires Alice and Bob to distinguish matrix pairs with $\mathrm{rk}(A+B) = k$ from those with $\det(A+B) = a$, where a is a nonzero field element, k is an integer with $k < n$, and A, B are Alice and Bob's respective inputs. We will now construct a dual matrix for $\mathrm{RANKDET}_{k,a}^{\mathbb{F},n}$ and

thereby obtain a lower bound on its approximate trace norm. As a dual matrix, we will use a linear combination of the dual matrices from our analyses of the rank and determinant problems.

THEOREM 4.4. *Let $n > k \geqslant 1$ be given integers. Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements, and let $a \in \mathbb{F} \setminus \{0\}$. Let F be the characteristic matrix of $\mathrm{RANKDET}_{k,a}^{\mathbb{F},n}$. Then for all reals $\delta \geqslant 0$ and all nonnegative integers ℓ, m with $\ell + m \leqslant k$,*

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1}{150}\left(1 - \delta - \frac{64}{q^{m+1}}\right) q^{\ell(k-\ell-m+1)/2}\, q^{n^2}, \tag{4.10}$$

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1-\delta}{150} \cdot q^{k/2}\, q^{n^2}. \tag{4.11}$$

Proof. This proof combines our ideas in Theorems 3.14 and 4.3, and our dual matrix here will be a linear combination of the dual matrices used in those theorems.

Fix nonnegative integers ℓ, m with $\ell + m \leqslant k$, and let $\varphi\colon \{0, 1, \ldots, n\} \to \mathbb{R}$ be the corresponding function constructed in Lemma 3.9. This univariate function gives rise to a matrix E_φ, described in Definition 3.10. To restate equation (3.21) from our proof of Theorem 3.14,

$$\|E_\varphi\| \leqslant 128\|\varphi\|_1\, q^{-\ell(k-\ell-m+1)/2}\, q^{-n^2}. \tag{4.12}$$

For $u \in \mathbb{F} \setminus \{0\}$, define G_u as in Lemma 4.2. As our dual matrix, we will use

$$\Phi = E_\varphi + \sum_{b \in \mathbb{F}\setminus\{0,a\}} \frac{\varphi(n)}{q-1}\,(G_a - G_b). \tag{4.13}$$

CLAIM 4.5. *For every matrix pair (A, B),*

$$\Phi_{A,B} = \begin{cases} (E_\varphi)_{A,B} & \text{if } \det(A+B) = 0, \\ \varphi(n) q^{-n^2} |\mathrm{SL}(\mathbb{F}, n)|^{-1} & \text{if } \det(A+B) = a, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $\det(A + B) = 0$, then by definition $(G_u)_{A,B} = 0$ for every nonzero field element u. As a result, (4.13) gives $\Phi_{A,B} = (E_\varphi)_{A,B}$ in this case.

In what follows, we treat the complementary case when $\det(A + B) \neq 0$. For all such matrix pairs,

$$(E_\varphi)_{A,B} = \sum_{i=0}^{n} \varphi(i)(E_i)_{A,B} = \varphi(n)(E_n)_{A,B} = \frac{\varphi(n)}{q^{n^2}|\mathscr{M}_n|} = \frac{\varphi(n)}{q^{n^2}(q-1)|\mathrm{SL}(\mathbb{F}, n)|},$$

where the first three steps are immediate from Definition 3.10, and the last step uses (4.1). In particular,

$$\Phi_{A,B} = \frac{\varphi(n)}{q^{n^2}(q-1)|\mathrm{SL}(\mathbb{F}, n)|} + \sum_{b \in \mathbb{F}\setminus\{0,a\}} \frac{\varphi(n)}{q-1}\,((G_a)_{A,B} - (G_b)_{A,B}). \tag{4.14}$$

If $\det(A + B) = a$, then by definition $(G_a)_{A,B} = q^{-n^2}|\mathrm{SL}(\mathbb{F}, n)|^{-1}$ and $(G_b)_{A,B} = 0$ for all $b \in \mathbb{F} \setminus \{0, a\}$, so that (4.14) gives

$$\Phi_{A,B} = \frac{\varphi(n)}{q^{n^2}(q-1)|\mathrm{SL}(\mathbb{F}, n)|} + \sum_{b \in \mathbb{F}\setminus\{0,a\}} \frac{\varphi(n)}{(q-1)q^{n^2}|\mathrm{SL}(\mathbb{F}, n)|} = \frac{\varphi(n)}{q^{n^2}|\mathrm{SL}(\mathbb{F}, n)|}.$$

If, on the other hand, $\det(A+B) = c$ for some $c \in \mathbb{F} \setminus \{0, a\}$, then by definition $(G_a)_{A,B} = 0$ and likewise $(G_b)_{A,B} = 0$ for every $b \neq c$, so that (4.14) simplifies to

$$\Phi_{A,B} = \frac{\varphi(n)}{q^{n^2}(q-1)|\mathrm{SL}(\mathbb{F}, n)|} - \frac{\varphi(n)}{(q-1)}(G_c)_{A,B} = 0. \qquad \square$$

We proceed to establish key analytic and metric properties of Φ. To begin with,

$$\begin{aligned}
\|\Phi\| &\leqslant \|E_\varphi\| + \sum_{b \in \mathbb{F}\setminus\{0,a\}} \frac{|\varphi(n)|}{q-1} \|G_a - G_b\| \\
&\leqslant \|E_\varphi\| + \sum_{b \in \mathbb{F}\setminus\{0,a\}} \frac{\|\varphi\|_1}{q-1} \|G_a - G_b\| \\
&\leqslant 128\|\varphi\|_1 \, q^{-\ell(k-\ell-m+1)/2} \, q^{-n^2} + \sum_{b \in \mathbb{F}\setminus\{0,a\}} \frac{\|\varphi\|_1}{q-1} \cdot 8q^{-3(n^2-1)/2} \\
&\leqslant (128q^{-\ell(k-\ell-m+1)/2} + 8q^{-(n^2-3)/2})q^{-n^2}\|\varphi\|_1, \qquad (4.15)
\end{aligned}$$

where the first step uses the triangle inequality, and the third step is a substitution from (4.12) and equation (4.5) of Lemma 4.2. To simplify this bound, recall from the theorem hypothesis that $n > k \geqslant 1$ and $\ell, m \geqslant 0$. Therefore, $\ell(k-\ell-m+1) \leqslant \ell(k-\ell+1) \leqslant (k+1)^2/4 \leqslant n^2/4 \leqslant n^2 - 3$. This results in $q^{-(n^2-3)/2} \leqslant q^{-\ell(k-\ell-m+1)/2}$, and thus (4.15) simplifies to

$$\|\Phi\| \leqslant 136q^{-\ell(k-\ell-m+1)/2}q^{-n^2}\|\varphi\|_1. \qquad (4.16)$$

Next, we examine $\|\Phi\|_1$. We have

$$\sum_{\mathrm{rk}(A+B)=n} |\Phi_{A,B}| = \sum_{\det(A+B)=a} |\Phi_{A,B}| = \sum_{\det(A+B)=a} \frac{|\varphi(n)|}{q^{n^2}|\mathrm{SL}(\mathbb{F}, n)|} = |\varphi(n)|,$$

where the first and second steps are immediate from Claim 4.5, and the last step applies (4.2). Also,

$$\sum_{\mathrm{rk}(A+B)<n} |\Phi_{A,B}| = \sum_{\mathrm{rk}(A+B)<n} |(E_\varphi)_{A,B}| = \|E_\varphi\| - \sum_{\mathrm{rk}(A+B)=n} |(E_\varphi)_{A,B}| = \|\varphi\|_1 - |\varphi(n)|,$$

where the first step uses Claim 4.5, and the last step invokes Lemma 3.11. These two equations yield

$$\|\Phi\|_1 = \|\varphi\|_1. \qquad (4.17)$$

Continuing,

$$\begin{aligned}
\sum_{\mathrm{dom}\, F} F_{A,B}\Phi_{A,B} &= \sum_{\det(A+B)=a} \Phi_{A,B} - \sum_{\mathrm{rk}(A+B)=k} \Phi_{A,B} \\
&= \sum_{\det(A+B)=a} \frac{\varphi(n)}{q^{n^2}|\mathrm{SL}(\mathbb{F}, n)|} - \sum_{\mathrm{rk}(A+B)=k} (E_\varphi)_{A,B} \\
&= \varphi(n) - \varphi(k) \\
&= |\varphi(n)| + |\varphi(k)| \\
&= \|\varphi\|_1 - \sum_{r \notin \{k,n\}} |\varphi(r)|, \qquad (4.18)
\end{aligned}$$

where the second step uses Claim 4.5, the third step invokes Lemma 3.11 and (4.2), and the fourth step is valid due to Lemma 3.9(i), (ii). Finally,

$$\begin{aligned}\sum_{\overline{\operatorname{dom} F}} |\Phi_{A,B}| &= \sum_{\operatorname{rk}(A+B)\notin\{n,k\}} |\Phi_{A,B}| + \sum_{\substack{\operatorname{rk}(A+B)=n\\ \det(A+B)\neq a}} |\Phi_{A,B}| \\ &= \sum_{\operatorname{rk}(A+B)\notin\{n,k\}} |\Phi_{A,B}| \\ &= \sum_{\operatorname{rk}(A+B)\notin\{n,k\}} |(E_\varphi)_{A,B}| \\ &= \sum_{r\notin\{n,k\}} |\varphi(r)|, \end{aligned} \tag{4.19}$$

where the second and third steps use Claim 4.5, and the last step uses Lemma 3.11. Now

$$\begin{aligned}&\sum_{\operatorname{dom} F} F_{A,B}\Phi_{A,B} - \delta\|\Phi\|_1 - \sum_{\overline{\operatorname{dom} F}} |\Phi_{A,B}| \\ &\qquad = \|\varphi\|_1 - \delta\|\varphi\|_1 - 2\sum_{r\notin\{n,k\}} |\varphi(r)| \\ &\qquad \geqslant \left(1 - \delta - 2\sum_{r\notin\{n,k\}} |\varphi(r)|\right)\|\varphi\|_1, \end{aligned} \tag{4.20}$$

where the first step uses (4.17)–(4.19), and the last step is legitimate by Lemma 3.9(i).

Proposition 2.9 implies, in view of (4.16) and (4.20), that

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1}{136}\left(1 - \delta - 2\sum_{r\notin\{n,k\}} |\varphi(r)|\right) q^{\ell(k-\ell-m+1)/2}\, q^{n^2}. \tag{4.21}$$

Since $\sum_{r\notin\{n,k\}} |\varphi(r)| \leqslant 32q^{-m-1}$ by Lemma 3.9(v), this proves (4.10). The alternative lower bound (4.11) follows by taking $\ell = k$ and $m = 0$ in (4.21) and noting that $\sum_{r\notin\{n,k\}} |\varphi(r)| = 0$ in this case (by Lemma 3.9(iii)). □

By virtue of the approximate trace norm method, Theorem 4.4 yields the following tight lower bound on the communication complexity of the rank versus determinant problem.

THEOREM (restatement of Theorem 1.7). *There is an absolute constant $c > 0$ such that for every finite field $\mathbb{F}$, every field element $a \in \mathbb{F} \setminus \{0\}$, and all integers $n > k \geqslant 0$,*

$$Q^*_{\frac{1}{2} - \frac{1}{4|\mathbb{F}|^{k/3}}}(\mathrm{RANKDET}^{\mathbb{F},n}_{k,a}) \geqslant c(1 + k^2 \log|\mathbb{F}|). \tag{4.22}$$

Proof. For $k = 0$, the claimed lower bound follows from the fact that $\mathrm{RANKDET}^{\mathbb{F},n}_{0,a}$ is nonconstant and hence has communication complexity at least 1 bit. For $k \geqslant 1$, our lower bounds on the approximate trace norm of $\mathrm{RANKDET}^{\mathbb{F},n}_{k,a}$ are identical to those for $\mathrm{RANK}^{\mathbb{F},n,n}_{k,n}$ (Theorems 4.4 and Theorem 3.14, respectively). Accordingly, the proof here is identical to that of Theorem 3.15, with equations (4.10) and (4.11) of Theorem 4.4 used in place of the corresponding equations (3.16) and (3.17) of Theorem 3.14. □

As a consequence, we obtain an optimal communication lower bound for the unrestricted determinant problem.

THEOREM (restatement of Theorem 1.6). *There is an absolute constant $c > 0$ such that for every finite field $\mathbb{F}$, every pair of distinct elements $a, b \in \mathbb{F}$, and all integers $n \geqslant 2$,*

$$Q^*_{\frac{1}{2}-\frac{1}{4|\mathbb{F}|^{(n-1)/3}}}(\mathrm{DET}^{\mathbb{F},n}_{a,b}) \geqslant cn^2 \log|\mathbb{F}|. \tag{4.23}$$

Proof. If $ab = 0$, then $\mathrm{DET}^{\mathbb{F},n}_{a,b}$ contains as a subproblem either $\mathrm{RANKDET}^{\mathbb{F},n}_{n-1,b}$ (when $a = 0$) or $\neg\mathrm{RANKDET}^{\mathbb{F},n}_{n-1,a}$ (when $b = 0$), and therefore (4.23) follows from Theorem 1.7. If a and b are both nonzero, Theorem 4.3 gives

$$Q^*_{\frac{1}{2}-\frac{1}{4|\mathbb{F}|^{(n-1)/3}}}(\mathrm{DET}^{\mathbb{F},n}_{a,b}) \geqslant c'n^2 \log|\mathbb{F}| - \frac{1}{2}\log 24$$

for a small enough constant $c' > 0$. Taking a weighted average of this lower bound with the trivial lower bound of 1 bit settles (4.23). □

5. The subspace sum and intersection problems

As discussed in the introduction, our analysis of the subspace sum and subspace intersection problems has similarities with the rank problem but also diverges from it in important ways. Instead of additively composed matrices whose rows and columns are indexed by elements of $\mathbb{F}_q^{n\times n}$, we now have matrices with rows and columns indexed by subspaces, and each entry (A, B) depends solely on the dimension of $A \cap B$. While the construction of the univariate dual object is similar to that for the rank problem, its relation to the singular values of the dual matrix is significantly more intricate, and computing the spectral norm of the dual matrix is now a challenge. Our study of the spectral norm is based on ideas due to Knuth [12]. We start in Section 5.1 by formalizing the equivalence of the subspace sum and subspace intersection problems, which allows us to focus on the latter problem from then on. As a first step toward solving the subspace intersection problem, we collect necessary technical results about subspace combinatorics in Section 5.2. In Section 5.3, we give a formal definition of subspace matrices, state several auxiliary results, and compare our analysis of their spectrum to that of Knuth. In Section 5.4, we fully determine the spectrum of subspace matrices. In Sections 5.5–5.7, we use this spectral study along with our techniques developed in Section 3 to prove optimal lower bounds on the communication complexity of the subspace intersection problem. Sections 5.8 and 5.9 conclude with matching communication upper bounds. As in previous sections, we let q denote an arbitrary prime power and adopt $\mathbb{F}_q$ throughout as the underlying field.

5.1. Equivalence of the subspace sum and intersection problems. The equivalence of the subspace sum and subspace intersection problems from the standpoint of communication complexity is a straightforward consequence of the identity (2.1), valid for any linear subspaces S and T in a finite-dimensional vector space. We formalize this equivalence below.

PROPOSITION 5.1. *Let n, m, ℓ be nonnegative integers with $\max\{m, \ell\} \leqslant n$. Then for all integers d, D with $d \neq D$,*

$$\mathrm{SUM}^{\mathbb{F},n,m,\ell}_{d,D} = \mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{m+\ell-d,m+\ell-D}, \tag{5.1}$$

$$\mathrm{SUM}^{\mathbb{F},n,m,\ell}_{d} = \mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{m+\ell-d}. \tag{5.2}$$

Proof. Let $S, T \subseteq \mathbb{F}^n$ be arbitrary subspaces of dimension m and ℓ, respectively. Since $\dim(S+T) = m + \ell - \dim(S \cap T)$, we have

$$\mathrm{SUM}^{\mathbb{F},n,m,\ell}_{d,D}(S, T) = \mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{m+\ell-d,m+\ell-D}(S, T),$$

settling (5.1). Analogously, for any subspaces $S, T \subseteq \mathbb{F}^n$ of dimension m and ℓ, respectively, we have $\dim(S + T) \leqslant d$ if and only if $\dim(S \cap T) \geqslant m + \ell - d$, which implies (5.2). □

We will now prove our main result on the subspace sum problem (stated in the introduction as Theorems 1.8 and 1.9) assuming our corresponding result on subspace intersection (Theorem 1.10). In the rest of this work, we will focus on proving Theorem 1.10.

Proof of Theorems 1.8 *and* 1.9 *assuming Theorem* 1.10. Recall that Theorem 1.8 is a special case of Theorem 1.9, corresponding to $\gamma = 1/3$. Therefore, it suffices to prove Theorem 1.9. Define $r = m + \ell - D$ and $R = m + \ell - d$. Then the hypotheses $\max\{m, \ell\} \leqslant d < D \leqslant \min\{m + \ell, n\}$ and $\gamma \in [\frac{1}{3}q^{-(2d-m-\ell)/5}, \frac{1}{3}]$ of Theorem 1.9 can be equivalently stated as

$$\max\{0, m + \ell - n\} \leqslant r < R \leqslant \min\{m, \ell\}, \tag{5.3}$$

$$\gamma \in [\tfrac{1}{3}q^{-(m+\ell-2R)/5}, \tfrac{1}{3}]. \tag{5.4}$$

Recall from Proposition 5.1 that $\mathrm{SUM}_{d,D}^{\mathbb{F},n,m,\ell}$ is the same function as $\mathrm{INTERSECT}_{R,r}^{\mathbb{F},n,m,\ell}$, which in turn is the negation of $\mathrm{INTERSECT}_{r,R}^{\mathbb{F},n,m,\ell}$. Now the bounds for $\mathrm{SUM}_{d,D}^{\mathbb{F},n,m,\ell}$ claimed in Theorem 1.9 follow from the bounds for $\mathrm{INTERSECT}_{r,R}^{\mathbb{F},n,m,\ell}$ in Theorem 1.10, upon substituting $R = m + \ell - d$. This appeal to Theorem 1.10 is legitimate due to (5.3) and (5.4).

Analogously, $\mathrm{SUM}_{d}^{\mathbb{F},n,m,\ell}$ is the same function as $\mathrm{INTERSECT}_{R}^{\mathbb{F},n,m,\ell}$ (Proposition 5.1), and therefore the bounds claimed for $\mathrm{SUM}_{d}^{\mathbb{F},n,m,\ell}$ in Theorem 1.9 follow from the bounds for $\mathrm{INTERSECT}_{R}^{\mathbb{F},n,m,\ell}$ in Theorem 1.10, upon substituting $R = m + \ell - d$. □

5.2. Counting subspaces satisfying combinatorial constraints. When it comes to counting, one could hope that the transition from subsets to subspaces would be straightforward and amount to replacing binomial coefficients with their Gaussian counterparts. Unfortunately, this is not the case. Many basic results for sets have no analogues in the subspace setting. For example, the well-known inclusion-exclusion formula (2.1) is valid for two subspaces but does not generalize to any larger number. As a consequence, it is in general a subtle task to count the subspaces of a given dimension that satisfy basic combinatorial constraints relative to other given subspaces. We start by counting, for given subspaces A and C, all d-dimensional subspaces that contain C and avoid $A \setminus C$.

Lemma 5.2 (Counting subspaces externally). *Let A and C be linear subspaces of an n-dimensional vector space V over $\mathbb{F}_q$. Let $d \geqslant 0$ be an integer. Then the number of dimension-d linear subspaces X such that $C \subseteq X \subseteq V$ and $A \cap X = A \cap C$ is*

$$q^{(\dim(A)-\dim(A\cap C))(d-\dim(C))} \binom{n - \dim(A + C)}{d - \dim(C)}_q. \tag{5.5}$$

Proof. The lemma is trivially true for $d \notin [\dim(C), n]$ since the Gaussian binomial coefficient in (5.5) is zero in that case. In what follows, we consider the complementary case $d \in [\dim(C), n]$.

Let $\mathscr{X}$ be the set of subspaces X in the statement of the lemma. Fix a basis $v_1, v_2, \ldots, v_{\dim(C)}$ for C. Let $\mathscr{B}$ be the set of all d-tuples $(v_1, \ldots, v_{\dim(C)}, u_1, \ldots, u_{d-\dim(C)})$ of vectors in V such that for all i,

$$u_i \notin A + C + \operatorname{span}\{u_1, u_2, \ldots, u_{i-1}\}. \tag{5.6}$$

Then each element of $\mathscr{B}$ is an ordered basis, with

$$|\mathscr{B}| = \prod_{i=1}^{d-\dim(C)} (q^n - q^{\dim(A+C)+i-1}). \tag{5.7}$$

CLAIM 5.3. *Every subspace $X \in \mathscr{X}$ has precisely*

$$\prod_{i=1}^{d-\dim(C)} (q^d - q^{\dim(C)+i-1}) \tag{5.8}$$

ordered bases in $\mathscr{B}$.

Proof. Let us say that a sequence of vectors $(u_1, u_2, \ldots, u_k)$ in X is *good* if (5.6) holds for all $i = 1, 2, \ldots, k$. We will prove that for every good sequence of k vectors in X, where $k < d - \dim(C)$, there are exactly $q^d - q^{\dim(C)+k}$ vectors $u_{k+1} \in X$ such that the sequence $(u_1, u_2, \ldots, u_{k+1})$ is good. Indeed, letting S, S', T in Fact 2.3 be the subspaces $X, C + \operatorname{span}\{u_1, u_2, \ldots, u_k\}, A$, respectively, we obtain

$$\begin{aligned} X \cap (A + C + \operatorname{span}\{u_1, u_2, \ldots, u_k\}) &= (X \cap A) + C + \operatorname{span}\{u_1, u_2, \ldots, u_k\} \\ &= (C \cap A) + C + \operatorname{span}\{u_1, u_2, \ldots, u_k\} \\ &= C + \operatorname{span}\{u_1, u_2, \ldots, u_k\}. \end{aligned}$$

Therefore, the only vectors $u_{k+1} \in X$ for which the sequence $(u_1, u_2, \ldots, u_{k+1})$ is not good are the elements of $C + \operatorname{span}\{u_1, u_2, \ldots, u_k\}$, which is a subspace of dimension $\dim(C) + k$ because it is spanned by the linearly independent vectors $v_1, v_2, \ldots, v_{\dim(C)}, u_1, u_2, \ldots, u_k$. In conclusion, out of the q^d vectors of X, there are precisely $q^{\dim(C)+k}$ vectors u_{k+1} for which the sequence $u_1, u_2, \ldots, u_{k+1}$ is not good.

It now follows immediately that the number of good sequences $(u_1, u_2, \ldots, u_{d-\dim(C)})$ of vectors in X is (5.8) as claimed, with $q^d - q^{\dim(C)}$ ways to choose u_1, then $q^d - q^{\dim(C)+1}$ ways to choose u_2 given u_1, then $q^d - q^{\dim(C)+2}$ ways to choose u_3 given u_1, u_2, and so on. □

CLAIM 5.4. *Every element of $\mathscr{B}$ is an ordered basis for some subspace in $\mathscr{X}$.*

Proof. Fix a tuple $(u_1, u_2, \ldots, u_{d-\dim(C)})$ with (5.6) for all i, and let

$$X = \operatorname{span}\{v_1, \ldots, v_{\dim(C)}, u_1, \ldots, u_{d-\dim(C)}\}.$$

Then clearly X is a d-dimensional subspace with $C \subseteq X \subseteq V$. This in particular means that $A \cap X$ contains $A \cap C$. It remains to prove the opposite inclusion, $A \cap X \subseteq A \cap C$. For this, fix arbitrary scalars α_i, β_j such that

$$\sum \alpha_i v_i + \sum \beta_j u_j \in A.$$

If some β_j were nonzero, we could take $j^* = \max\{j : \beta_j \neq 0\}$ and obtain $u_{j^*} \in \beta_{j^*}^{-1}(A - \sum \alpha_i v_i - \sum_{j<j^*} \beta_j u_j)$, contradicting (5.6). This means that $\beta_j = 0$ for all j, with the consequence that the vector $\sum \alpha_i v_i + \sum \beta_j u_j = \sum \alpha_i v_i$ belongs to C. This settles the containment $A \cap X \subseteq A \cap C$ and completes the proof. □

Claims 5.3 and 5.4 imply that $|\mathscr{X}|$ is the quotient of (5.7) by (5.8), namely,

$$\begin{aligned} |\mathscr{X}| &= \prod_{i=1}^{d-\dim(C)} \frac{q^n - q^{\dim(A+C)+i-1}}{q^d - q^{\dim(C)+i-1}} \\ &= \left(\frac{q^{\dim(A+C)}}{q^{\dim(C)}}\right)^{d-\dim(C)} \binom{n - \dim(A+C)}{d - \dim(C)}_q \\ &= q^{(\dim(A)-\dim(A\cap C))(d-\dim(C))} \binom{n - \dim(A+C)}{d - \dim(C)}_q. \end{aligned}$$

This completes the proof of the lemma. □

COROLLARY 5.5 (Counting subspaces internally). *Let $S' \subseteq S$ be linear subspaces in a vector space over $\mathbb{F}_q$. Let $d \geqslant 0$ be an integer. Then the number of dimension-d linear subspaces T with $S' \subseteq T \subseteq S$ is*

$$\binom{\dim(S) - \dim(S')}{d - \dim(S')}_q. \tag{5.9}$$

Proof. Set $V = S$, $C = S'$, and $A = \{0\}$ in the statement of Lemma 5.2 □

We now generalize Lemma 5.2 by allowing $A \cap X$ to be any subspace of A of a given dimension t.

LEMMA 5.6. *Let A, B be linear subspaces of an n-dimensional vector space V over $\mathbb{F}_q$. Define $r = \dim(A \cap B)$. Let d and t be nonnegative integers. Then the number of dimension-d linear subspaces X such that $B \subseteq X \subseteq V$ and $\dim(A \cap X) = t$ is*

$$q^{(\dim(A)-t)(d-t-\dim(B)+r)} \binom{n - \dim(A) - \dim(B) + r}{d - t - \dim(B) + r}_q \binom{\dim(A) - r}{t - r}_q. \tag{5.10}$$

Proof. The lemma is trivially true for $t \notin [r, \dim(A)]$ since the last Gaussian binomial coefficient in (5.10) is zero in that case. In what follows, we consider the complementary case $t \in [r, \dim(A)]$.

Let $\mathscr{X}$ be the set of all dimension-d subspaces X with $B \subseteq X \subseteq V$ and $\dim(A \cap X) = t$. Let $\mathscr{A}$ be the set of all dimension-t subspaces A' with $A \cap B \subseteq A' \subseteq A$. By Corollary 5.5,

$$|\mathscr{A}| = \binom{\dim(A) - r}{t - r}_q. \tag{5.11}$$

For any $X \in \mathscr{X}$, the subspace $A \cap X$ is by definition a dimension-t subspace of A that contains $A \cap B$. This makes it possible to define a function $f \colon \mathscr{X} \to \mathscr{A}$ by $f(X) = A \cap X$.

CLAIM 5.7. *For every $A' \in \mathscr{A}$,*

$$|f^{-1}(A')| = q^{(\dim(A)-t)(d-t-\dim(B)+r)} \binom{n - \dim(A) - \dim(B) + r}{d - t - \dim(B) + r}_q. \tag{5.12}$$

Proof. Define $C = A' + B$. Then $A \cap C = A' + A \cap B$ by Fact 2.3, which in view of $A \cap B \subseteq A'$ further yields

$$A \cap C = A'. \tag{5.13}$$

Now

$$\begin{aligned} |f^{-1}(A')| &= |\{X : X \text{ is a subspace of dimension } d \text{ with } B \subseteq X \subseteq V \text{ and } A \cap X = A'\}| \\ &= |\{X : X \text{ is a subspace of dimension } d \text{ with } C \subseteq X \subseteq V \text{ and } A \cap X = A'\}| \\ &= |\{X : X \text{ is a subspace of dimension } d \text{ with } C \subseteq X \subseteq V \text{ and } A \cap X = A \cap C\}| \\ &= q^{(\dim(A)-\dim(A\cap C))(d-\dim(C))} \binom{n - \dim(A + C)}{d - \dim(C)}_q, \end{aligned} \tag{5.14}$$

where the first step is immediate from the definitions of $\mathscr{X}$ and f; the second step holds because the condition $B \subseteq X$ is logically equivalent to $A' + B \subseteq X$ due to $A' \subseteq X$; the third step applies (5.13); and the final step uses Lemma 5.2.

It remains to calculate the dimensions of the relevant subspaces in (5.14). We have $\dim(C) = \dim(A' + B) = \dim(A') + \dim(B) - \dim(A' \cap B)$, which along with $A' \cap B = A \cap B$ and $\dim(A') = t$ yields

$$\dim(C) = t + \dim(B) - r. \tag{5.15}$$

It is immediate from (5.13) that

$$\dim(A \cap C) = t. \tag{5.16}$$

Finally, we have $\dim(A + C) = \dim(A + A' + B) = \dim(A + B)$ and therefore

$$\dim(A + C) = \dim(A) + \dim(B) - r. \tag{5.17}$$

Substituting (5.15)–(5.17) into (5.14), we arrive at the sought equality (5.12). □

Claim 5.7 implies that $|\mathscr{X}|$ is the product of the right-hand side of (5.11) and the right-hand side of (5.12), as was to be shown. □

COROLLARY 5.8. *Let $S' \subseteq S$ be linear subspaces in a vector space over $\mathbb{F}_q$. Let d and t be nonnegative integers. Then the number of dimension-d linear subspaces $T \subseteq S$ with $\dim(S' \cap T) = t$ is*

$$q^{(\dim(S')-t)(d-t)} \binom{\dim(S) - \dim(S')}{d-t}_q \binom{\dim(S')}{t}_q. \tag{5.18}$$

Proof. Invoke Lemma 5.6 with $V = S$, $A = S'$, and $B = \{0\}$. □

5.3. Subspace matrices. In [12], Knuth defined *combinatorial matrices of type* (n, t) as matrices whose rows and columns are indexed by t-element subsets of a fixed n-element set, and whose (A, B) entry depends only on $|A \cap B|$. We begin with analogous definitions in the setting of linear subspaces. Let $\mathbb{F}$ be a given finite field. For each $d = 0, 1, 2, \ldots, n$, fix an ordering on the set of dimension-d subspaces of $\mathbb{F}^n$.

DEFINITION 5.9. Let n, m, ℓ be nonnegative integers with $\max\{m, \ell\} \leqslant n$. For any $r \geqslant 0$, define $J_r^{\mathbb{F},n,m,\ell}$ to be the matrix whose rows are indexed by dimension-m subspaces of $\mathbb{F}^n$, columns indexed by dimension-ℓ subspaces of $\mathbb{F}^n$, and entries given by

$$(J_r^{\mathbb{F},n,m,\ell})_{A,B} = \begin{cases} 1 & \text{if } \dim(A \cap B) = r, \\ 0 & \text{otherwise,} \end{cases}$$

where the row index A and column index B use the ordering on the subspaces of $\mathbb{F}^n$ fixed at the beginning.

Thus, the (A, B) entry of $J_r^{\mathbb{F},n,m,\ell}$ depends only on the dimension of $A \cap B$ rather than the subspaces A, B themselves. By passing to the linear span of all such matrices for fixed $\mathbb{F}, n, m, \ell$, we obtain a matrix family that we call *subspace matrices*.

DEFINITION 5.10 (Subspace matrices). For a function $\varphi\colon \mathbb{Z} \to \mathbb{R}$, we define

$$J_\varphi^{\mathbb{F},n,m,\ell} = \sum_{r=0}^{\min\{m,\ell\}} \varphi(r) J_r^{\mathbb{F},n,m,\ell}. \tag{5.19}$$

Recall that throughout this manuscript, the underlying field is $\mathbb{F} = \mathbb{F}_q$ for an arbitrary prime power q. To avoid notational clutter, we will write simply $J_r^{n,m,\ell}$ and $J_\varphi^{n,m,\ell}$ to mean $J_r^{\mathbb{F},n,m,\ell}$ and $J_\varphi^{\mathbb{F},n,m,\ell}$, respectively.

To determine the eigenvalues of combinatorial matrices with rows and columns indexed by t-element subsets of $\{1, 2, \ldots, n\}$, Knuth investigates a certain homogeneous system of linear equations with variables indexed by s-element subsets and the equations themselves corresponding to $(s-1)$-element subsets. He refers to the solutions to such systems as (n, s)-*kernel systems*. It turns out that the linear space of kernel systems has a basis supported on variables labeled by a certain type of sets, which Knuth calls *basic sets* and which he fully describes in a combinatorial way. For any $s \in \{1, 2, \ldots, t\}$ and any (n, s)-kernel system (x_u), he shows that the corresponding vector (z_w),

indexed by t-element subsets w and given by $z_w = \sum_{u \subseteq w} x_u$, is an eigenvector for any combinatorial matrix of type (n, t). These vectors (z_w) for various values of s, together with the all-ones vector, make up a complete set of eigenvectors, and Knuth's analysis also reveals the associated eigenvalues.

Even setting aside the more subtle combinatorial nature of subspaces described in Section 5.2, it is not clear how to generalize Knuth's notion of basic sets to linear subspaces. For this reason, we do not appeal to combinatorial machinery and rely instead on linear-algebraic arguments. As another point of departure, our problem requires understanding the singular values of a general subspace matrix $J_\varphi^{n,m,\ell}$, whereas Knuth studied combinatorial matrices that are symmetric (analogous to the symmetric subspace matrices $J_\varphi^{n,m,m}$ in our setting). We note that the eigenvalues of symmetric subspace matrices $J_\varphi^{n,m,m}$ were also determined by Delsarte [10] and Eisfeld [11], and their properties were studied in [3, 8]. However, these previous analyses do not seem to apply to the general case of interest to us, namely, that of subspace matrices $J_\varphi^{n,m,\ell}$ for arbitrary m, ℓ.

We start by studying the subspace matrices $J_k^{n,m,k}$, which play a particularly important role in our analysis. The following lemma investigates their rank.

LEMMA 5.11. *Let n, m, k be nonnegative integers with $m \geqslant k \geqslant 0$ and $n \geqslant m + k$. Then*

$$\operatorname{rk} J_k^{n,m,k} = \binom{n}{k}_q. \tag{5.20}$$

Proof. In the degenerate case $n = 0$, the matrix $J_k^{n,m,k} = J_0^{0,0,0} = \begin{bmatrix}1\end{bmatrix}$ clearly has rank $\binom{0}{0}_q = 1$. In what follows, we treat the case $n \geqslant 1$. Here, we will exhibit reals $z_0, z_1, \ldots, z_k$ such that for all k-dimensional subspaces $A, B \subseteq \mathbb{F}_q^n$,

$$\sum_{X \subseteq \mathbb{F}_q^n \colon \dim X = m} z_{\dim(A \cap X)} (J_k^{n,m,k})_{X,B} = \delta_{\dim(A \cap B), k}. \tag{5.21}$$

Put differently, this means that every vector of the standard basis $e_1, e_2, \ldots$ can be obtained as a linear combination of the rows of $J_k^{n,m,k}$, immediately implying (5.20). Rewriting (5.21),

$$\sum_{i=0}^{k} z_i \sum_{\substack{X \subseteq \mathbb{F}_q^n \colon \dim X = m, \\ \dim(A \cap X) = i}} (J_k^{n,m,k})_{X,B} = \delta_{\dim(A \cap B), k} \qquad \forall A, B. \tag{5.22}$$

The inner summation equals the number of m-dimensional subspaces X with $B \subseteq X \subseteq \mathbb{F}_q^n$ and $\dim(A \cap X) = i$. Applying Lemma 5.6, we find that (5.22) is equivalent to

$$\sum_{i=0}^{k} z_i q^{(k-i)(m-i-k+r)} \binom{n-2k+r}{m-i-k+r}_q \binom{k-r}{i-r}_q = \delta_{r,k}, \qquad r = 0, 1, \ldots, k, \tag{5.23}$$

where r corresponds to $\dim(A \cap B)$ in (5.22). Write (5.23) in matrix form as

$$Mz = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \end{bmatrix}^{\mathsf{T}}, \tag{5.24}$$

where $M = [M_{r,i}]$ is the real matrix of order $k + 1$ given by

$$M_{r,i} = q^{(k-i)(m-i-k+r)} \binom{n-2k+r}{m-i-k+r}_q \binom{k-r}{i-r}_q$$

for $r, i \in \{0, 1, \ldots, k\}$. All entries of M below the diagonal are zero because $\binom{k-r}{i-r}_q = 0$ for $r > i$. The diagonal entries, on the other hand, are

$$M_{r,r} = q^{(k-r)(m-k)} \binom{n-2k+r}{m-k}_q,$$

which is nonzero because $n - 2k + r \geqslant m - k$ by the hypothesis that $n \geqslant m + k$. This makes M an upper triangular matrix with nonzero entries on the diagonal. Then M is invertible, and a solution z to (5.24) is guaranteed to exist. ∎

We will recover the k-th eigenspace of $J_\varphi^{n,m,m}$ as the image of $\ker J_{k-1}^{n,k-1,k}$ under the linear map $J_k^{n,m,k}$. The first step is to understand how the map $J_i^{n,m,k}$ acts on $\ker J_{k-1}^{n,k-1,k}$ for different values of i.

LEMMA 5.12. *Let $n \geqslant m \geqslant k$ be positive integers. Then for all $i = 0, 1, \ldots, k-1$ and $x \in \ker J_{k-1}^{n,k-1,k}$,*

$$J_i^{n,m,k} x = -q^{k-i-1} \cdot \frac{q^{i+1} - 1}{q^{k-i} - 1} J_{i+1}^{n,m,k} x. \tag{5.25}$$

Proof. Consider the matrix product $M = J_i^{n,m,k-1} J_{k-1}^{n,k-1,k}$. Let us compute the generic entry $M_{A,B}$, where $A, B \subseteq \mathbb{F}_q^n$ are subspaces of dimension m and k, respectively. By definition, $M_{A,B}$ is the number of $(k-1)$-dimensional subspaces $X \subseteq B$ such that $\dim(A \cap X) = i$. Invoking Corollary 5.8 with $S = B$ and $S' = A \cap B$, we obtain

$$(J_i^{n,m,k-1} J_{k-1}^{n,k-1,k})_{A,B} = q^{(r-i)(k-1-i)} \binom{k-r}{k-1-i}_q \binom{r}{i}_q,$$

where $r = \dim(A \cap B)$. Rewriting this equation in matrix form,

$$J_i^{n,m,k-1} J_{k-1}^{n,k-1,k} = \sum_{r=0}^{k} q^{(r-i)(k-1-i)} \binom{k-r}{k-1-i}_q \binom{r}{i}_q J_r^{n,m,k}.$$

In this equation, the product of the q-binomial coefficients vanishes whenever $r > i+1$ or $r < i$. Therefore, the above summation contains only two nonzero terms, namely,

$$J_i^{n,m,k-1} J_{k-1}^{n,k-1,k} = \sum_{r \in \{i, i+1\}} q^{(r-i)(k-1-i)} \binom{k-r}{k-1-i}_q \binom{r}{i}_q J_r^{n,m,k}.$$

Simplifying,

$$J_i^{n,m,k-1} J_{k-1}^{n,k-1,k} = \frac{q^{k-i} - 1}{q - 1} J_i^{n,m,k} + q^{k-1-i} \cdot \frac{q^{i+1} - 1}{q - 1} J_{i+1}^{n,m,k}.$$

Applying this matrix equation to a vector $x \in \ker J_{k-1}^{n,k-1,k}$ gives

$$0 = \frac{q^{k-i} - 1}{q - 1} J_i^{n,m,k} x + q^{k-1-i} \cdot \frac{q^{i+1} - 1}{q - 1} J_{i+1}^{n,m,k} x,$$

which directly implies (5.25). ∎

COROLLARY 5.13. *Let $n \geqslant m \geqslant k$ be positive integers. Then for all $r = 0, 1, \ldots, k$ and $x \in \ker J_{k-1}^{n,k-1,k}$,*

$$J_r^{n,m,k} x = (-1)^{k-r} q^{\binom{k-r}{2}} \binom{k}{r}_q J_k^{n,m,k} x. \tag{5.26}$$

Proof. The proof is by induction on $k-r$ for fixed integers n, m, k. For the base case $r = k$, the equality in (5.26) is trivial. For the inductive step with $k - r > 0$, we have

$$\begin{aligned} J_r^{n,m,k} x &= -q^{k-r-1} \cdot \frac{q^{r+1}-1}{q^{k-r}-1} J_{r+1}^{n,m,k} x \\ &= -q^{k-r-1} \cdot \frac{q^{r+1}-1}{q^{k-r}-1} \cdot (-1)^{k-r-1} q^{\binom{k-r-1}{2}} \binom{k}{r+1}_q J_k^{n,m,k} x \\ &= (-1)^{k-r} q^{\binom{k-r}{2}} \binom{k}{r}_q J_k^{n,m,k} x, \end{aligned}$$

where the first step uses Lemma 5.12, and the second step applies the inductive hypothesis. □

Let $A, B \subseteq \mathbb{F}_q^n$ be arbitrary subspaces of dimension m and ℓ, respectively. Recall from Fact 2.4 that for fixed n, m, ℓ, the dimension of $A \cap B$ is uniquely determined by the dimension of $A^\perp \cap B^\perp$. This makes the subspace matrix $J_\varphi^{n,m,\ell}$ identical, up to a permutation of the rows and columns, to the subspace matrix $J_{\varphi'}^{n,n-m,n-\ell}$ for an appropriate function φ'. We record this fact as our next lemma. Its role in our work will be to simplify the calculation of the singular values of $J_\varphi^{n,m.\ell}$ and the eigenvalues of $J_\varphi^{n,m,m}$ by reducing the general case to the case $m+\ell \leqslant n$ and $m \leqslant n/2$, respectively.

LEMMA 5.14. *Let n, m, ℓ be nonnegative integers with $\max\{m, \ell\} \leqslant n$. Let $\varphi\colon \mathbb{Z} \to \mathbb{R}$ be given. Then:*

(i) $J_\varphi^{n,m,\ell} = P J_{\varphi'}^{n,n-m,n-\ell} Q$, where P, Q are permutation matrices and $\varphi'\colon \mathbb{Z} \to \mathbb{R}$ is defined by $\varphi'(t) = \varphi(t + m + \ell - n)$;

(ii) $J_\varphi^{n,m,m} = P J_{\varphi''}^{n,n-m,n-m} P^{-1}$, where P is a permutation matrix and $\varphi''\colon \mathbb{Z} \to \mathbb{R}$ is defined by $\varphi''(t) = \varphi(t + 2m - n)$.

Proof. Recall that for any $d \in \{0, 1, \ldots, n\}$, the map $S \mapsto S^\perp$ is a bijection between the subspaces of $\mathbb{F}_q^n$ of dimension d and those of dimension $n - d$. For subspaces $A, B \subseteq \mathbb{F}_q^n$ of dimension m and ℓ, respectively, we have

$$\begin{aligned} (J_\varphi^{n,m,\ell})_{A,B} &= \varphi(\dim(A \cap B)) \\ &= \varphi(\dim(A^\perp \cap B^\perp) + m + \ell - n) \\ &= \varphi'(\dim(A^\perp \cap B^\perp)) \\ &= (J_{\varphi'}^{n,n-m,n-\ell})_{A^\perp, B^\perp}, \end{aligned}$$

where the second step uses Fact 2.4. Rewriting this conclusion in matrix form,

$$J_\varphi^{n,m,\ell} = [(J_{\varphi'}^{n,n-m,n-\ell})_{A^\perp, B^\perp}]_{A,B},$$

where A, B range over all subspaces of dimension m and ℓ, respectively. The matrix on the right-hand side is clearly $J_{\varphi'}^{n,n-m,n-\ell}$, up to a reordering of the rows and columns. This settles (i).

An argument analogous to the above yields

$$J_\varphi^{n,m,m} = [(J_{\varphi''}^{n,n-m,n-m})_{A^\perp, B^\perp}]_{A,B},$$

where A, B range over all subspaces of dimension m. The matrix on the right-hand side is the result of permuting the rows and columns of $J_{\varphi''}^{n,n-m,n-m}$ according to the same permutation, which is another way of phrasing (ii). □

5.4. Eigenvalues and eigenvectors of subspace matrices. Our description of the spectrum of each $J_\varphi^{n,m,\ell}$ is in terms of a function which we now define.

DEFINITION 5.15. For nonnegative integers n, m, ℓ, r, k with $\max\{m, \ell\} \leqslant n$ and $k \leqslant \min\{m, \ell\}$, define

$$\Lambda_r^{n,m,\ell}(k) = \sum_{i=0}^{k} (-1)^i \binom{k}{i}_q q^{\binom{i}{2}+(m-r)(\ell-r-i)} \binom{n-m-i}{\ell-r-i}_q \binom{m-k+i}{r-k+i}_q.$$

More generally, for any $\varphi\colon \mathbb{Z} \to \mathbb{R}$, define

$$\Lambda_\varphi^{n,m,\ell}(k) = \sum_{r=0}^{\min\{m,\ell\}} \varphi(r) \Lambda_r^{n,m,\ell}(k).$$

As part of our analysis of the eigenvalues of $J_\varphi^{n,m,m}$, we will determine its eigenspaces and show that they are pairwise orthogonal. The orthogonality will follow from the pairwise distinctness of the corresponding eigenvalues, with the following lemma playing a crucial role.

LEMMA 5.16. *Let n, m be nonnegative integers with $m \leqslant n/2$. Then the numbers $\Lambda_0^{n,m,m}(k)$ for $k = 0, 1, \ldots, m$ are pairwise distinct.*

Proof. For $r = 0$, the q-binomial coefficient $\binom{m-k+i}{r-k+i}_q$ in Definition 5.15 vanishes unless $i = k$. As a result,

$$\begin{aligned}\Lambda_0^{n,m,m}(k) &= (-1)^k q^{\binom{k}{2}+m(m-k)} \binom{n-m-k}{m-k}_q \\ &= (-1)^k q^{\binom{k}{2}+m(m-k)} \binom{n-m-k}{n-2m}_q.\end{aligned}$$

For $k \in \{0, 1, \ldots, m\}$, the q-binomial coefficient in the last expression is clearly positive and a nonincreasing function of k, whereas the exponent of q is a strictly decreasing function of k. It follows that the numbers $|\Lambda_0^{n,m,m}(k)|$ for $k = 0, 1, \ldots, m$ form a strictly decreasing sequence. □

As in [12], we treat the all-ones eigenvector separately.

PROPOSITION 5.17. *Let n, m, ℓ, r be nonnegative integers with $\max\{m, \ell\} \leqslant n$. Then*

$$J_r^{n,m,\ell}\,\mathbf{1} = q^{(m-r)(\ell-r)} \binom{n-m}{\ell-r}_q \binom{m}{r}_q \mathbf{1} \tag{5.27}$$

$$= \Lambda_r^{n,m,\ell}(0)\,\mathbf{1}, \tag{5.28}$$

$$\|J_r^{n,m,\ell}\|_1 = q^{(m-r)(\ell-r)} \binom{n-m}{\ell-r}_q \binom{m}{r}_q \binom{n}{m}_q. \tag{5.29}$$

More generally, for $\varphi\colon \mathbb{Z} \to \mathbb{R}$,

$$J_\varphi^{n,m,\ell}\,\mathbf{1} = \Lambda_\varphi^{n,m,\ell}(0)\,\mathbf{1}, \tag{5.30}$$

$$\|J_\varphi^{n,m,\ell}\|_1 = \sum_{r=0}^{\min\{m,\ell\}} |\varphi(r)|\, q^{(m-r)(\ell-r)} \binom{n-m}{\ell-r}_q \binom{m}{r}_q \binom{n}{m}_q. \tag{5.31}$$

Proof. Let $A \subseteq \mathbb{F}_q^n$ be a subspace of dimension m. By definition, $(J_r^{n,m,\ell}\,\mathbf{1})_A$ is the number of ℓ-dimensional subspaces $X \subseteq \mathbb{F}_q^n$ with $\dim(A \cap X) = r$. Taking $S' = A$ and $S = \mathbb{F}_q^n$ in Corollary 5.8, we obtain

$$(J_r^{n,m,\ell}\,\mathbf{1})_A = q^{(m-r)(\ell-r)} \binom{n-m}{\ell-r}_q \binom{m}{r}_q.$$

This settles (5.27), which in turn implies (5.28) by Definition 5.15. Since there are exactly $\binom{n}{m}_q$ subspaces $A \subseteq \mathbb{F}_q^n$ of dimension m, equation (5.29) is immediate from (5.27). Equation (5.30) follows by linearity from (5.19) and (5.28). Analogously, (5.31) follows from (5.19) and (5.29) since the matrices $J_r^{n,m,\ell}$ for $r \geqslant 0$ have disjoint support. $\square$

The following lemma is the cornerstone of our analysis of the spectrum of subspace matrices $J_\varphi^{n,m,\ell}$. It generalizes Knuth's work from sets to subspaces ($m = \ell$) and further to the asymmetric case of interest to us ($m \neq \ell$).

LEMMA 5.18. *Let n, m, ℓ be positive integers with $n \geqslant m + \ell$. Let $k \in \{1, 2, \ldots, \min\{m, \ell\}\}$ and $x \in \ker J_{k-1}^{n,k-1,k}$ be given. Then for all integers $t \geqslant 0$,*

$$J_t^{n,m,\ell} J_k^{n,\ell,k} x = \Lambda_t^{n,m,\ell}(k) J_k^{n,m,k} x. \tag{5.32}$$

More generally, for all $\varphi\colon \mathbb{Z} \to \mathbb{R}$,

$$J_\varphi^{n,m,\ell} J_k^{n,\ell,k} x = \Lambda_\varphi^{n,m,\ell}(k) J_k^{n,m,k} x. \tag{5.33}$$

Proof. Fix an arbitrary integer $t \geqslant 0$ and define $M = J_t^{n,m,\ell} J_k^{n,\ell,k}$. Let us compute the generic entry $M_{A,B}$, where A, B are subspaces of $\mathbb{F}_q^n$ of dimension m and k, respectively. By definition, $M_{A,B}$ is the number of ℓ-dimensional subspaces X such that $\dim(A \cap X) = t$ and $B \subseteq X \subseteq \mathbb{F}_q^n$. Lemma 5.6 implies that

$$(J_t^{n,m,\ell} J_k^{n,\ell,k})_{A,B} = q^{(m-t)(\ell-t-k+r)} \binom{n-m-k+r}{\ell-t-k+r}_q \binom{m-r}{t-r}_q,$$

where $r = \dim(A \cap B)$. Rewriting this equation in matrix form, we obtain

$$J_t^{n,m,\ell} J_k^{n,\ell,k} = \sum_{r=0}^{k} q^{(m-t)(\ell-t-k+r)} \binom{n-m-k+r}{\ell-t-k+r}_q \binom{m-r}{t-r}_q J_r^{n,m,k}.$$

Applying this matrix identity to a vector $x \in \ker J_{k-1}^{n,k-1,k}$, we find

$$\begin{aligned}
J_t^{n,m,\ell} J_k^{n,\ell,k} x &= \sum_{r=0}^{k} q^{(m-t)(\ell-t-k+r)} \binom{n-m-k+r}{\ell-t-k+r}_q \binom{m-r}{t-r}_q J_r^{n,m,k} x \\
&= \sum_{r=0}^{k} q^{(m-t)(\ell-t-k+r)} \binom{n-m-k+r}{\ell-t-k+r}_q \binom{m-r}{t-r}_q \cdot (-1)^{k-r} q^{\binom{k-r}{2}} \binom{k}{r}_q J_k^{n,m,k} x \\
&= \sum_{r=0}^{k} q^{(m-t)(\ell-t-k+r)} \binom{n-m-k+r}{\ell-t-k+r}_q \binom{m-r}{t-r}_q \cdot (-1)^{k-r} q^{\binom{k-r}{2}} \binom{k}{k-r}_q J_k^{n,m,k} x \\
&= \sum_{i=0}^{k} q^{(m-t)(\ell-t-i)} \binom{n-m-i}{\ell-t-i}_q \binom{m-k+i}{t-k+i}_q \cdot (-1)^{i} q^{\binom{i}{2}} \binom{k}{i}_q J_k^{n,m,k} x \\
&= \Lambda_t^{n,m,\ell}(k)\, J_k^{n,m,k} x,
\end{aligned}$$

where the second step uses Corollary 5.13, the fourth step is a change of variable, and the last step is immediate by Definition 5.15. This settles (5.32). Now for any $\varphi\colon \mathbb{Z} \to \mathbb{R}$,

$$J_\varphi^{n,m,\ell} J_k^{n,\ell,k} x = \sum_{t=0}^{\min\{m,\ell\}} \varphi(t) J_t^{n,m,\ell} J_k^{n,\ell,k} x = \sum_{t=0}^{\min\{m,\ell\}} \varphi(t) \Lambda_t^{n,m,\ell}(k) J_k^{n,m,k} x = \Lambda_\varphi^{n,m,\ell}(k) J_k^{n,m,k} x,$$

where the first step uses (5.19), the second step applies (5.32), and the last step is valid by Definition 5.15. $\square$

We are now in a position to describe the eigenvalues of every symmetric subspace matrix.

THEOREM 5.19 (Eigenvalues of $J_\varphi^{n,m,m}$). *Let $n \geqslant m \geqslant 0$ be given integers.*

(i) *If $m \leqslant n/2$, then the eigenvalues of $J_\varphi^{n,m,m}$ for a given function $\varphi\colon \mathbb{Z} \to \mathbb{R}$ are $\Lambda_\varphi^{n,m,m}(k)$ for $k = 0, 1, \ldots, m$, with corresponding multiplicities $\binom{n}{k}_q - \binom{n}{k-1}_q$ for $k = 0, 1, \ldots, m$.*

(ii) *If $m \geqslant n/2$, then the eigenvalues of $J_\varphi^{n,m,m}$ for a given function $\varphi\colon \mathbb{Z} \to \mathbb{R}$ are $\Lambda_\psi^{n,n-m,n-m}(k)$ for $k = 0, 1, \ldots, n-m$, with corresponding multiplicities $\binom{n}{k}_q - \binom{n}{k-1}_q$ for $k = 0, 1, \ldots, n-m$, with $\psi\colon \mathbb{Z} \to \mathbb{R}$ given by $\psi(t) = \varphi(t + 2m - n)$.*

Proof. We first show that (i) implies (ii). Recall from Lemma 5.14 that $J_\varphi^{n,m,m}$ is permutation-similar to $J_\psi^{n,n-m,n-m}$ with $\psi\colon \mathbb{Z} \to \mathbb{R}$ given by $\psi(t) = \varphi(t + 2m - n)$. The eigenvalues of $J_\psi^{n,n-m,n-m}$ are, by part (i) of this theorem, $\Lambda_\psi^{n,n-m,n-m}(k)$ for $k = 0, 1, \ldots, n-m$, with corresponding multiplicities $\binom{n}{k}_q - \binom{n}{k-1}_q$ for $k = 0, 1, \ldots, n-m$. It follows that these are also the eigenvalues of $J_\varphi^{n,m,m}$ because a similarity transformation preserves the eigenvalues and their multiplicities. This settles (ii).

It remains to prove (i), where by hypothesis

$$m \leqslant \frac{n}{2}. \tag{5.34}$$

Define subspaces $S_0, S_1, \ldots, S_m$ of the $\binom{n}{m}_q$-dimensional real vector space by

$$S_0 = \operatorname{span}\{\mathbf{1}\},$$
$$S_k = \{J_k^{n,m,k} x : x \in \ker J_{k-1}^{n,k-1,k}\}, \qquad k = 1, 2, \ldots, m.$$

CLAIM 5.20. *Let $k \in \{0, 1, \ldots, m\}$. Then $\dim S_k = \binom{n}{k}_q - \binom{n}{k-1}_q$.*

Proof. We need only consider $k \geqslant 1$, the claim being trivial otherwise. Observe from (5.34) and Lemma 5.11 that $J_k^{n,m,k}$ has rank $\binom{n}{k}_q$. Put another way, its columns are linearly independent. Since S_k is the image of $\ker J_{k-1}^{n,k-1,k}$ under $J_k^{n,m,k}$, it follows that

$$\dim S_k = \dim \ker J_{k-1}^{n,k-1,k}. \tag{5.35}$$

Another appeal to (5.34) and Lemma 5.11 reveals that the columns of $J_{k-1}^{n,k,k-1}$ are linearly independent. This makes $J_{k-1}^{n,k-1,k} = (J_{k-1}^{n,k,k-1})^\mathsf{T}$ a matrix of order $\binom{n}{k-1}_q \times \binom{n}{k}_q$ with linearly independent rows, whence $\dim \ker J_{k-1}^{n,k-1,k} = \binom{n}{k}_q - \binom{n}{k-1}_q$. In view of (5.35), the proof is complete. □

CLAIM 5.21. *Let $k \in \{0, 1, \ldots, m\}$. Then every vector of S_k is an eigenvector of $J_\varphi^{n,m,m}$ with eigenvalue $\Lambda_\varphi^{n,m,m}(k)$.*

Proof. For $k = 0$, the claim is immediate from (5.30) of Proposition 5.17. Consider now the complementary case $k \in \{1, 2, \ldots, m\}$. Here, n and m are positive integers. Invoking Lemma 5.18 with $\ell = m$ and (5.34) yields $J_\varphi^{n,m,m} v = \Lambda_\varphi^{n,m,m}(k) v$ for all $v \in S_k$, as desired. □

CLAIM 5.22. *For any $k, k' \in \{0, 1, \ldots, m\}$ with $k \neq k'$, the subspaces S_k and $S_{k'}$ are orthogonal.*

Proof. Taking $\varphi = \mathbf{1}_{\{0\}}$ in Claim 5.21 shows that $S_0, S_1, \ldots, S_m$ are eigenspaces of the symmetric matrix $J_0^{n,m,m}$ with eigenvalues $\Lambda_0^{n,m,m}(0), \Lambda_0^{n,m,m}(1), \ldots, \Lambda_0^{n,m,m}(m)$, respectively. But these $m + 1$ numbers are pairwise distinct by (5.34) and Lemma 5.16. It now follows from Fact 2.5 that $S_0, S_1, \ldots, S_m$ are pairwise orthogonal. □

As we just established with Claim 5.22, the subspaces $S_0, S_1, \ldots, S_m$ are pairwise orthogonal. Since they are subspaces over the *reals,* we infer that $\dim(\sum_{k=0}^m S_k) = \sum_{k=0}^m \dim S_k$. Using $\dim S_k = \binom{n}{k}_q - \binom{n}{k-1}_q$ from Claim 5.20, we arrive at

$$\dim \left(\sum_{k=0}^m S_k \right) = \sum_{k=0}^m \left(\binom{n}{k}_q - \binom{n}{k-1}_q \right) = \binom{n}{m}_q - \binom{n}{-1}_q = \binom{n}{m}_q .$$

In other words, a basis for the vector space in question can be obtained by concatenating bases for $S_0, S_1, \ldots, S_m$. Lastly, recall from Claim 5.21 that S_k (for $k = 0, 1, \ldots, m$) is an eigenspace of $J_\varphi^{n,m,m}$ with eigenvalue $\Lambda_\varphi^{n,m,m}(k)$. This settles (i) and completes the proof of the theorem. □

At last, we adapt the previous proof to the asymmetric case ($m \neq \ell$) and determine the singular values of every subspace matrix $J_\varphi^{n,m,\ell}$.

THEOREM 5.23 (Singular values of $J_\varphi^{n,m,\ell}$). *Let n, m, ℓ be nonnegative integers with* $\max\{m, \ell\} \leqslant n$.

(i) *If $m + \ell \leqslant n$, then the singular values of $J_\varphi^{n,m,\ell}$ for a given function $\varphi\colon \mathbb{Z} \to \mathbb{R}$ are*

$$\sqrt{\Lambda_\varphi^{n,m,\ell}(k)\, \Lambda_\varphi^{n,\ell,m}(k)}, \qquad k = 0, 1, \ldots, \min\{m, \ell\},$$

with corresponding multiplicities $\binom{n}{k}_q - \binom{n}{k-1}_q$ for $k = 0, 1, \ldots, \min\{m, \ell\}$.

(ii) *If $m + \ell \geqslant n$, then the singular values of $J_\varphi^{n,m,\ell}$ for a given function $\varphi\colon \mathbb{Z} \to \mathbb{R}$ are*

$$\sqrt{\Lambda_\psi^{n,n-m,n-\ell}(k)\, \Lambda_\psi^{n,n-\ell,n-m}(k)}, \qquad k = 0, 1, \ldots, \min\{n-m, n-\ell\},$$

with corresponding multiplicities $\binom{n}{k}_q - \binom{n}{k-1}_q$ for $k = 0, 1, \ldots, \min\{n-m, n-\ell\}$, where $\psi\colon \mathbb{Z} \to \mathbb{R}$ is given by $\psi(t) = \varphi(t + m + \ell - n)$.

Proof. We first show that (i) implies (ii). Recall from Lemma 5.14 that the matrix $J_\varphi^{n,m,\ell}$ is the same, up to a reordering of the rows and columns, as $J_\psi^{n,n-m,n-\ell}$ with $\psi\colon \mathbb{Z} \to \mathbb{R}$ given by $\psi(t) = \varphi(t + m + \ell - n)$. The singular values of $J_\psi^{n,n-m,n-\ell}$ are, by part (i) of this theorem, $\sqrt{\Lambda_\psi^{n,n-m,n-\ell}(k)\, \Lambda_\psi^{n,n-\ell,n-m}(k)}$ for $k = 0, 1, \ldots, \min\{n-m, n-\ell\}$, with corresponding multiplicities $\binom{n}{k}_q - \binom{n}{k-1}_q$ for $k = 0, 1, \ldots, \min\{n-m, n-\ell\}$. It follows that these are also the singular values of $J_\varphi^{n,m,\ell}$ because reordering the columns or rows does not change the singular values or their multiplicities. This establishes (ii).

It remains to settle (i), where by hypothesis

$$m + \ell \leqslant n. \tag{5.36}$$

We may further assume that

$$m \leqslant \ell, \tag{5.37}$$

for otherwise we can work with the transposed matrix $(J_\varphi^{n,m,\ell})^{\mathsf{T}} = J_\varphi^{n,\ell,m}$, the singular values being invariant under matrix transposition. By (5.36), (5.37), and Fact 2.12,

$$\binom{n}{m}_q \leqslant \binom{n}{\ell}_q . \tag{5.38}$$

Another consequence of (5.36) and (5.37) is that $m \leqslant n/2$, which makes it possible to define subspaces $S_0, S_1, \ldots, S_m$ of the $\binom{n}{m}_q$-dimensional real vector space as in the proof of part (i) of Theorem 5.19. In particular, Claims 5.20–5.22 apply as before.

CLAIM 5.24. *Let $k \in \{0, 1, \ldots, m\}$. Then every vector of S_k is an eigenvector of $J_\varphi^{n,m,\ell} J_\varphi^{n,\ell,m}$ with eigenvalue $\Lambda_\varphi^{n,m,\ell}(k)\Lambda_\varphi^{n,\ell,m}(k)$.*

Proof. For $k = 0$, a double application of Proposition 5.17 yields $J_\varphi^{n,m,\ell} J_\varphi^{n,\ell,m} \mathbf{1} = J_\varphi^{n,m,\ell} \Lambda_\varphi^{n,\ell,m}(0)\, \mathbf{1} = \Lambda_\varphi^{n,m,\ell}(0)\Lambda_\varphi^{n,\ell,m}(0)\, \mathbf{1}$, as desired. Consider now $k \in \{1, 2, \ldots, m\}$. In this case, due to (5.37), the integers n, m, ℓ are positive and satisfy $\min\{m, \ell\} = m$. Then for any $x \in \ker J_{k-1}^{n,k-1,k}$,

$$\begin{aligned}
(J_\varphi^{n,m,\ell} J_\varphi^{n,\ell,m}) J_k^{n,m,k} x &= J_\varphi^{n,m,\ell}(J_\varphi^{n,\ell,m} J_k^{n,m,k} x) \\
&= J_\varphi^{n,m,\ell}(\Lambda_\varphi^{n,\ell,m}(k) J_k^{n,\ell,k} x) \\
&= \Lambda_\varphi^{n,\ell,m}(k) J_\varphi^{n,m,\ell} J_k^{n,\ell,k} x \\
&= \Lambda_\varphi^{n,\ell,m}(k)\Lambda_\varphi^{n,m,\ell}(k) J_k^{n,m,k} x,
\end{aligned}$$

where the second and fourth steps apply Lemma 5.18 with (5.36) (note that the roles of m and ℓ are reversed in the first application). We have shown that for each $x \in \ker J_{k-1}^{n,k-1,k}$, its image under $J_k^{n,m,k}$ is an eigenvector of $J_\varphi^{n,m,\ell} J_\varphi^{n,\ell,m}$ with eigenvalue $\Lambda_\varphi^{n,\ell,m}(k)\Lambda_\varphi^{n,m,\ell}(k)$. Since S_k is by definition the image of $\ker J_{k-1}^{n,k-1,k}$ under $J_k^{n,m,k}$, the claim is proved. □

Recall from Claims 5.20 and 5.22 that the subspaces $S_0, S_1, \ldots, S_m$ are pairwise orthogonal, with $\dim S_k = \binom{n}{k}_q - \binom{n}{k-1}_q$. As in the proof of Theorem 5.19, this implies that the real vector space in question is a direct sum of $S_0, S_1, \ldots, S_m$. In view of Claim 5.24, we conclude that the eigenvalues of $J_\varphi^{n,m,\ell} J_\varphi^{n,\ell,m}$ are $\Lambda_\varphi^{n,m,\ell}(k)\Lambda_\varphi^{n,\ell,m}(k)$ for $k = 0, 1, \ldots, m$, with corresponding multiplicities $\binom{n}{k}_q - \binom{n}{k-1}_q$ for $k = 0, 1, \ldots, m$. This completes the proof since the singular values of $J_\varphi^{n,m,\ell}$ are, by (5.38) and Fact 2.6, the square roots of the eigenvalues of $J_\varphi^{n,m,\ell}(J_\varphi^{n,m,\ell})^\intercal = J_\varphi^{n,m,\ell} J_\varphi^{n,\ell,m}$, counting multiplicities. □

5.5. Normalized subspace matrices. To study the communication complexity of the subspace intersection problem, we now define normalized versions of subspace matrices.

DEFINITION 5.25. Let n, m, ℓ be nonnegative integers with $m + \ell \leqslant n$, and let $\mathbb{F}$ be a finite field. Define

$$\overline{J}_r^{\mathbb{F},n,m,\ell} = \frac{1}{\|J_r^{\mathbb{F},n,m,\ell}\|_1} \cdot J_r^{\mathbb{F},n,m,\ell}, \qquad r = 0, 1, 2, \ldots, \min\{m, \ell\}. \tag{5.39}$$

For any function $\varphi\colon \mathbb{Z} \to \mathbb{R}$, define

$$\overline{J}_\varphi^{\mathbb{F},n,m,\ell} = \sum_{r=0}^{\min\{m,\ell\}} \varphi(r) \overline{J}_r^{\mathbb{F},n,m,\ell}. \tag{5.40}$$

The requirement $m + \ell \leqslant n$ in Definition 5.25 serves to ensure that $J_r^{\mathbb{F},n,m,\ell} \neq 0$ for each $r = 0, 1, \ldots, \min\{m, \ell\}$, so that the normalization in (5.39) is meaningful. As elsewhere in this manuscript, we will work with the generic field $\mathbb{F} = \mathbb{F}_q$ and will henceforth write $\overline{J}_r^{n,m,\ell}$ and $\overline{J}_\varphi^{n,m,\ell}$ instead of $\overline{J}_r^{\mathbb{F},n,m,\ell}$ and $\overline{J}_\varphi^{\mathbb{F},n,m,\ell}$.

The following lemma relates the metric properties of a normalized subspace matrix $\overline{J}_\varphi^{n,m,\ell}$ to the corresponding univariate function φ.

LEMMA 5.26 (Metric properties of $\overline{J}_\varphi^{n,m,\ell}$). *Let n, m, ℓ be nonnegative integers with $m + \ell \leqslant n$. Let $\varphi\colon \mathbb{Z} \to \mathbb{R}$ be a given function. Then:*

$$\sum_{\substack{S\in\mathscr{S}(\mathbb{F}_q^n,m),\\ T\in\mathscr{S}(\mathbb{F}_q^n,\ell):\\ \dim(S\cap T)=r}} (\overline{J}_\varphi^{n,m,\ell})_{S,T} = \varphi(r), \qquad r = 0, 1, \ldots, \min\{m, \ell\}. \tag{5.41}$$

Moreover,

$$\|\overline{J}_\varphi^{n,m,\ell}\|_1 = \sum_{r=0}^{\min\{m,\ell\}} |\varphi(r)|. \tag{5.42}$$

Proof. We have

$$\begin{aligned}
\sum_{S,T:\dim(S\cap T)=r} (\overline{J}_\varphi^{n,m,\ell})_{S,T} &= \sum_{S,T:\dim(S\cap T)=r} \sum_{i=0}^{\min\{m,\ell\}} \frac{\varphi(i)}{\|J_i^{n,m,\ell}\|_1} \cdot (J_i^{n,m,\ell})_{S,T} \\
&= \sum_{S,T:\dim(S\cap T)=r} \frac{\varphi(r)}{\|J_r^{n,m,\ell}\|_1} \cdot (J_r^{n,m,\ell})_{S,T} \\
&= \frac{\varphi(r)}{\|J_r^{n,m,\ell}\|_1} \sum_{S,T:\dim(S\cap T)=r} (J_r^{n,m,\ell})_{S,T} \\
&= \varphi(r),
\end{aligned} \tag{5.43}$$

where the second step uses $(J_i^{n,m,\ell})_{S,T} = 0$ for $i \neq r$, and the final step is valid because $(J_r^{n,m,\ell})_{S,T}$ equals 1 if $\dim(S \cap T) = r$ and 0 otherwise. This proves (5.41). An analogous argument yields

$$\sum_{S,T:\dim(S\cap T)=r} |(\overline{J}_\varphi^{n,m,\ell})_{S,T}| = |\varphi(r)|.$$

Summing this equation over r gives (5.42). □

To describe the singular values of a normalized subspace matrix $\overline{J}_\varphi^{n,m,\ell}$, we introduce a normalized counterpart of the function Λ from Definition 5.15.

DEFINITION 5.27. Let n, m, ℓ, k be nonnegative integers with $m+\ell \leqslant n$ and $k \leqslant \min\{m, \ell\}$. Define

$$\overline{\Lambda}_r^{n,m,\ell}(k) = \frac{1}{\|J_r^{n,m,\ell}\|_1} \Lambda_r^{n,m,\ell}(k), \qquad r = 0, 1, \ldots, \min\{m, \ell\}.$$

More generally, for any $\varphi\colon \mathbb{Z} \to \mathbb{R}$, define

$$\overline{\Lambda}_\varphi^{n,m,\ell}(k) = \sum_{r=0}^{\min\{m,\ell\}} \varphi(r) \overline{\Lambda}_r^{n,m,\ell}(k).$$

With this notation, we obtain the following counterpart of Theorem 5.23 for normalized subspace matrices.

THEOREM 5.28. *Let n, m, ℓ be nonnegative integers with $m + \ell \leqslant n$. Let $\varphi\colon \mathbb{Z} \to \mathbb{R}$ be given. Then the singular values of $\overline{J}_\varphi^{n,m,\ell}$ are: $\sqrt{\overline{\Lambda}_\varphi^{n,m,\ell}(k)\, \overline{\Lambda}_\varphi^{n,\ell,m}(k)}$ with multiplicity $\binom{n}{k}_q - \binom{n}{k-1}_q$, where $k = 0, 1, \ldots, \min\{m, \ell\}$.*

Proof. By definition, $\overline{J}_{\varphi}^{n,m,\ell} = J_{\varphi'}^{n,m,\ell}$ with $\varphi' \colon \mathbb{Z} \to \mathbb{R}$ given by

$$\varphi'(r) = \begin{cases} \varphi(r)/\|J_r^{n,m,\ell}\|_1 & \text{if } r \in \{0,1,\dots,\min\{m,\ell\}\}, \\ 0 & \text{otherwise.} \end{cases}$$

Recall from Theorem 5.23 that the singular values of $J_{\varphi'}^{n,m,\ell}$ are $\sqrt{\Lambda_{\varphi'}^{n,m,\ell}(k)\,\Lambda_{\varphi'}^{n,\ell,m}(k)}$ with multiplicity $\binom{n}{k}_q - \binom{n}{k-1}_q$, where $k = 0,1,\dots,\min\{m,\ell\}$. Since $\Lambda_{\varphi'}^{n,m,\ell}(k) = \overline{\Lambda}_{\varphi}^{n,m,\ell}(k)$ and $\Lambda_{\varphi'}^{n,\ell,m}(k) = \overline{\Lambda}_{\varphi}^{n,\ell,m}(k)$ by Definition 5.27, the proof is complete. ∎

With our next lemma, we establish key algebraic and analytic properties of $\overline{\Lambda}_r^{n,m,\ell}(k)$.

LEMMA 5.29. *Let n, m, ℓ, k be nonnegative integers with $m + \ell \leqslant n$ and $k \leqslant \min\{m,\ell\}$. Then:*

(i) *for n, m, ℓ, k fixed, $\overline{\Lambda}_r^{n,m,\ell}(k)$ as a function of $r \in \{0,1,\dots,\min\{m,\ell\}\}$ is a polynomial in q^r of degree at most k;*
(ii) *$|\overline{\Lambda}_r^{n,m,\ell}(k)| \leqslant 8\binom{n}{m}_q^{-1} q^{-k(m-r)/2}$ for $r = 0,1,\dots,\min\{m,\ell\}$.*

Proof. Let $r \in \{0,1,\dots,\min\{m,\ell\}\}$ be given. Then

$$\begin{aligned} \overline{\Lambda}_r^{n,m,\ell}(k) &= \frac{1}{\|J_r^{n,m,\ell}\|_1} \Lambda_r^{n,m,\ell}(k) \\ &= \frac{1}{\|J_r^{n,m,\ell}\|_1} \sum_{i=0}^{k} (-1)^i \binom{k}{i}_q q^{\binom{i}{2}+(m-r)(\ell-r-i)} \binom{n-m-i}{\ell-r-i}_q \binom{m-k+i}{r-k+i}_q \\ &= \binom{n}{m}_q^{-1} \sum_{i=0}^{k} (-1)^i \binom{k}{i}_q \frac{q^{\binom{i}{2}+(m-r)(\ell-r-i)}}{q^{(m-r)(\ell-r)}} \cdot \frac{\binom{n-m-i}{\ell-r-i}_q}{\binom{n-m}{\ell-r}_q} \cdot \frac{\binom{m-k+i}{r-k+i}_q}{\binom{m}{r}_q}, \end{aligned} \tag{5.44}$$

where the first step restates Definition 5.27, the second step applies Definition 5.15, and the final step uses Proposition 5.17. To simplify (5.44), observe that

$$\frac{\binom{n-m-i}{\ell-r-i}_q}{\binom{n-m}{\ell-r}_q} = \frac{q^{\ell-r}-1}{q^{n-m}-1} \cdot \frac{q^{\ell-r}-q}{q^{n-m}-q} \cdot \cdots \cdot \frac{q^{\ell-r}-q^{i-1}}{q^{n-m}-q^{i-1}}. \tag{5.45}$$

Indeed, if $\ell - r - i < 0$, then the left-hand side is zero by definition, and the right-hand side also evaluates to zero. In the complementary case $\ell - r - i \geqslant 0$, one obtains (5.45) directly from the definition of Gaussian binomial coefficients. One analogously verifies that

$$\frac{\binom{m-k+i}{r-k+i}_q}{\binom{m}{r}_q} = \frac{q^r-1}{q^m-1} \cdot \frac{q^r-q}{q^m-q} \cdot \cdots \cdot \frac{q^r-q^{k-i-1}}{q^m-q^{k-i-1}}, \tag{5.46}$$

by considering the cases $r - k + i < 0$ and $r - k + i \geqslant 0$. Substituting (5.45) and (5.46) into (5.44) gives

$$\begin{aligned} \overline{\Lambda}_r^{n,m,\ell}(k) = \binom{n}{m}_q^{-1} \sum_{i=0}^{k} (-1)^i \binom{k}{i}_q q^{\binom{i}{2}-(m-r)i} \cdot \frac{q^{\ell-r}-1}{q^{n-m}-1} \cdot \frac{q^{\ell-r}-q}{q^{n-m}-q} \cdot \cdots \cdot \frac{q^{\ell-r}-q^{i-1}}{q^{n-m}-q^{i-1}} \\ \times \frac{q^r-1}{q^m-1} \cdot \frac{q^r-q}{q^m-q} \cdot \cdots \cdot \frac{q^r-q^{k-i-1}}{q^m-q^{k-i-1}}. \end{aligned} \tag{5.47}$$

To verify the algebraic property (i), rewrite (5.47) to obtain

$$\overline{\Lambda}_r^{n,m,\ell}(k) = \binom{n}{m}_q^{-1} \sum_{i=0}^{k} (-1)^i \binom{k}{i}_q q^{\binom{i}{2}-mi} \cdot \frac{q^\ell - q^r}{q^{n-m}-1} \cdot \frac{q^\ell - q^{r+1}}{q^{n-m}-q} \cdot \cdots \cdot \frac{q^\ell - q^{r+i-1}}{q^{n-m}-q^{i-1}} \\ \times \frac{q^r-1}{q^m-1} \cdot \frac{q^r-q}{q^m-q} \cdot \cdots \cdot \frac{q^r-q^{k-i-1}}{q^m-q^{k-i-1}}.$$

The i-th summand in this expression is, for fixed values of n, m, ℓ, k, clearly a polynomial in q^r of degree at most $i + (k-i) = k$. This settles (i).

We now turn to the analytic property, (ii). Dropping the zero terms from the summation in (5.47), and applying the triangle inequality,

$$|\overline{\Lambda}_r^{n,m,\ell}(k)| \leqslant \binom{n}{m}_q^{-1} \sum_{i=\max\{0,k-r\}}^{\min\{k,\ell-r\}} \binom{k}{i}_q q^{\binom{i}{2}-(m-r)i} \cdot \frac{q^{\ell-r}-1}{q^{n-m}-1} \cdot \frac{q^{\ell-r}-q}{q^{n-m}-q} \cdot \cdots \cdot \frac{q^{\ell-r}-q^{i-1}}{q^{n-m}-q^{i-1}} \\ \times \frac{q^r-1}{q^m-1} \cdot \frac{q^r-q}{q^m-q} \cdot \cdots \cdot \frac{q^r-q^{k-i-1}}{q^m-q^{k-i-1}}.$$

The first i fractions on the right-hand side are each bounded by $q^{\ell-r}/q^{n-m}$, whereas the other $k-i$ fractions are each bounded by q^r/q^m. Using these estimates leads to

$$\begin{aligned} |\overline{\Lambda}_r^{n,m,\ell}(k)| &\leqslant \binom{n}{m}_q^{-1} \sum_{i=\max\{0,k-r\}}^{\min\{k,\ell-r\}} \binom{k}{i}_q q^{\binom{i}{2}-(m-r)i} \cdot q^{(\ell-r-n+m)i} \cdot q^{-(m-r)(k-i)} \\ &\leqslant \binom{n}{m}_q^{-1} \sum_{i=\max\{0,k-r\}}^{\min\{k,\ell-r\}} 4q^{i(k-i)+\binom{i}{2}-(m-r)i+(\ell-r-n+m)i-(m-r)(k-i)} \\ &\leqslant \binom{n}{m}_q^{-1} \sum_{i=\max\{0,k-r\}}^{\min\{k,\ell-r\}} 4q^{i(k-i)+\binom{i}{2}-(m-r)i-ri-(m-r)(k-i)} \\ &= \binom{n}{m}_q^{-1} \sum_{i=\max\{0,k-r\}}^{\min\{k,\ell-r\}} 4q^{i(k-r-i)+\binom{i}{2}-k(m-r)}, \end{aligned} \tag{5.48}$$

where the second step uses Corollary 2.14, and the third step is valid since $n \geqslant m+\ell$ by hypothesis. Let $A(i)$ denote the exponent of q in (5.48). Then $A(i)$ is an integer-valued function of i that strictly decreases on $[k-r, \infty)$. As a result, (5.48) yields

$$\begin{aligned} |\overline{\Lambda}_r^{n,m,\ell}(k)| &\leqslant \binom{n}{m}_q^{-1} \sum_{t=0}^{\infty} 4q^{A(\max\{0,k-r\})-t} \\ &\leqslant 8\binom{n}{m}_q^{-1} q^{A(\max\{0,k-r\})}, \end{aligned}$$

where the second step uses a geometric series along with $q \geqslant 2$. Therefore, the proof of (ii) will be complete once we show that

$$A(\max\{0, k-r\}) \leqslant -\frac{k(m-r)}{2}. \tag{5.49}$$

There are two cases to consider. If $k \leqslant r$, then $A(\max\{0,k-r\}) = A(0) = -k(m-r) \leqslant -k(m-r)/2$, where the last step uses the hypothesis that $r \leqslant m$. If $k > r$, then $A(\max\{0,k-r\}) = A(k-r) = \binom{k-r}{2} - k(m-r) \leqslant k(k-r)/2 - k(m-r) \leqslant -k(m-r)/2$, where the last step uses the hypothesis that $k \leqslant m$. This settles (5.49) and completes the proof of the lemma. □

5.6. Approximate trace norm of the subspace problem. We have reached a pivotal point in our study of the subspace intersection problem, where we analyze the approximate trace norm of its characteristic matrix. As in our analysis of the rank problem (Section 3), we start by constructing a suitable univariate dual object.

LEMMA 5.30. *Let Δ, R, d_1, d_2 be nonnegative integers with $0 < R \leqslant \Delta - d_1 - d_2$. Then there is a function $\psi\colon \{0, 1, \ldots, \Delta\} \to \mathbb{R}$ such that:*

(i) $\psi(0) = -1$;
(ii) $\psi(R) > 0$;
(iii) $\psi(r) = 0$ for $r \in \{0, 1, \ldots, \Delta\} \setminus (\{R + d_1 + 1, R + d_1 + 2, \ldots, \Delta - d_2\} \cup \{0, R\})$;
(iv) $\sum_{r=0}^{\Delta} \psi(r)\xi(q^r) = 0$ for every polynomial ξ of degree at most $\Delta - R - d_1 - d_2$;
(v) $\sum_{r \in \{0,\ldots,\Delta\} \setminus \{0,R\}} |\psi(r)| \leqslant 32q^{-d_1-1}$.

Proof. By hypothesis, $d_1 + d_2 \leqslant \Delta - R < \Delta$. As a result, we may invoke Lemma 3.9 with parameters n, k, ℓ, m set to $\Delta, \Delta - R, d_2, d_1$, respectively, to obtain a function $\varphi\colon \{0, 1, \ldots, \Delta\} \to \mathbb{R}$ such that:

(i′) $\varphi(\Delta) = 1$;
(ii′) $\varphi(\Delta - R) < 0$;
(iii′) $\varphi(r) = 0$ for $r \in \{0, 1, \ldots, \Delta\} \setminus (\{d_2, d_2 + 1, \ldots, \Delta - R - d_1 - 1\} \cup \{\Delta - R, \Delta\})$;
(iv′) $\sum_{r=0}^{\Delta} \varphi(r)\xi(q^{-r}) = 0$ for every polynomial ξ of degree at most $\Delta - R - d_1 - d_2$;
(v′) $\sum_{r \in \{0,\ldots,\Delta\} \setminus \{\Delta-R,\Delta\}} |\varphi(r)| \leqslant 32q^{-d_1-1}$.

Define $\psi\colon \{0, 1, \ldots, \Delta\} \to \mathbb{R}$ by $\psi(r) = -\varphi(\Delta - r)$. Then (i), (ii), (iii), and (v) are immediate from (i′), (ii′), (iii′), and (v′), respectively. The remaining item (iv) follows from (iv′) via

$$\sum_{r=0}^{\Delta} \psi(r)\xi(q^r) = -\sum_{r=0}^{\Delta} \varphi(\Delta - r)\xi(q^{r-\Delta} \cdot q^{\Delta}) = -\sum_{i=0}^{\Delta} \varphi(i)\xi(q^{-i} \cdot q^{\Delta}) = 0. \qquad \square$$

With the univariate dual object ψ now constructed, we will use the associated subspace matrix $\Phi = \overline{J}_{\psi}^{n,m,\ell}$ as a dual witness to prove our sought lower bound on the approximate trace norm. The theorem below only treats a canonical case of the subspace intersection problem. However, we will see shortly that this result allows us to tackle all parameter settings.

THEOREM 5.31. *Let n, m, ℓ, R be given integers with $0 < R \leqslant \min\{m, \ell\}$ and $m + \ell \leqslant n$. Let F be the characteristic matrix of* $\mathrm{INTERSECT}_{0,R}^{\mathbb{F}_q,n,m,\ell}$. *Then for all reals $\delta \geqslant 0$ and all nonnegative integers d_1, d_2 with $d_1 + d_2 \leqslant \min\{m, \ell\} - R$,*

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1}{8}\left(1 - \delta - \frac{64}{q^{d_1+1}}\right)\binom{n}{m}_q^{1/2}\binom{n}{\ell}_q^{1/2} q^{(\min\{m,\ell\}-R-d_1-d_2+1)(m+\ell-2\min\{m,\ell\}+2d_2)/4}, \tag{5.50}$$

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1-\delta}{8}\binom{n}{m}_q^{1/2}\binom{n}{\ell}_q^{1/2} q^{(m+\ell-2R)/4}. \tag{5.51}$$

Proof. Structurally, the proof is similar to that of Theorem 3.14. Let $\Delta = \min\{m, \ell\}$. Then $0 < R \leqslant \Delta - d_1 - d_2$ by hypothesis. Let $\psi\colon \{0, 1, \ldots, \Delta\} \to \mathbb{R}$ be the function constructed in Lemma 5.30,

and extend ψ to all of $\mathbb{Z}$ by defining $\psi(r) = 0$ for $r \notin \{0, 1, \ldots, \Delta\}$. Then

$$\begin{aligned}
&\sum_{\operatorname{dom} F} F_{S,T}(\overline{J}_\psi^{n,m,\ell})_{S,T} - \delta\|\overline{J}_\psi^{n,m,\ell}\|_1 - \sum_{\overline{\operatorname{dom} F}} |(\overline{J}_\psi^{n,m,\ell})_{S,T}| \\
&\qquad = -\sum_{\dim(S\cap T)=0} (\overline{J}_\psi^{n,m,\ell})_{S,T} + \sum_{\dim(S\cap T)=R} (\overline{J}_\psi^{n,m,\ell})_{S,T} - \delta\|\overline{J}_\psi^{n,m,\ell}\|_1 \\
&\qquad\qquad - \sum_{\dim(S\cap T)\notin\{0,R\}} |(\overline{J}_\psi^{n,m,\ell})_{S,T}| \\
&\qquad = -\psi(0) + \psi(R) - \delta\|\psi\|_1 - \sum_{r\notin\{0,R\}} |\psi(r)| \\
&\qquad = |\psi(0)| + |\psi(R)| - \delta\|\psi\|_1 - \sum_{r\notin\{0,R\}} |\psi(r)| \\
&\qquad = (1-\delta)\|\psi\|_1 - 2\sum_{r\notin\{0,R\}} |\psi(r)| \\
&\qquad \geqslant \left(1 - \delta - 2\sum_{r\notin\{0,R\}} |\psi(r)|\right)\|\psi\|_1, \qquad (5.52)
\end{aligned}$$

where the second step uses Lemma 5.26, the third step is valid by Lemma 5.30(i)–(ii), and the fifth step is justified by Lemma 5.30(i).

We now analyze the spectral norm of $\overline{J}_\psi^{n,m,\ell}$. Recall from Lemma 5.29(i) that for fixed n, m, ℓ and fixed $k \in \{0, 1, \ldots, \Delta\}$, the quantity $\overline{\Lambda}_r^{n,m,\ell}(k)$ as a function of $r \in \{0, 1, \ldots, \Delta\}$ is a polynomial in q^r of degree at most k. As a result,

$$\begin{aligned}
&\max_{k\in\{0,1,\ldots,\Delta-R-d_1-d_2\}} \sqrt{\overline{\Lambda}_\psi^{n,m,\ell}(k)\,\overline{\Lambda}_\psi^{n,\ell,m}(k)} \\
&\qquad = \max_{k\in\{0,1,\ldots,\Delta-R-d_1-d_2\}} \sqrt{\overline{\Lambda}_\psi^{n,\ell,m}(k) \cdot \sum_{r=0}^{\Delta} \psi(r)\overline{\Lambda}_r^{n,m,\ell}(k)} \\
&\qquad = \max_{k\in\{0,1,\ldots,\Delta-R-d_1-d_2\}} \sqrt{\overline{\Lambda}_\psi^{n,\ell,m}(k) \cdot 0} \\
&\qquad = 0, \qquad (5.53)
\end{aligned}$$

where the first step applies Definition 5.27, and the second step uses Lemma 5.30(iv). Next, for all $k \in \{0, 1, \ldots, \Delta\}$,

$$\begin{aligned}
|\overline{\Lambda}_\psi^{n,m,\ell}(k)\,\overline{\Lambda}_\psi^{n,\ell,m}(k)| &= \left|\sum_{r=0}^{\Delta} \psi(r)\overline{\Lambda}_r^{n,m,\ell}(k)\right| \cdot \left|\sum_{r=0}^{\Delta} \psi(r)\overline{\Lambda}_r^{n,\ell,m}(k)\right| \\
&= \left|\sum_{r=0}^{\Delta-d_2} \psi(r)\overline{\Lambda}_r^{n,m,\ell}(k)\right| \cdot \left|\sum_{r=0}^{\Delta-d_2} \psi(r)\overline{\Lambda}_r^{n,\ell,m}(k)\right| \\
&\leqslant \|\psi\|_1 \max_{r=0,1,\ldots,\Delta-d_2} |\overline{\Lambda}_r^{n,m,\ell}(k)| \cdot \|\psi\|_1 \max_{r=0,1,\ldots,\Delta-d_2} |\overline{\Lambda}_r^{n,\ell,m}(k)| \\
&\leqslant \|\psi\|_1^2 \cdot 8\binom{n}{m}_q^{-1} q^{-k(m-\Delta+d_2)/2} \cdot 8\binom{n}{\ell}_q^{-1} q^{-k(\ell-\Delta+d_2)/2},
\end{aligned}$$

where the first step applies Definition 5.27, the second step uses Lemma 5.30(iii), and the last step invokes Lemma 5.29(ii) to bound $\overline{\Lambda}_r^{n,m,\ell}(k)$ and then again (with the roles of m and ℓ interchanged) to bound $\overline{\Lambda}_r^{n,\ell,m}(k)$. It follows that

$$\begin{aligned}
&\max_{k\in\{\Delta-R-d_1-d_2+1,\ldots,\Delta-1,\Delta\}} \sqrt{\overline{\Lambda}_\psi^{n,m,\ell}(k)\,\overline{\Lambda}_\psi^{n,\ell,m}(k)} \\
&\qquad \leqslant \max_{k\in\{\Delta-R-d_1-d_2+1,\ldots,\Delta-1,\Delta\}} 8\|\psi\|_1 \left(\binom{n}{m}_q \binom{n}{\ell}_q q^{k(m-\Delta+d_2)/2} q^{k(\ell-\Delta+d_2)/2} \right)^{-1/2} \\
&\qquad = 8\|\psi\|_1 \left(\binom{n}{m}_q \binom{n}{\ell}_q q^{(\Delta-R-d_1-d_2+1)(m+\ell-2\Delta+2d_2)/2} \right)^{-1/2}. \qquad (5.54)
\end{aligned}$$

As a result,

$$\begin{aligned}
\|\overline{J}_\psi^{n,m,\ell}\| &= \max_{k\in\{0,1,\ldots,\Delta\}} \sqrt{\overline{\Lambda}_\psi^{n,m,\ell}(k)\,\overline{\Lambda}_\psi^{n,\ell,m}(k)} \\
&\leqslant 8\|\psi\|_1 \left(\binom{n}{m}_q \binom{n}{\ell}_q q^{(\Delta-R-d_1-d_2+1)(m+\ell-2\Delta+2d_2)/2} \right)^{-1/2}, \qquad (5.55)
\end{aligned}$$

where the first step appeals to Theorem 5.28, and the second step substitutes the upper bounds from (5.53) and (5.54).

We are now in a position to complete the proof of the theorem. Proposition 2.9 with $\Phi = \overline{J}_\psi^{n,m,\ell}$ implies, in view of (5.52) and (5.55), that

$$\|F\|_{\Sigma,\delta} \geqslant \frac{1}{8} \left(1 - \delta - 2 \sum_{r\notin\{0,R\}} |\psi(r)| \right) \binom{n}{m}_q^{1/2} \binom{n}{\ell}_q^{1/2} q^{(\Delta-R-d_1-d_2+1)(m+\ell-2\Delta+2d_2)/4}.$$

Since $\sum_{r\notin\{0,R\}} |\psi(r)| \leqslant 32q^{-d_1-1}$ by Lemma 5.30(v), this settles (5.50). In the special case $d_1 = 0$ and $d_2 = \Delta - R$, we have $\sum_{r\notin\{0,R\}} |\psi(r)| = 0$ from Lemma 5.30(iii), whence (5.51). ∎

5.7. Communication lower bounds. We will now prove an optimal lower bound on the communication complexity of the subspace intersection problem. To simplify the exposition, we will first consider the canonical case where Alice and Bob need to determine whether the intersection of their subspaces has dimension 0 versus dimension R, corresponding to the approximate trace norm result that we just obtained. The general lower bound for all parameter settings will then follow using the reduction of Proposition 2.26.

LEMMA 5.32. *Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements. Let n, m, ℓ, R be nonnegative integers with*

$$0 < R \leqslant \min\{m, \ell\}, \qquad (5.56)$$

$$R < \max\{m, \ell\}, \qquad (5.57)$$

$$m + \ell \leqslant n. \qquad (5.58)$$

Then

$$Q^*_{(1-\gamma)/2}(\text{INTERSECT}_{0,R}^{\mathbb{F},n,m,\ell}) \geqslant c(\log_q\lceil q^{m-R}\gamma\rceil + 1)(\log_q\lceil q^{\ell-R}\gamma\rceil + 1)\log q \qquad (5.59)$$

for all $\gamma \in [\frac{1}{3}q^{-(m+\ell-2R)/5}, 1]$, where $c > 0$ is an absolute constant independent of $\mathbb{F}, n, m, \ell, R, \gamma$.

Proof. Due to the symmetry between m and ℓ in the statement of the lemma, we may assume that

$$m \geqslant \ell, \qquad (5.60)$$

corresponding to the mnemonic "m for more, ℓ for less." The hypotheses (5.58) ensures that there is a pair of subspaces in $\mathscr{S}(\mathbb{F}^n, m) \times \mathscr{S}(\mathbb{F}^n, \ell)$ whose intersection has dimension 0; analogously, (5.56) and (5.58) ensure that there is a pair of subspaces in $\mathscr{S}(\mathbb{F}^n, m) \times \mathscr{S}(\mathbb{F}^n, \ell)$ whose intersection has dimension R. This makes $\mathrm{INTERSECT}_{0,R}^{\mathbb{F},n,m,\ell}$ a nonconstant function, with the trivial lower bound

$$Q^*_{(1-\gamma)/2}(\mathrm{INTERSECT}_{0,R}^{\mathbb{F},n,m,\ell}) \geqslant 1. \tag{5.61}$$

It suffices to prove that the characteristic matrix F of this communication problem satisfies

$$\|F\|_{\Sigma,1-\gamma} \geqslant c' \binom{n}{m}_q^{1/2} \binom{n}{\ell}_q^{1/2} q^{c'(\log_q \lceil q^{m-R}\gamma \rceil + 1)(\log_q \lceil q^{\ell-R}\gamma \rceil + 1)} \tag{5.62}$$

for some absolute constant $c' > 0$. Indeed, once this lower bound is established, an appeal to Theorem 2.23 yields

$$\begin{aligned} Q^*_{(1-\gamma)/2}&(\mathrm{INTERSECT}_{0,R}^{\mathbb{F},n,m,\ell}) \\ &\geqslant \frac{1}{2} \log \frac{c' q^{c'(\log_q \lceil q^{m-R}\gamma \rceil + 1)(\log_q \lceil q^{\ell-R}\gamma \rceil + 1)}}{3} \\ &= \frac{c'}{2} (\log_q \lceil q^{m-R}\gamma \rceil + 1)(\log_q \lceil q^{\ell-R}\gamma \rceil + 1) \log q - \frac{1}{2} \log \frac{3}{c'}. \end{aligned} \tag{5.63}$$

Taking a weighted arithmetic average of (5.61) and (5.63) settles (5.59).

In what follows, we prove (5.62). We first examine the case $\gamma \leqslant q^{-\ell+R+23}$. Equation (5.51) of Theorem 5.31 yields

$$\begin{aligned} \|F\|_{\Sigma,1-\gamma} &\geqslant \frac{\gamma}{8} \binom{n}{m}_q^{1/2} \binom{n}{\ell}_q^{1/2} q^{(m+\ell-2R)/4} \\ &\geqslant \frac{1}{24} \binom{n}{m}_q^{1/2} \binom{n}{\ell}_q^{1/2} q^{(m+\ell-2R)/20}, \end{aligned} \tag{5.64}$$

where the second step uses the lemma hypothesis that $\gamma \geqslant \frac{1}{3} q^{-(m+\ell-2R)/5}$. Moreover,

$$\begin{aligned} m + \ell - 2R &\geqslant m - R \\ &\geqslant \frac{1}{2}(m - R + 1) \\ &\geqslant \frac{1}{2}(m - R + 1) \cdot \frac{1}{24}(\log_q \lceil q^{\ell-R}\gamma \rceil + 1) \\ &\geqslant \frac{1}{48}(\log_q \lceil q^{m-R}\gamma \rceil + 1)(\log_q \lceil q^{\ell-R}\gamma \rceil + 1), \end{aligned} \tag{5.65}$$

where the first step uses (5.56), the second step is valid by (5.57) and (5.60), the third step is legitimate because $\gamma \leqslant q^{-\ell+R+23}$ in the case under consideration, and the last step uses the lemma hypothesis that $\gamma \leqslant 1$. Equations (5.64) and (5.65) imply (5.62) for $c' = 1/960$.

We now examine the complementary case, $\gamma \geqslant q^{-\ell+R+23}$. This assumption on γ, along with the lemma hypothesis that $\gamma \leqslant 1$, implies that the integer $d_1 = \lfloor \log_q(128/\gamma) \rfloor$ is an element of $\{0, 1, 2, \ldots, \ell - R\}$. This in turn means that the integer $d_2 = \lceil (\ell - R - d_1)/2 \rceil$ is also an element of $\{0, 1, 2, \ldots, \ell - R\}$. We have $d_1 + d_2 = d_1 + \lceil (\ell - R - d_1)/2 \rceil \leqslant d_1 + (\ell - R - d_1) = \ell - R = \min\{m, \ell\} - R$, where the last step uses (5.60). As a result, Theorem 5.31 is applicable with parameters d_1 and d_2,

and equation (5.50) yields

$$\begin{aligned}
\|F\|_{\Sigma,1-\gamma} &\geqslant \frac{1}{8}\left(\gamma - \frac{64}{q^{d_1+1}}\right)\binom{n}{m}_q^{1/2}\binom{n}{\ell}_q^{1/2} q^{(\min\{m,\ell\}-R-d_1-d_2+1)(m+\ell-2\min\{m,\ell\}+2d_2)/4} \\
&\geqslant \frac{1}{8}\left(\gamma - \frac{64}{q^{d_1+1}}\right)\binom{n}{m}_q^{1/2}\binom{n}{\ell}_q^{1/2} q^{(\ell-R-d_1-d_2+1)(m-\ell+2d_2)/4} \\
&\geqslant \frac{\gamma}{16}\binom{n}{m}_q^{1/2}\binom{n}{\ell}_q^{1/2} q^{(\ell-R-d_1-d_2+1)(m-\ell+2d_2)/4} \\
&\geqslant \frac{\gamma}{16}\binom{n}{m}_q^{1/2}\binom{n}{\ell}_q^{1/2} q^{(\ell-R-d_1)(m-R-d_1)/8} \\
&= \frac{1}{16}\binom{n}{m}_q^{1/2}\binom{n}{\ell}_q^{1/2} q^{(\ell-R-\lfloor\log_q(128/\gamma)\rfloor)(m-R-\lfloor\log_q(128/\gamma)\rfloor)/8-\log_q(1/\gamma)}, \qquad (5.66)
\end{aligned}$$

where the second step applies (5.60), the third and fifth steps use the definition of d_1, and the fourth step uses the definition of d_2. Recall that $\gamma \geqslant q^{-\ell+R+23}$ in the case under consideration, and $\gamma \in [\frac{1}{3}q^{-(m+\ell-2R)/5}, 1]$ by the lemma hypothesis. We may therefore use Claim 5.33, stated and proved below, to simplify to the right-hand side of (5.66) as follows:

$$\|F\|_{\Sigma,1-\gamma} \geqslant \frac{1}{16}\binom{n}{m}_q^{1/2}\binom{n}{\ell}_q^{1/2} q^{(\log_q\lceil q^{m-R}\gamma\rceil+1)(\log_q\lceil q^{\ell-R}\gamma\rceil+1)/160}.$$

This establishes (5.62) with $c' = 1/160$, completing the proof of the lemma. □

Claim 5.33. *For any γ with $\max\{q^{-\ell+R+23}, \frac{1}{3}q^{-(m+\ell-2R)/5}\} \leqslant \gamma \leqslant 1$,*

$$\begin{aligned}
&\frac{1}{8}\left(\ell - R - \left\lfloor\log_q\frac{128}{\gamma}\right\rfloor\right)\left(m - R - \left\lfloor\log_q\frac{128}{\gamma}\right\rfloor\right) - \log_q\frac{1}{\gamma} \\
&\qquad\qquad \geqslant \frac{1}{160}(\log_q\lceil q^{m-R}\gamma\rceil + 1)(\log_q\lceil q^{\ell-R}\gamma\rceil + 1). \qquad (5.67)
\end{aligned}$$

Proof. The proof is somewhat tedious but straightforward. To begin with,

$$\begin{aligned}
&\frac{1}{8}\left(\ell - R - \left\lfloor\log_q\frac{128}{\gamma}\right\rfloor\right)\left(m - R - \left\lfloor\log_q\frac{128}{\gamma}\right\rfloor\right) - \log_q\frac{1}{\gamma} \\
&\qquad = \frac{1}{8}\left\lceil\log_q\frac{q^{\ell-R}\gamma}{128}\right\rceil\left(m - R - \left\lfloor\log_q\frac{128}{\gamma}\right\rfloor\right) - \log_q\frac{1}{\gamma} \\
&\qquad \geqslant \frac{1}{8}\left\lceil\log_q\frac{q^{\ell-R}\gamma}{128}\right\rceil\left(m - R - \left\lfloor\log_q\frac{128}{\gamma}\right\rfloor - \frac{1}{2}\log_q\frac{1}{\gamma}\right), \qquad (5.68)
\end{aligned}$$

where the last step uses the fact that $\frac{1}{8}\lceil\log_q(q^{\ell-R}\gamma/128)\rceil \geqslant 2$ due to the hypothesis $\gamma \geqslant q^{-\ell+R+23}$. We now bound from below the factors in (5.68). We have

$$\log_q\frac{q^{\ell-R}\gamma}{128} \geqslant \log_q\frac{q^{\ell-R}\gamma}{q^7} \geqslant \log_q\frac{\lceil q^{\ell-R}\gamma\rceil}{q^8} = \log_q\lceil q^{\ell-R}\gamma\rceil - 8 \geqslant \frac{1}{2}(\log_q\lceil q^{\ell-R}\gamma\rceil + 1), \quad (5.69)$$

where the second and fourth steps are valid because $q^{\ell-R}\gamma \geqslant q^{23}$ by hypothesis. The other factor in (5.68) can be bounded as follows:

$$\begin{aligned}
m - R - \left\lfloor \log_q \frac{128}{\gamma} \right\rfloor - \frac{1}{2}\log_q \frac{1}{\gamma} &\geqslant m - R - \log_q \frac{q^7}{\gamma^{3/2}} \\
&\geqslant m - R - \log_q \frac{q^7}{(\max\{q^{-\ell+R+23}, \frac{1}{3}q^{-(m+\ell-2R)/5}\})^{3/2}} \\
&\geqslant m - R - 7 - \frac{3}{2}\min\left\{\ell - R - 23, \frac{1}{5}(m+\ell-2R)+2\right\} \\
&\geqslant m - R - 7 - \frac{3}{2}\min\left\{m - R - 23, \frac{2}{5}(m-R)+2\right\} \\
&\geqslant m - R - 7 - \frac{3}{2}\left(\frac{1}{3}(m-R-23) + \frac{2}{3}\left(\frac{2}{5}(m-R)+2\right)\right) \\
&= \frac{1}{10}(m-R) + \frac{5}{2} \\
&\geqslant \frac{1}{10}(\log_q \lceil q^{m-R}\gamma \rceil + 1), \qquad (5.70)
\end{aligned}$$

where the first step applies the bound $128 \leqslant q^7$ and drops the floor operator, the second step uses the hypothesis for γ, the fourth step is valid by (5.60), the fifth step replaces the minimum by a weighted average, and the last step is legitimate because $\gamma \leqslant 1$ by hypothesis. Now (5.67) follows from (5.68)–(5.70). □

We now extend the previous lemma to all possible parameter settings, thus obtaining the desired communication lower bound for subspace intersection.

THEOREM 5.34. *Let $c > 0$ be the absolute constant from Lemma 5.32. Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements, and let n, m, ℓ, r, R be integers with $\max\{0, m+\ell-n\} \leqslant r < R \leqslant \min\{m, \ell\}$. Then $\max\{m, \ell\} \leqslant n$. Furthermore, for all $\gamma \in [\frac{1}{3}q^{-(m+\ell-2R)/5}, 1]$,*

$$Q^*_{\frac{1-\gamma}{2}}(\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{r,R}) \geqslant \begin{cases} 1 & \text{if } R = m = \ell, \\ c(\log_q \lceil q^{m-R}\gamma \rceil + 1)(\log_q \lceil q^{\ell-R}\gamma \rceil + 1)\log q & \text{otherwise.} \end{cases}$$

Proof. The hypothesis $\max\{0, m+\ell-n\} \leqslant r < R \leqslant \min\{m, \ell\}$ implies that $m+\ell-n \leqslant \min\{m, \ell\}$, which is equivalent to $\max\{m, \ell\} \leqslant n$.

Recall from Proposition 2.25 that for each integer $d \in [\max\{0, m+\ell-n\}, \min\{m, \ell\}]$, there are subspaces $S \in \mathscr{S}(\mathbb{F}^n, m)$ and $T \in \mathscr{S}(\mathbb{F}^n, \ell)$ with $\dim(S \cap T) = d$. This makes $\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{r,R}$ a nonconstant function, which means that its ε-error quantum communication complexity for each $\varepsilon \in [0, 1/2)$ is at least 1 bit. This settles the claimed communication lower bounds in the case $R = m = \ell$.

In what follows, we focus on the complementary case when R, m, ℓ are not all equal. In view of $R \leqslant \min\{m, \ell\}$, we infer that $R < \max\{m, \ell\}$. This new inequality, and the theorem hypotheses that $m + \ell - n \leqslant r < R \leqslant \min\{m, \ell\}$ and $\gamma \in [\frac{1}{3}q^{-(m+\ell-2R)/5}, 1]$, can be equivalently stated as

$$R - r < \max\{m - r, \ell - r\}, \qquad (5.71)$$

$$0 < R - r \leqslant \min\{m - r, \ell - r\}, \qquad (5.72)$$

$$(m - r) + (\ell - r) \leqslant n - r, \qquad (5.73)$$

$$\gamma \in [\tfrac{1}{3}q^{-((m-r)+(\ell-r)-2(R-r))/5}, 1]. \qquad (5.74)$$

Now

$$Q^*_{(1-\gamma)/2}(\mathrm{INTERSECT}^{\mathbb{F},n,m,\ell}_{r,R}) \geqslant Q^*_{(1-\gamma)/2}(\mathrm{INTERSECT}^{\mathbb{F},n-r,m-r,\ell-r}_{0,R-r}) \\ \geqslant c(\log_q\lceil q^{m-R}\gamma\rceil+1)(\log_q\lceil q^{\ell-R}\gamma\rceil+1)\log q, \tag{5.75}$$

where the first step uses Proposition 2.26, and the second step is valid by Lemma 5.32 whose application is in turn justified by (5.71)–(5.74). □

Theorem 5.34 settles the *quantum* communication lower bound of Theorem 1.10 for the *promise* subspace intersection problem, and hence also the *randomized* communication lower bound for the *total* subspace intersection problem.

5.8. Communication upper bounds for small error. In this section and the next, we prove communication upper bounds matching our lower bound for the subspace intersection problem. We start with a technical lemma.

LEMMA 5.35. *Let n, m, ℓ, r, Δ be nonnegative integers with $r \leqslant \min\{m, \ell\}$ and $\max\{m, \ell\} \leqslant n$. Fix a finite field $\mathbb{F}$, and let $S \in \mathscr{S}(\mathbb{F}^n, m)$ and $T \in \mathscr{S}(\mathbb{F}^n, \ell)$ be given subspaces. Let $X \in \mathbb{F}^{(m+\ell-r+\Delta)\times n}$ and $Y \in \mathbb{F}^{(m+\ell-2r+3\Delta)\times(m+\ell-r+\Delta)}$ be uniformly random matrices. Then with probability at least $1 - 16|\mathbb{F}|^{-\Delta-1}$, one has*

$$\dim(X(S)) = \dim(S), \tag{5.76}$$
$$\dim(X(T)) = \dim(T), \tag{5.77}$$
$$\dim(Y((X(S))^\perp)) = \dim((X(S))^\perp), \tag{5.78}$$
$$\dim(Y((X(T))^\perp)) = \dim((X(T))^\perp). \tag{5.79}$$

Assuming (5.76)–(5.79)*, the subspaces $S' = Y((X(S))^\perp)$ and $T' = Y((X(T))^\perp)$ satisfy*

$$\dim(S') = \ell - r + \Delta, \tag{5.80}$$
$$\dim(T') = m - r + \Delta, \tag{5.81}$$
$$\dim(S' \cap T') = m + \ell - r + \Delta - \dim(X(S+T)) \\ + \dim((X(S))^\perp + (X(T))^\perp) - \dim(Y((X(S))^\perp + (X(T))^\perp)). \tag{5.82}$$

Proof. Abbreviate $q = |\mathbb{F}|$. Let E_1, E_2, E_3, E_4 be the events that correspond to (5.76)–(5.79), respectively. Applying Lemma 2.20 with $t = m - 1$ and $d = m + \ell - r + \Delta$ gives

$$\mathbf{P}[\neg E_1] \leqslant 4q^{-(\ell-r+\Delta+1)} \leqslant 4q^{-\Delta-1}. \tag{5.83}$$

Analogously, applying Lemma 2.20 with $t = \ell - 1$ and $d = m + \ell - r + \Delta$ shows that

$$\mathbf{P}[\neg E_2] \leqslant 4q^{-(m-r+\Delta+1)} \leqslant 4q^{-\Delta-1}. \tag{5.84}$$

Conditioned on $E_1 \wedge E_2$, we have

$$\dim((X(S))^\perp) = m + \ell - r + \Delta - \dim(X(S)) = \ell - r + \Delta, \tag{5.85}$$
$$\dim((X(T))^\perp) = m + \ell - r + \Delta - \dim(X(T)) = m - r + \Delta. \tag{5.86}$$

As a result, invoking Lemma 2.20 with $t = \ell - r + \Delta - 1$ and $d = m + \ell - 2r + 3\Delta$ shows that

$$\mathbf{P}[\neg E_3 \mid E_1 \wedge E_2] \leqslant 4q^{-(m+\ell-2r+3\Delta)+(\ell-r+\Delta-1)} \leqslant 4q^{-2\Delta-1}. \tag{5.87}$$

Analogously, invoking Lemma 2.20 with $t = m - r + \Delta - 1$ and $d = m + \ell - 2r + 3\Delta$ shows that

$$\mathbf{P}[\neg E_4 \mid E_1 \wedge E_2] \leqslant 4q^{-(m+\ell-2r+3\Delta)+(m-r+\Delta-1)} \leqslant 4q^{-2\Delta-1}. \tag{5.88}$$

Now

$$\begin{aligned}\mathbf{P}[E_1 \wedge E_2 \wedge E_3 \wedge E_4] &= \mathbf{P}[E_1 \wedge E_2]\,\mathbf{P}[E_3 \wedge E_4 \mid E_1 \wedge E_2] \\ &\geqslant \mathbf{P}[E_1 \wedge E_2] - \mathbf{P}[\neg(E_3 \wedge E_4) \mid E_1 \wedge E_2] \\ &\geqslant 1 - \mathbf{P}[\neg E_1] - \mathbf{P}[\neg E_2] - \mathbf{P}[\neg E_3 \mid E_1 \wedge E_2] - \mathbf{P}[\neg E_4 \mid E_1 \wedge E_2] \\ &\geqslant 1 - 16q^{-\Delta-1},\end{aligned}$$

where the last step uses (5.83)–(5.88). This settles the first part of the lemma.

In what follows, we assume (5.76)–(5.79). Then (5.80) follows from $\dim(S') = \dim((X(S))^\perp) = \ell - r + \Delta$, where the last step uses (5.85). Analogously, (5.81) follows from $\dim(T') = \dim((X(T))^\perp) = m - r + \Delta$, where the last step uses (5.86). Toward the remaining equation (5.82), we have

$$\begin{aligned}\dim((X(S))^\perp + (X(T))^\perp) &= \dim(((X(S)) \cap (X(T)))^\perp) \\ &= m + \ell - r + \Delta - \dim((X(S)) \cap (X(T))) \\ &= m + \ell - r + \Delta - (\dim(X(S)) + \dim(X(T)) - \dim(X(S) + X(T))) \\ &= -r + \Delta + \dim(X(S+T)),\end{aligned}$$

where the first step uses Fact 2.4, and the last step uses (5.76), (5.77), and the linearity of X. With this substitution, (5.82) is equivalent to

$$\dim(S' \cap T') = m + \ell - 2r + 2\Delta - \dim(Y((X(S))^\perp + (X(T))^\perp)). \tag{5.89}$$

Due to (5.80), (5.81), and $Y((X(S))^\perp + (X(T))^\perp) = Y((X(S))^\perp) + Y((X(T))^\perp) = S' + T'$, equation (5.89) is a restatement of $\dim(S' \cap T') = \dim(S') + \dim(T') - \dim(S' + T')$, which is a well-known identity valid for any subspaces S', T'. □

We are now ready to prove our communication upper bound for subspace intersection in the regime where the error probability is a small constant or tends to 0. In the next section, we will generalize this result to the more challenging regime where the error tends to 1/2.

THEOREM 5.36 (Small error). *Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements. Let n, m, ℓ, R be integers with $0 < R \leqslant \min\{m, \ell\}$ and $\max\{m, \ell\} \leqslant n$. Then for each $0 < \varepsilon \leqslant 1/3$,*

$$R_\varepsilon(\mathrm{INTERSECT}_R^{\mathbb{F},n,m,\ell}) = O\left(\left(m - R + \left\lceil \log_q \frac{1}{\varepsilon} \right\rceil\right)\left(\ell - R + \left\lceil \log_q \frac{1}{\varepsilon} \right\rceil\right)\log q\right). \tag{5.90}$$

If in addition $m = \ell = R$, then for each $0 < \varepsilon \leqslant 1/3$,

$$R_\varepsilon(\mathrm{INTERSECT}_R^{\mathbb{F},n,m,\ell}) = O\left(\log \frac{1}{\varepsilon}\right). \tag{5.91}$$

Proof. Define $r = R - 1$. For an integer $\Delta \geqslant 0$ to be set later, consider the following protocol Π. On input a pair of subspaces $S \in \mathscr{S}(\mathbb{F}^n, m)$ for Alice and $T \in \mathscr{S}(\mathbb{F}^n, \ell)$ for Bob, the parties use their shared randomness to pick independent and uniformly random matrices $X \in \mathbb{F}^{(m+\ell-r+\Delta)\times n}$ and $Y \in \mathbb{F}^{(m+\ell-2r+3\Delta)\times(m+\ell-r+\Delta)}$. Next, they verify the four conditions (5.76)–(5.79). This can be done using only two bits of communication, with Alice and Bob verifying the conditions pertaining to their respective inputs. If any of these conditions fail, they output a uniformly random value in $\{-1, 1\}$. In the complementary case, Alice and Bob compute

$$\begin{aligned}S' &= Y((X(S))^\perp), \\ T' &= Y((X(T))^\perp),\end{aligned}$$

respectively. The owner of the smaller of the subspaces S' and T' sends it to the other party in the form of a basis, who then computes $\dim(S' \cap T')$ and outputs 1 if and only if $\dim(S' \cap T') \leqslant \Delta$.

We first analyze the communication cost of Π. If any of the conditions (5.76)–(5.79) fail, the communication cost is 2 bits. If all four conditions hold, then $\dim(S') = \ell - r + \Delta$ and $\dim(T') = m - r + \Delta$ by Lemma 5.35. As a result, a basis for the smaller of the subspaces S' and T' can be communicated using $(m + \ell - 2r + 3\Delta)(\min\{m, \ell\} - r + \Delta)\lceil \log q \rceil$ bits, where the first factor is the dimension of the ambient space. Altogether, the communication cost is at most

$$\begin{aligned} 2 + (2\max\{m, \ell\} - 2r + 3\Delta)(\min\{m, \ell\} - r + \Delta)\lceil \log q \rceil + 1 \\ = O((m - r + \Delta)(\ell - r + \Delta)\log q). \end{aligned} \tag{5.92}$$

We now analyze the correctness probability. To this end, we prove the following claim.

Claim 5.37. *The output of the protocol is correct whenever the matrices X, Y satisfy* (5.76)–(5.79) *as well as the additional conditions*

$$\dim(X(S + T)) \geqslant \min\{\dim(S + T), m + \ell - r\}, \tag{5.93}$$

$$\dim(Y((X(S))^\perp + (X(T))^\perp)) = \dim((X(S))^\perp + (X(T))^\perp). \tag{5.94}$$

Proof. Recall from Lemma 5.35 that (5.76)–(5.79) force (5.82), which in view of (5.94) simplifies to

$$\dim(S' \cap T') = m + \ell - r + \Delta - \dim(X(S + T)). \tag{5.95}$$

We first consider the case $\dim(S \cap T) \leqslant r$. Here $\dim(S + T) \geqslant m + \ell - r$, which along with (5.93) implies that $\dim(X(S + T)) \geqslant m + \ell - r$. Substituting this lower bound into (5.95) gives $\dim(S' \cap T') \leqslant \Delta$. As a result, Π outputs the correct value in this case.

In the complementary case $\dim(S \cap T) \geqslant r + 1$, we have $\dim(S + T) \leqslant m + \ell - r - 1$ and therefore also $\dim(X(S + T)) \leqslant m + \ell - r - 1$. Substituting this upper bound into (5.95) gives $\dim(S' \cap T') \geqslant \Delta + 1$, showing that the output of Π is correct in this case as well. □

Condition (5.93) fails with probability at most $4q^{-\Delta-1}$, by Lemma 2.20 with $d = m + \ell - r + \Delta$ and $t = \min\{\dim(S + T), m + \ell - r\} - 1$. Moreover, conditioned on (5.76) and (5.77), one has

$$\begin{aligned} \dim((X(S))^\perp + (X(T))^\perp) &\leqslant \dim((X(S))^\perp) + \dim((X(T))^\perp) \\ &= 2(m + \ell - r + \Delta) - \dim(X(S)) - \dim(X(T)) \\ &\leqslant m + \ell - 2r + 2\Delta \end{aligned}$$

and hence (5.94) fails with probability at most $4q^{-(m+\ell-2r+3\Delta)+(m+\ell-2r+2\Delta-1)} \leqslant 4q^{-\Delta-1}$, by Lemma 2.20 with $d = m + \ell - 2r + 3\Delta$ and $t = \dim((X(S))^\perp + (X(T))^\perp) - 1$. Since (5.76)–(5.79) are simultaneously true with probability at least $1 - 16q^{-\Delta-1}$ (by Lemma 5.35), we conclude that the six conditions (5.76)–(5.79), (5.93), (5.94) hold simultaneously with probability at least $1 - 16q^{-\Delta-1} - 4q^{-\Delta-1} - 4q^{-\Delta-1} = 1 - 24q^{-\Delta-1}$. Now Claim 5.37 implies that the described protocol Π has error probability at most $24q^{-\Delta-1}$. Since we calculated Π's cost to be (5.92), we conclude that

$$R_{24/q^{\Delta+1}}(\mathrm{INTERSECT}_R^{\mathbb{F},n,m,\ell}) = O((m - r + \Delta)(\ell - r + \Delta)\log q).$$

Taking $\Delta = \lfloor \log_q(24/\varepsilon) \rfloor$ now settles (5.90). For the additional upper bound (5.91), observe that $\mathrm{INTERSECT}_R^{\mathbb{F},n,m,\ell}$ for $m = \ell = R$ is the equality problem with domain $\mathscr{S}(\mathbb{F}^n, m) \times \mathscr{S}(\mathbb{F}^n, m)$. The claimed upper bound now follows because it is well-known [14, Chapter 3.3] that the equality problem over any domain has ε-error randomized communication complexity $O(\log(1/\varepsilon))$. □

5.9. Communication upper bounds for large error. To study the large-error regime, we recall a basic fact on vector spaces.

Proposition 5.38. *Let A, A' be subspaces such that $A' \subseteq A$. Then for any subspace B,*

$$\dim(A \cap B) - \dim(A' \cap B) \leqslant \dim(A) - \dim(A'). \tag{5.96}$$

Proof. Since $A \cap B + A'$ is a subspace of A, we have $\dim(A \cap B + A') \leqslant \dim(A)$. Expanding the left-hand side yields $\dim(A \cap B) + \dim(A') - \dim(A \cap B \cap A') \leqslant \dim(A)$, which is clearly equivalent to (5.96). □

We now revisit the subspaces S' and T' in Lemma 5.35 and study the distribution of $\dim(S' \cap T')$.

LEMMA 5.39. *Let n, m, ℓ, r, Δ be nonnegative integers with $r < \min\{m, \ell\}$ and $\max\{m, \ell\} \leqslant n$. Fix a finite field $\mathbb{F}$ with $q = |\mathbb{F}|$ elements, and let $S \in \mathscr{S}(\mathbb{F}^n, m)$ and $T \in \mathscr{S}(\mathbb{F}^n, \ell)$ be given subspaces. Let $X \in \mathbb{F}^{(m+\ell-r+\Delta)\times n}$ and $Y \in \mathbb{F}^{(m+\ell-2r+3\Delta)\times(m+\ell-r+\Delta)}$ be uniformly random matrices. Let Z be the indicator random variable for the event that* (5.76)–(5.79) *hold. Define $S' = Y((X(S))^\perp)$ and $T' = Y((X(T))^\perp)$. Then:*

(i) $\mathbf{E}[Zq^{\dim(S' \cap T')}] \leqslant q^\Delta (1 + 8q^{-\Delta})^2$ *whenever* $\dim(S \cap T) \leqslant r$;
(ii) $\mathbf{E}[Zq^{\min\{\dim(S' \cap T'), \Delta+1\}}] \geqslant q^{\Delta+1}(1 - 16q^{-\Delta-1})$ *whenever* $\dim(S \cap T) \geqslant r + 1$.

Proof. (i) Consider the random variables

$$A = m + \ell - r - \min\{\dim(X(S + T)), m + \ell - r\},$$
$$B = \dim((X(S))^\perp + (X(T))^\perp) - \dim(Y((X(S))^\perp + (X(T))^\perp)).$$

Then the inequality

$$Zq^{\dim(S' \cap T')} \leqslant Zq^{A+B+\Delta} \tag{5.97}$$

is trivially true for $Z = 0$ and follows from equation (5.82) of Lemma 5.35 for $Z = 1$. The hypothesis $\dim(S \cap T) \leqslant r$ implies that $\dim(S + T) = \dim(S) + \dim(T) - \dim(S \cap T) \geqslant m + \ell - r$. As a result, applying Lemma 2.20 with $d = m + \ell - r + \Delta$ and $T = m + \ell - r$ gives

$$\mathop{\mathbf{E}}_{X}[q^A] \leqslant 1 + 8q^{-\Delta}. \tag{5.98}$$

Now, let Z' be the indicator random variable for the event that (5.76) and (5.77) hold. Then $Z' = 1$ implies that

$$\begin{aligned}\dim((X(S))^\perp + (X(T))^\perp) &\leqslant \dim((X(S))^\perp) + \dim((X(T))^\perp) \\ &= 2(m + \ell - r + \Delta) - \dim(X(S)) - \dim(X(T)) \\ &\leqslant m + \ell - 2r + 2\Delta.\end{aligned}$$

As a result, Lemma 2.20 is applicable with $d = m + \ell - 2r + 3\Delta$ and $T = \dim((X(S))^\perp + (X(T))^\perp)$ and gives

$$Z' \mathop{\mathbf{E}}_{Y}[q^B \mid X] \leqslant Z'(1 + 8q^{-\Delta}). \tag{5.99}$$

It remains to put these ingredients together:

$$\begin{aligned}\mathbf{E}[Zq^{\dim(S' \cap T')}] &\leqslant \mathbf{E}[Zq^{A+B+\Delta}] \\ &\leqslant \mathbf{E}[Z'q^{A+B+\Delta}] \\ &= q^\Delta \mathop{\mathbf{E}}_{X} q^A Z' \mathop{\mathbf{E}}_{Y}[q^B \mid X] \\ &\leqslant q^\Delta \mathop{\mathbf{E}}_{X} q^A Z'(1 + 8q^{-\Delta}) \\ &\leqslant q^\Delta \mathop{\mathbf{E}}_{X} q^A (1 + 8q^{-\Delta}) \\ &\leqslant q^\Delta (1 + 8q^{-\Delta})^2,\end{aligned}$$

where the first step uses (5.97), the second step is justified by $Z \leqslant Z'$, the fourth step applies (5.99), and the last step uses (5.98).

(ii) Assume now that $\dim(S \cap T) \geqslant r+1$. For $Z = 1$, equation (5.82) of Lemma 5.35 gives

$$\begin{aligned}\dim(S' \cap T') &\geqslant m + \ell - r + \Delta - \dim(X(S+T)) \\ &\geqslant m + \ell - r + \Delta - \dim(S+T) \\ &= m + \ell - r + \Delta - \dim(S) - \dim(T) + \dim(S \cap T) \\ &= -r + \Delta + \dim(S \cap T) \\ &\geqslant \Delta + 1.\end{aligned}$$

Now

$$\begin{aligned}\mathbf{E}[Zq^{\min\{\dim(S'\cap T'),\Delta+1\}}] &\geqslant q^{\Delta+1}\,\mathbf{E}[Z] \\ &\geqslant q^{\Delta+1}(1 - 16q^{-\Delta-1}),\end{aligned}$$

where the second step uses Lemma 5.35. □

At last, we are in a position to prove our claimed communication upper bound for the subspace intersection problem.

THEOREM 5.40 (Large error). *Let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements, and let n, m, ℓ, R be integers with $\max\{0, m+\ell-n\} < R \leqslant \min\{m, \ell\}$. Then $\max\{m, \ell\} \leqslant n$ and*

$$R_{\frac{1}{2} - \frac{1}{16q^{m+\ell-2R+16}}}(\text{INTERSECT}_R^{\mathbb{F},n,m,\ell}) \leqslant 2. \tag{5.100}$$

Furthermore, for each $\gamma \in [\frac{1}{3}q^{-(m+\ell-2R)/3}, \frac{1}{3}]$,

$$R_{(1-\gamma)/2}(\text{INTERSECT}_R^{\mathbb{F},n,m,\ell}) = O((\log_q\lceil\gamma q^{m-R}\rceil + 1)(\log_q\lceil\gamma q^{\ell-R}\rceil + 1)\log q). \tag{5.101}$$

If in addition $m = \ell = R$, then

$$R_{1/3}(\text{INTERSECT}_R^{\mathbb{F},n,m,\ell}) = O(1). \tag{5.102}$$

Proof. The hypothesis $\max\{0, m+\ell-n\} < R \leqslant \min\{m, \ell\}$ implies that $m + \ell - n \leqslant \min\{m, \ell\}$, which is equivalent to $\max\{m, \ell\} \leqslant n$. The bound (5.102) is immediate from Theorem 5.36.

In the rest of the proof, define $r = R - 1$. We will first settle (5.100). Let Δ be a nonnegative integer to be chosen later. Consider the following protocol Π'. On input a pair of subspaces $S \in \mathscr{S}(\mathbb{F}^n, m)$ for Alice and $T \in \mathscr{S}(\mathbb{F}^n, \ell)$ for Bob, the parties use their shared randomness to pick independent and uniformly random matrices $X \in \mathbb{F}^{(m+\ell-r+\Delta)\times n}$ and $Y \in \mathbb{F}^{(m+\ell-2r+3\Delta)\times(m+\ell-r+\Delta)}$. Alice and Bob compute $S' = Y((X(S))^\perp)$ and $T' = Y((X(T))^\perp)$, respectively. Note that S' and T' are subspaces in an ambient vector space V of dimension $m + \ell - 2r + 3\Delta$. Let Z be the indicator random variable for the event that the four conditions (5.76)–(5.79) hold. Alice and Bob use shared randomness to pick a uniformly random vector $v \in V$. They output 1 in the event that $Z = 1$ and $v \in S' \cap T'$, and output a uniformly random ± 1 value otherwise. The communication cost of this protocol is 2 bits since Alice can privately verify the conditions (5.76), (5.78), and $v \in S'$, and likewise Bob can privately verify the conditions (5.77), (5.79), and $v \in T'$. Observe further that

$$\mathbf{E}[\Pi'(S,T) \mid X, Y] = Zq^{\dim(S'\cap T') - (m+\ell-2r+3\Delta)}.$$

Passing to expectations over X and Y, we arrive at

$$\mathbf{E}\,\Pi'(S,T) = q^{-(m+\ell-2r+3\Delta)}\,\mathbf{E}[Zq^{\dim(S'\cap T')}].$$

Applying Lemma 5.39, we find that $\Pi'(S,T)$ has expectation at most $\alpha' = q^{-m-\ell+2r-2\Delta}(1+8q^{-\Delta})^2$ if $\dim(S \cap T) \leqslant r$, and at least $\beta' = q^{-m-\ell+2r-2\Delta}q(1 - 16q^{-\Delta-1})$ if $\dim(S \cap T) \geqslant r+1$. Taking $\Delta = 7$, one calculates that $\beta' - \alpha' \geqslant q^{-m-\ell+2r-14}/2$. Now Proposition 2.24 implies that

$$R_{\frac{1}{2} - \frac{1}{16q^{m+\ell-2r+14}}}(\neg\,\text{INTERSECT}_R^{\mathbb{F},n,m,\ell}) \leqslant 2,$$

which is equivalent to (5.100).

In what follows, we prove the remaining upper bound (5.101). Due to the symmetry between m and ℓ, we may assume without loss of generality that

$$m \geqslant \ell. \tag{5.103}$$

Let k and Δ be nonnegative integers to be set later, where

$$1 \leqslant k \leqslant \ell - r. \tag{5.104}$$

We will adapt Π' to obtain a new protocol Π'' that satisfies the following inequalities for all subspaces $S, T \subseteq \mathbb{F}^n$ of dimension m and ℓ, respectively:

$$\mathbf{E}[\Pi''(S,T) \mid X, Y] \geqslant q^{-k-\Delta} Z q^{\min\{\dim(S' \cap T'), \Delta+1\}}, \tag{5.105}$$

$$\mathbf{E}[\Pi''(S,T) \mid X, Y] \leqslant q^{-k-\Delta} Z q^{\dim(S' \cap T')}. \tag{5.106}$$

On input S and T, Alice and Bob in Π'' choose uniformly random matrices X and Y as before. They then compute the indicator random variable Z, which is a function of X, Y, S, T. If $Z = 0$, they output a uniformly random ± 1 value. Clearly, (5.105) and (5.106) hold in this case.

In the complementary case $Z = 1$, Alice and Bob compute $S' = Y((X(S))^{\perp})$ and $T' = Y((X(T))^{\perp})$, respectively. Lemma 5.35 with $Z = 1$ implies that S' and T' are subspaces of dimension $\ell - r + \Delta$ and $m - r + \Delta$, respectively, in an ambient vector space of dimension $m + \ell - 2r + 3\Delta$. This makes it possible for Bob to find a subspace U of dimension $m - r + \Delta + k$ such that $T' \subseteq U$, and send U to Alice. An application of Proposition 5.38 yields

$$\dim(S' \cap U) - \dim(S' \cap T') \leqslant \dim(U) - \dim(T') = k. \tag{5.107}$$

What Alice does next depends on the dimension of $S' \cap U$.

(i) If $\dim(S' \cap U) \geqslant k + \Delta + 1$, then (5.107) implies that $\dim(S' \cap T') \geqslant \Delta + 1$. Therefore, (5.105) and (5.106) amount to the requirement that the protocol's output have expectation at least q^{-k+1} and at most $q^{-k-\Delta+\dim(S' \cap T')} \in [q^{-k+1}, \infty)$. To meet this requirement, Alice simply outputs a random ± 1 value with expectation q^{-k+1}.

(ii) If $\dim(S' \cap U) \leqslant k + \Delta$, Alice identifies a $(k+\Delta)$-dimensional subspace S'' with the property that $S' \cap U \subseteq S'' \subseteq S'$, which exists because $k + \Delta \leqslant \ell - r + \Delta$ due to (5.104). She then picks a uniformly random vector $v \in S''$ and sends it to Bob, who outputs 1 if $v \in T'$ and a uniformly random ± 1 value otherwise. In this case, Alice and Bob's expected output is

$$\frac{q^{\dim(S'' \cap T')}}{q^{\dim(S'')}} = \frac{q^{\dim(S'' \cap T')}}{q^{k+\Delta}} = \frac{q^{\dim(S'' \cap U \cap T')}}{q^{k+\Delta}} = \frac{q^{\dim(S' \cap U \cap T')}}{q^{k+\Delta}} = \frac{q^{\dim(S' \cap T')}}{q^{k+\Delta}},$$

where the second step uses $T' \subseteq U$, the third step uses the defining property $S' \cap U \subseteq S'' \subseteq S'$ of the set S'', and the last step is valid due to $T' \subseteq U$. This agrees with (5.105) and (5.106), which require that the protocol's output have expectation between $q^{-k-\Delta} q^{\min\{\dim(S' \cap T'), \Delta+1\}}$ and $q^{-k-\Delta} q^{\dim(S' \cap T')}$.

The proof of (5.105) and (5.106) is now complete.

Since U has co-dimension $\ell - r + 2\Delta - k$, it can be communicated in the form of a basis for $U^{\perp}$ using $(\ell - r + 2\Delta - k)(m + \ell - 2r + 3\Delta)\lceil \log q \rceil$ bits. The vector v takes $(m + \ell - 2r + 3\Delta)\lceil \log q \rceil$ bits to send. In view of (5.103), we conclude that

$$\operatorname{cost}(\Pi'') = O((\ell - r + 2\Delta - k + 1)(m - r + \Delta)\lceil \log q \rceil + 1). \tag{5.108}$$

Lastly, we will show that Π'' is a distinguisher for the subspace intersection problem. For this, pass to expectations with respect to X and Y in (5.105) and (5.106) to obtain

$$\mathbf{E}\, \Pi''(S,T) \geqslant q^{-k-\Delta}\, \mathbf{E}[Z q^{\min\{\dim(S' \cap T'), \Delta+1\}}], \tag{5.109}$$

$$\mathbf{E}\, \Pi''(S,T) \leqslant q^{-k-\Delta}\, \mathbf{E}[Z q^{\dim(S' \cap T')}]. \tag{5.110}$$

Now Lemma 5.39 implies that $\Pi''(S,T)$ has expectation at most $\alpha'' = q^{-k}(1+8q^{-\Delta})^2$ if $\dim(S \cap T) \leqslant r$, and at least $\beta'' = q^{-k+1}(1-16q^{-\Delta-1})$ if $\dim(S \cap T) \geqslant r+1$. Taking $\Delta = 7$, one calculates that $\beta'' - \alpha'' \geqslant q^{-k}/2$. Now (5.108) and Proposition 2.24 imply that

$$R_{\frac{1}{2}-\frac{1}{16q^k}}(\neg \text{INTERSECT}_R^{\mathbb{F},n,m,\ell}) = O((\ell - r - k + 1)(m - r + 1)\log q) \tag{5.111}$$

for every positive integer $k \leqslant \ell - r$.

Let $\gamma \in [\frac{1}{3}q^{-(m+\ell-2R)/3}, \frac{1}{3}]$ be given. For $\gamma \in [q^{-4}, \frac{1}{3}]$, one obtains (5.101) from the bound $R_{1/3}(\text{INTERSECT}_R^{\mathbb{F},n,m,\ell}) = O((\ell-R+1)(m-R+1)\log q)$ of Theorem 5.36. For $\gamma \in [\frac{1}{3}q^{-(m+\ell-2R)/3}, q^{-4}]$, setting $k = \min\{\lfloor \log_q(1/\gamma) \rfloor - 3, \ell - r\}$ in (5.111) gives

$$\begin{aligned}
R_{(1-\gamma)/2}(\neg \text{INTERSECT}_R^{\mathbb{F},n,m,\ell}) &= O((\ell - r - \min\{\lfloor \log_q(1/\gamma) \rfloor - 3, \ell - r\} + 1)(m - r + 1)\log q) \\
&= O((\max\{\lceil \log_q(\gamma q^{\ell-r}) \rceil, 0\} + 4)(m - r + 1)\log q) \\
&= O((\log_q \lceil \gamma q^{\ell-r} \rceil + 1)(m - r + 1)\log q) \\
&= O((\log_q \lceil \gamma q^{\ell-R} \rceil + 1)(m - R + 1)\log q) \\
&= O((\log_q \lceil \gamma q^{\ell-R} \rceil + 1)(\log_q \lceil \gamma q^{m-R} \rceil + 1)\log q),
\end{aligned}$$

where the last step uses (5.103) and $\gamma \geqslant \frac{1}{3}q^{-(m+\ell-2R)/3}$. This completes the proof of (5.101). □

Theorem 5.40 settles the *randomized* communication upper bounds of Theorem 1.10 for the *total* subspace intersection problem, and hence also the *quantum* communication upper bound for the *promise* subspace intersection problem.

Acknowledgments

The authors are thankful to Alan Joel, Xiaoming Sun, Chengu Wang, and David Woodruff for their feedback on an earlier version of this manuscript. We are also grateful to Alan for useful discussions during this work, and to David for suggesting the application of our communication lower bounds to bilinear query complexity.

References

[1] S. Assadi, S. Khanna, and Y. Li, *On estimating maximum matching size in graph streams*, in Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 2017, pp. 1723–1742, doi:10.1137/1.9781611974782.113.

[2] S. Assadi, G. Kol, R. R. Saxena, and H. Yu, *Multi-pass graph streaming lower bounds for cycle counting, MAX-CUT, matching size, and other problems*, in *Proceedings of the Sixty-First Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 2020, pp. 354–364, doi:10.1109/FOCS46700.2020.00041.

[3] A. E. Brouwer, S. M. Cioaba, F. Ihringer, and M. McGinnis, *The smallest eigenvalues of Hamming graphs, Johnson graphs and other distance-regular graphs with classical parameters*, J. Comb. Theory, Ser. B, 133 (2018), pp. 88–121, doi:10.1016/J.JCTB.2018.04.005.

[4] M. Bury and C. Schwiegelshohn, *Sublinear estimation of weighted matchings in dynamic data streams*, in Proceedings of the Twenty-Third Annual European Symposium on Algorithms (ESA), 2015, pp. 263–274, doi:10.1007/978-3-662-48350-3_23.

[5] L. Chen, G. Kol, D. Paramonov, R. R. Saxena, Z. Song, and H. Yu, *Almost optimal super-constant-pass streaming lower bounds for reachability*, in *Proceedings of the Fifty-Third Annual ACM Symposium on Theory of Computing* (STOC), 2021, pp. 570–583, doi:10.1145/3406325.3451038.

[6] J. I. Chu and G. Schnitger, *The communication complexity of several problems in matrix computation*, J. Complex., 7 (1991), pp. 395–407, doi:10.1016/0885-064X(91)90027-U.

[7] J. I. Chu and G. Schnitger, *Communication complexity of matrix computation over finite fields*, Math. Syst. Theory, 28 (1995), pp. 215–228, doi:10.1007/BF01303056.

[8] S. M. Cioaba and H. Gupta, *On the eigenvalues of Grassmann graphs, bilinear forms graphs and Hermitian forms graphs*, Graphs Comb., 38 (2022), p. 30, doi:10.1007/S00373-021-02445-Z.

[9] K. L. Clarkson and D. P. Woodruff, *Numerical linear algebra in the streaming model*, in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing* (STOC), 2009, pp. 205–214, doi:10.1145/1536414.1536445.
[10] P. Delsarte, *Association schemes and t-designs in regular semilattices*, J. Comb. Theory, Ser. A, 20 (1976), pp. 230–243, doi:10.1016/0097-3165(76)90017-0.
[11] J. Eisfeld, *The eigenspaces of the Bose-Mesner-algebras of the association schemes corresponding to projective spaces and polar spaces*, Des. Codes Cryptogr., 17 (1999), pp. 129–150, doi:10.1023/A:1008366907558.
[12] D. E. Knuth, *Selected Papers on Discrete Mathematics*, CSLI Publications, 2001.
[13] I. Kremer, *Quantum communication*, master's thesis, Hebrew University, Computer Science Department, 1995.
[14] E. Kushilevitz and N. Nisan, *Communication complexity*, Cambridge University Press, 1997.
[15] T. Lee and A. Shraibman, *Lower bounds in communication complexity*, Foundations and Trends in Theoretical Computer Science, 3 (2009), pp. 263–398, doi:10.1561/0400000040.
[16] Y. Li, X. Sun, C. Wang, and D. P. Woodruff, *On the communication complexity of linear algebraic problems in the message passing model*, in *Proceedings of the Twenty-Eighth International Symposium on Distributed Computing* (DISC), vol. 8784, 2014, pp. 499–513, doi:10.1007/978-3-662-45174-8_34.
[17] N. Linial and A. Shraibman, *Lower bounds in communication complexity based on factorization norms*, Random Struct. Algorithms, 34 (2009), pp. 368–394, doi:10.1002/rsa.20232.
[18] L. Lovász and M. E. Saks, *Lattices, Möbius functions and communication complexity*, in *Proceedings of the Twenty-Ninth Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 1988, pp. 81–90, doi:10.1109/SFCS.1988.21924.
[19] P. B. Miltersen, N. Nisan, S. Safra, and A. Wigderson, *On data structures and asymmetric communication complexity*, J. Comput. Syst. Sci., 57 (1998), pp. 37–49, doi:10.1006/JCSS.1998.1577.
[20] J. M. Phillips, E. Verbin, and Q. Zhang, *Lower bounds for number-in-hand multiparty communication complexity, made easy*, SIAM J. Comput., 45 (2016), pp. 174–196, doi:10.1137/15M1007525.
[21] C. Rashtchian, D. P. Woodruff, and H. Zhu, *Vector-matrix-vector queries for solving linear algebra, statistics, and graph problems*, in *Proceedings of the Twenty-Fourth International Workshop on Randomization and Computation* (RANDOM), vol. 176 of LIPIcs, 2020, pp. 26:1–26:20, doi:10.4230/LIPICS.APPROX/RANDOM.2020.26.
[22] A. A. Razborov, *Quantum communication complexity of symmetric predicates*, Izvestiya: Mathematics, 67 (2003), pp. 145–159.
[23] A. A. Sherstov, *Communication lower bounds using dual polynomials*, Bulletin of the EATCS, 95 (2008), pp. 59–93.
[24] A. A. Sherstov, *The pattern matrix method*, SIAM J. Comput., 40 (2011), pp. 1969–2000, doi:10.1137/080733644. Preliminary version in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing* (STOC), 2008.
[25] A. A. Sherstov, *Strong direct product theorems for quantum communication and query complexity*, SIAM J. Comput., 41 (2012), pp. 1122–1165, doi:10.1137/110842661. Preliminary version in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing* (STOC), 2011.
[26] R. P. Stanley, *Enumerative Combinatorics*, vol. I, Cambridge University Press, 2nd ed., 2012.
[27] X. Sun and C. Wang, *Randomized communication complexity for linear algebra problems over finite fields*, in *Proceedings of the Twenty-Ninth International Symposium on Theoretical Aspects of Computer Science* (STACS), vol. 14, 2012, pp. 477–488, doi:10.4230/LIPICS.STACS.2012.477.
[28] R. de Wolf, *Quantum Computing and Communication Complexity*, PhD thesis, University of Amsterdam, 2001.
[29] A. C.-C. Yao, *Some complexity questions related to distributive computing*, in *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing* (STOC), 1979, pp. 209–213, doi:10.1145/800135.804414.
[30] A. C.-C. Yao, *Quantum circuit complexity*, in *Proceedings of the Thirty-Fourth Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 1993, pp. 352–361, doi:10.1109/SFCS.1993.366852.

Appendix A. Fourier spectrum of nonsingularity

Throughout this section, the underlying field is $\mathbb{F}_q$ for an arbitrary prime power q. The root of unity ω and the notation ω^x for $x \in \mathbb{F}_q$ are as defined in Section 2.4. The objective of this appendix is to prove Lemma 3.5. Our proof is shorter and simpler than the approach of Sun and Wang [27], who proved Lemma 3.5 for fields of prime order. What our proofs have in common is the following proposition [27].

PROPOSITION A.1 (Sun and Wang). *For any integers $n \geqslant 1$ and $r \in \{0, 1, \ldots, n\}$,*

$$\Gamma_n(n, r) = \mathop{\mathbf{E}}_{X \in \mathscr{M}_n} \omega^{X_{1,1} + \cdots + X_{r,r}}.$$

Proof (due to Sun and Wang). Let X, Y, Z be independent and uniformly random nonsingular matrices of order n. Then by Proposition 2.19(ii), the product XI_rY is a uniformly random matrix of rank r. Therefore,

$$\begin{aligned}\Gamma_n(n, r) &= \mathbf{E}\, \omega^{\langle Z, XI_rY \rangle} \\ &= \mathbf{E}\, \omega^{\langle X^\mathsf{T} Z Y^\mathsf{T}, I_r \rangle} \\ &= \mathbf{E}\, \omega^{\langle X, I_r \rangle} \\ &= \mathbf{E}\, \omega^{X_{1,1} + X_{2,2} + \cdots + X_{r,r}},\end{aligned}$$

where the second step uses Fact 2.2(ii), and the third step is legitimate because $X^\mathsf{T} Z Y^\mathsf{T}$ is a uniformly random nonsingular matrix by Proposition 2.19(i). □

We are now ready to establish our result of interest.

LEMMA (restatement of Lemma 3.5). *For any integers $n \geqslant 1$ and $r \in \{0, 1, \ldots, n\}$,*

$$\Gamma_n(n, r) = \frac{(-1)^r q^{\binom{r}{2}}}{(q^n - 1)(q^n - q) \cdots (q^n - q^{r-1})}.$$

Proof. Consider independent random matrices X and L of order n, where X is a uniformly random nonsingular matrix and L is a uniformly random nonsingular *lower-diagonal* matrix. By Proposition 2.19(i), the product XL is a uniformly random nonsingular matrix. Therefore, Proposition A.1 implies that

$$\Gamma_n(n, r) = \mathbf{E}\, \omega^{\sum_{i=1}^r (XL)_{i,i}}.$$

We will say that X is *nice* if $X_{i,j} = 0$ for all (i, j) pairs such that $i \in \{1, 2, \ldots, r\}$ and $j > i$.

CLAIM A.2. *One has*

$$\mathop{\mathbf{E}}_{L} \left[\omega^{\sum_{i=1}^r (XL)_{i,i}} \mid X \right] = \begin{cases} (-1)^r (q-1)^{-r} & \text{if } X \text{ is nice,} \\ 0 & \text{otherwise.} \end{cases}$$

This claim, to be proved shortly, implies that

$$\Gamma_n(n, r) = \frac{(-1)^r}{(q-1)^r}\, \mathbf{P}[X \text{ is nice}]. \tag{A.1}$$

The probability of the nonsingular matrix X being nice is straightforward to calculate: there are $q - 1$ choices for the first row, $q(q-1)$ choices for the second row, $q^2(q-1)$ choices for the third row, and so on up to row r, whence

$$\mathop{\mathbf{P}}_{X}[X \text{ is nice}] = \frac{\prod_{i=1}^r q^{i-1}(q-1)}{(q^n - 1)(q^n - q) \cdots (q^n - q^{r-1})}.$$

Making this substitution in (A.1) completes the proof. □

Proof of Claim A.2. Conditioned on X, the columns of XL are independent random variables. Therefore,

$$\begin{aligned}\mathop{\mathbf{E}}_{L}\left[\omega^{\sum_{i=1}^{r}(XL)_{i,i}} \mid X\right] &= \prod_{i=1}^{r} \mathop{\mathbf{E}}_{L}\left[\omega^{(XL)_{i,i}} \mid X\right] \\ &= \prod_{i=1}^{r} \mathop{\mathbf{E}}_{L}\left[\omega^{\sum_{j=i}^{n} X_{i,j}L_{j,i}} \mid X\right]. \end{aligned} \tag{A.2}$$

The entries of L are independent random variables, with the diagonal entries distributed uniformly on $\mathbb{F}_q \setminus \{0\}$ and the subdiagonal entries distributed uniformly on $\mathbb{F}_q$. If X is not nice, then $X_{i,k} \neq 0$ for some $i \in \{1, 2, \ldots, r\}$ and $k > i$, which means that the corresponding summation $\sum_{j=i}^{n} X_{i,j}L_{j,i}$ is a uniformly random field element. This forces (A.2) to vanish, due to (2.14). When X is nice, on the other hand, (A.2) simplifies as follows:

$$\begin{aligned}\prod_{i=1}^{r} \mathop{\mathbf{E}}_{L}\left[\omega^{\sum_{j=i}^{n} X_{i,j}L_{j,i}} \mid X\right] &= \prod_{i=1}^{r} \mathop{\mathbf{E}}_{L}\left[\omega^{X_{i,i}L_{i,i}} \mid X\right] \\ &= \prod_{i=1}^{r} \mathop{\mathbf{E}}_{a_i \in \mathbb{F}_q \setminus \{0\}} \omega^{a_i} \\ &= \left(\frac{\sum_{a \in \mathbb{F}_q} \omega^a - 1}{q-1}\right)^r \\ &= \frac{(-1)^r}{(q-1)^r}, \end{aligned}$$

where the second step is legitimate because $X_{i,i}$ is nonzero and $L_{i,i}$ is a uniformly random nonzero field element, and the last step uses (2.14). □

Appendix B. Multiparty lower bounds via symmetrization

The purpose of this appendix is to prove Proposition 1.11, which gives a generic method for transforming two-party communication lower bounds for a class of problems into corresponding multiparty lower bounds. Recall that we adopt the number-in-hand blackboard model of multiparty communication, reviewed in the introduction. The notation $R_\varepsilon(F)$ stands for the ε-error randomized communication complexity of the two-party or multiparty problem F. The *cost* of a protocol Π, denoted $\mathrm{cost}(\Pi)$, is the total number of bits written to the blackboard in the worst-case execution of Π.

Proposition (restatement of Proposition 1.11). *Let $(X, +)$ be a finite Abelian group, and let $f\colon X \to \{-1, 1, *\}$ be a given function. For $t \geqslant 2$, let $F_t\colon X^t \to \{-1, 1, *\}$ be the t-party communication problem given by $F_t(x_1, x_2, \ldots, x_t) = f(x_1 + x_2 + \cdots + x_t)$. Then for all $t \geqslant 2$,*

$$R_{1/6}(F_t) \geqslant \frac{1}{12} t R_{1/3}(F_2).$$

Proof. The proof uses the symmetrization technique of Phillips, Verbin, and Zhang [20]. Let Π be a randomized protocol for F_t with error probability $1/6$. We will use Π to construct a protocol for the two-party problem F_2 with error probability $1/3$ and communication cost at most $\mathrm{cost}(\Pi) \cdot 12/t$.

The protocol for F_2 is as follows. On input $(a, b) \in X \times X$, Alice and Bob use their shared randomness to pick uniformly random elements $r_1, r_2, \ldots, r_{t-1} \in X$ and uniformly random integers i, j with $1 \leqslant i < j \leqslant n$. Let

$$\mathbf{x} = (r_1, r_2, \ldots, r_{t-1}, -r_1 - r_2 - \cdots - r_{t-1}) + (0, \ldots, 0, a, 0, \ldots, 0, b, 0, \ldots, 0),$$

where the rightmost tuple has a in the i-th component, b in the j-th component, and zeroes everywhere else. Since the components of $\mathbf{x}$ sum to $a+b$, we have

$$F_t(\mathbf{x}) = F_2(a,b). \tag{B.1}$$

Moreover, $\mathbf{x}$ is a *uniformly random* tuple whose components sum to $a+b$ because the first $t-1$ components are distributed independently and uniformly at random on X, whereas the sum of the components is $a+b$. In particular, $\mathbf{x}$ and (i,j) are independent random variables.

By construction, Alice knows all the components of $\mathbf{x}$ except for the j-th, and Bob knows all the components except for the i-th. This makes it possible for them to run Π on $\mathbf{x}$, with Alice simulating all the parties other than the j-th, and Bob simulating all the parties other than the i-th. When Π requires the i-th party to speak, Alice sends his message to Bob, and analogously for the j-th party. For $k = 1, 2, \ldots, t$, consider the random variable $C(\mathbf{x}, k)$ defined as the total number of bits sent in Π by the k-th party on input $\mathbf{x}$. Then the number of bits exchanged by Alice and Bob is $C(\mathbf{x}, i) + C(\mathbf{x}, j)$. Using the independence of $\mathbf{x}$ and (i,j), we can now bound Alice and Bob's expected communication cost on input (a,b) as follows:

$$\mathbf{E}[C(\mathbf{x},i) + C(\mathbf{x},j)] = \frac{2}{t}\,\mathbf{E}[C(\mathbf{x},1) + \cdots + C(\mathbf{x},t)] \leqslant \frac{2}{t}\,\mathrm{cost}(\Pi). \tag{B.2}$$

By (B.1), the described two-party protocol computes F_2 with the same error probability that Π computes F_t, namely, $1/6$. Furthermore, by (B.2), the *expected* communication cost of the two-party protocol on any given input is at most $\mathrm{cost}(\Pi) \cdot 2/t$. By Markov's inequality, the probability of Alice and Bob exchanging at least $\mathrm{cost}(\Pi) \cdot 12/t$ bits is at most $1/6$. Therefore, one can obtain a protocol for F_2 with error $1/6 + 1/6 = 1/3$ by terminating the described protocol as soon as $\lfloor \mathrm{cost}(\Pi) \cdot 12/t \rfloor$ bits have been communicated. □

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il