Strong Inapproximability for a Promise Rank Problem

Venkatesan Guruswami, Xuandi Ren, and Shaoxuan Tang

August 19, 2026

Problem

In this work, we study the following problem.

Promise rank problem

For a linear subspace $\mathcal{L} \subseteq \mathbb{F}_q^{N \times N}$ of $N \times N$ matrices, let

$$\mathrm{minrank}(\mathcal{L}) := \min\{\mathrm{rank}(A) : 0 \neq A \in \mathcal{L}\}.$$

Given $\mathcal{L}$, distinguish

$$\mathrm{minrank}(\mathcal{L}) = 1 \qquad \text{from} \qquad \mathrm{minrank}(\mathcal{L}) > k.$$

Motivation

A classical diagonal embedding of Hamming-metric codes gives

$$\begin{array}{ccc} c \in C & \mapsto & \mathrm{diag}(c) \in \mathcal{L}_C \\ \|c\|_0 & = & \mathrm{rank}(\mathrm{diag}(c)) \end{array}$$

where $\mathcal{L}_C := \{\mathrm{diag}(c) : c \in C\}$.

Motivation

A classical diagonal embedding of Hamming-metric codes gives

$$\begin{array}{ccc} c \in C & \mapsto & \mathrm{diag}(c) \in \mathcal{L}_C \\ \|c\|_0 & = & \mathrm{rank}(\mathrm{diag}(c)) \end{array}$$

where $\mathcal{L}_C := \{\mathrm{diag}(c) : c \in C\}$.

Now we can directly apply hardness results for the Minimum Distance Problem (MDP) to get hardness results for $\mathrm{minrank}$.

Motivation

A classical diagonal embedding of Hamming-metric codes gives

$$\begin{array}{ccc} c \in C & \mapsto & \mathrm{diag}(c) \in \mathcal{L}_C \\ \|c\|_0 & = & \mathrm{rank}(\mathrm{diag}(c)) \end{array}$$

where $\mathcal{L}_C := \{\mathrm{diag}(c) : c \in C\}$.

Now we can directly apply hardness results for the Minimum Distance Problem (MDP) to get hardness results for $\mathrm{minrank}$.

However, the minimum Hamming weight of a hard instance C is not a constant. Therefore, it is natural to ask whether there is a rank-gap of 1 vs. k in the promise rank problem.

Motivation

A second motivation comes from recent PCP-free inapproximability results for MDP and SVP [BGLR25]. The paper starts from quadratic equations and proves that it is NP-hard to distinguish

$$\mathrm{minrank}(\mathcal{L}) = 1 \qquad \text{from} \qquad \mathrm{minrank}(\mathcal{L}) \geq 2.$$

Motivation

A second motivation comes from recent PCP-free inapproximability results for MDP and SVP [BGLR25]. The paper starts from quadratic equations and proves that it is NP-hard to distinguish

$$\mathrm{minrank}(\mathcal{L}) = 1 \qquad \text{from} \qquad \mathrm{minrank}(\mathcal{L}) \geq 2.$$

Composing $\mathcal{L}$ with a suitable balanced code C converts this rank gap into a Hamming-weight gap in $C \otimes C$:

$$\begin{aligned} \mathrm{rank}(X) = 1 \quad &\Longrightarrow \quad \|X\|_0 \leq (1+\varepsilon)d(C)^2, \\ \mathrm{rank}(X) \geq 2 \quad &\Longrightarrow \quad \|X\|_0 \geq (1+\alpha)d(C)^2. \end{aligned}$$

Motivation

A second motivation comes from recent PCP-free inapproximability results for MDP and SVP [BGLR25]. The paper starts from quadratic equations and proves that it is NP-hard to distinguish

$$\mathrm{minrank}(\mathcal{L}) = 1 \qquad \text{from} \qquad \mathrm{minrank}(\mathcal{L}) \geq 2.$$

Composing $\mathcal{L}$ with a suitable balanced code C converts this rank gap into a Hamming-weight gap in $C \otimes C$:

$$\begin{aligned} \mathrm{rank}(X) = 1 \quad &\Longrightarrow \quad \|X\|_0 \leq (1+\varepsilon)d(C)^2, \\ \mathrm{rank}(X) \geq 2 \quad &\Longrightarrow \quad \|X\|_0 \geq (1+\alpha)d(C)^2. \end{aligned}$$

This also motivates us to study the underlying problem directly: can the gap be amplified?

Our Results

For any finite field of characteristic 2, we give a deterministic reduction from $3\textsc{Sat}$ producing a rank gap of 1 versus k with matrix dimension $n^{O(\log k)}$, yielding the following inapproximability results.

Our Results

For any finite field of characteristic 2, we give a deterministic reduction from $3\textsc{Sat}$ producing a rank gap of 1 versus k with matrix dimension $n^{O(\log k)}$, yielding the following inapproximability results.

Theorem

Fix $r \geq 1$. Given $\mathcal{L} \subseteq \mathbb{F}_{2^r}^{N \times N}$, distinguishing

$$\mathrm{minrank}(\mathcal{L}) = 1 \quad \text{from} \quad \mathrm{minrank}(\mathcal{L}) > k$$

is impossible in polynomial time for:

(a) any constant $k > 1$, assuming P $\neq$ NP;

(b) $k = 2^{(\log N)^{1-\epsilon}}$, for any fixed $0 < \epsilon < 1$, assuming NP $\not\subseteq$ DTIME$(2^{\log^{O(1)} n})$;

(c) $k = N^{c/\log\log N}$, for some fixed $c > 0$, assuming NP $\not\subseteq \bigcap_{\delta>0}$ DTIME$(2^{n^{\delta}})$.

Our Results

We also give a deterministic reduction with matrix dimension $n^{O(k)}$ that works over any finite field, yielding the following inapproximability results.

Our Results

We also give a deterministic reduction with matrix dimension $n^{O(k)}$ that works over any finite field, yielding the following inapproximability results.

Theorem

Fix a finite field $\mathbb{F}_q$. Given $\mathcal{L} \subseteq \mathbb{F}_q^{N\times N}$, distinguishing

$$\mathrm{minrank}(\mathcal{L}) = 1 \quad \text{from} \quad \mathrm{minrank}(\mathcal{L}) > k$$

is impossible in polynomial time for:

(a) any constant $k > 1$, assuming P $\neq$ NP;

(b) $k = (\log N)^{1-\epsilon}$, for any fixed $0 < \epsilon < 1$, assuming NP $\not\subseteq$ DTIME$(2^{\log^{O(1)} n})$;

(c) $k = c\log N/\log\log N$, for some fixed constant $c > 0$, assuming NP $\not\subseteq \bigcap_{\delta>0}$ DTIME$(2^{n^{\delta}})$.

Quadratic Systems

In this talk, we focus on the $\mathbb{F}_2$ case.

Quadratic Systems

In this talk, we focus on the $\mathbb{F}_2$ case.

Let $y = (y_S)$ be a vector of variables over $\mathbb{F}_2$ and consider constant-free equations

$$g_j(y) = \sum_{S,T} c^{(j)}_{S,T} y_S y_T + \sum_R b^{(j)}_R y_R = 0, \qquad j = 1, \ldots, M.$$

Quadratic Systems

In this talk, we focus on the $\mathbb{F}_2$ case.

Let $y = (y_S)$ be a vector of variables over $\mathbb{F}_2$ and consider constant-free equations

$$g_j(y) = \sum_{S,T} c_{S,T}^{(j)} y_S y_T + \sum_R b_R^{(j)} y_R = 0, \qquad j = 1, \ldots, M.$$

For a rank-one matrix $A = yy^\top$, each equation becomes the homogeneous linear constraint

$$\sum_{S,T} c_{S,T}^{(j)} A_{S,T} + \sum_R b_R^{(j)} A_{R,R} = 0.$$

Quadratic Systems

In this talk, we focus on the $\mathbb{F}_2$ case.

Let $y = (y_S)$ be a vector of variables over $\mathbb{F}_2$ and consider constant-free equations

$$g_j(y) = \sum_{S,T} c_{S,T}^{(j)} y_S y_T + \sum_R b_R^{(j)} y_R = 0, \qquad j = 1, \ldots, M.$$

For a rank-one matrix $A = yy^\top$, each equation becomes the homogeneous linear constraint

$$\sum_{S,T} c_{S,T}^{(j)} A_{S,T} + \sum_R b_R^{(j)} A_{R,R} = 0.$$

We construct $\mathcal{L}$ as the subspace of symmetric matrices satisfying these constraints.

YES Case

The quadratic system $\mathcal{Q}$ is constructed so that if the 3SAT instance is satisfiable, then $\mathcal{Q}$ has a nonzero solution y. Then

$$g_1(y) = g_2(y) = \cdots = g_M(y) = 0.$$

YES Case

The quadratic system $\mathcal{Q}$ is constructed so that if the 3SAT instance is satisfiable, then $\mathcal{Q}$ has a nonzero solution y. Then

$$g_1(y) = g_2(y) = \cdots = g_M(y) = 0.$$

Let $A = yy^\top$. For every j,

$$\sum_{S,T} c^{(j)}_{S,T} A_{S,T} + \sum_{R} b^{(j)}_{R} A_{R,R} = g_j(y) = 0.$$

YES Case

The quadratic system $\mathcal{Q}$ is constructed so that if the 3SAT instance is satisfiable, then $\mathcal{Q}$ has a nonzero solution y. Then

$$g_1(y) = g_2(y) = \cdots = g_M(y) = 0.$$

Let $A = yy^\top$. For every j,

$$\sum_{S,T} c^{(j)}_{S,T} A_{S,T} + \sum_{R} b^{(j)}_{R} A_{R,R} = g_j(y) = 0.$$

Thus, A is a rank-one matrix in $\mathcal{L}$.

NO Case

In the NO case, suppose a nonzero feasible matrix has rank at most k. Since it is symmetric, it admits a decomposition

$$A = \sum_{i=1}^{t} u^{(i)} u^{(i)\top}, \qquad t \leq \left\lfloor \frac{3k}{2} \right\rfloor.$$

NO Case

In the NO case, suppose a nonzero feasible matrix has rank at most k. Since it is symmetric, it admits a decomposition

$$A = \sum_{i=1}^{t} u^{(i)} u^{(i)\top}, \qquad t \leq \left\lfloor \frac{3k}{2} \right\rfloor.$$

Substituting this decomposition into the jth matrix constraint gives

$$0 = \sum_{i=1}^{t} g_j\left(u^{(i)}\right), \qquad j = 1, \ldots, M.$$

NO Case

In the NO case, suppose a nonzero feasible matrix has rank at most k. Since it is symmetric, it admits a decomposition

$$A = \sum_{i=1}^{t} u^{(i)} u^{(i)\top}, \qquad t \leq \left\lfloor \frac{3k}{2} \right\rfloor.$$

Substituting this decomposition into the jth matrix constraint gives

$$0 = \sum_{i=1}^{t} g_j\left(u^{(i)}\right), \qquad j = 1, \ldots, M.$$

This is exactly the statement that $u^{(1)}, \ldots, u^{(t)}$ satisfy all the quadratic equations **in superposition**.

NO Case

We need to rule out the possibility of t assignments $u^{(1)}, \ldots, u^{(t)}$ satisfy all g_j in superposition.

NO Case

We need to rule out the possibility of t assignments $u^{(1)}, \dots, u^{(t)}$ satisfy all g_j in superposition.

If we allow these quadratic equations to contain constants, then Khot and Saket [KS14] give a construction with the required superposition soundness.

NO Case

We need to rule out the possibility of t assignments $u^{(1)}, \ldots, u^{(t)}$ satisfy all g_j in superposition.

If we allow these quadratic equations to contain constants, then Khot and Saket [KS14] give a construction with the required superposition soundness.

So we need to obtain a constant-free version of the Khot–Saket superposition reduction.

Constant-Free Reduction

The reduction has three steps:

$$\begin{array}{ccccccc} \boxed{z_i} & \longrightarrow & \boxed{x_0, x_1, \ldots, x_n} & \longrightarrow & \boxed{y_S} & \longrightarrow & \boxed{A_{S,T}} \\ \textsc{3Sat} & & \text{degree-}d\text{ system} & & \text{quadratic system } \mathcal{Q} & & \text{subspace } \mathcal{L} \end{array}$$

Choose $d = 100 \log k$, then the matrix dimension is $n^{O(\log k)}$.

Constant-Free Reduction

The reduction has three steps:

z_i	$\longrightarrow$	$x_0, x_1, \ldots, x_n$	$\longrightarrow$	y_S	$\longrightarrow$	$A_{S,T}$
3SAT		degree-d system		quadratic system $\mathcal{Q}$		subspace $\mathcal{L}$

Choose $d = 100 \log k$, then the matrix dimension is $n^{O(\log k)}$.

In the YES case, for a satisfying assignment a of 3SAT, we have

- $x_0 = 1$, $x_i = a_i$ for every $1 \leq i \leq n$.
- $y_S = \prod_{i \in S} x_i$ for every $S \subseteq \{0, 1, \ldots, n\}$ and $|S| \leq d$.
- $A = yy^\top$, thus $A_{S,T} = y_S y_T$.

Constant-Free Superposition Soundness

Constant-free superposition soundness, adapted from [KS14]

For $d = \Omega(\log t)$, if the 3SAT instance is unsatisfiable and $u^{(1)}, \ldots, u^{(t)}$ satisfy every equation of $\mathcal{Q}$ in superposition, then

$$\sum_{i=1}^{t} u_S^{(i)} = 0 \qquad \text{for every } S.$$

Constant-Free Superposition Soundness

Constant-free superposition soundness, adapted from [KS14]

For $d = \Omega(\log t)$, if the 3SAT instance is unsatisfiable and $u^{(1)}, \dots, u^{(t)}$ satisfy every equation of $\mathcal{Q}$ in superposition, then

$$\sum_{i=1}^{t} u_S^{(i)} = 0 \qquad \text{for every } S.$$

Recall $A = \sum_{i=1}^{t} u^{(i)} u^{(i)\top}$. Therefore

$$A_{S,S} = \sum_{i=1}^{t} (u_S^{(i)})^2 = \sum_{i=1}^{t} u_S^{(i)} = 0.$$

Constant-Free Superposition Soundness

Constant-free superposition soundness, adapted from [KS14]

For $d = \Omega(\log t)$, if the 3SAT instance is unsatisfiable and $u^{(1)}, \ldots, u^{(t)}$ satisfy every equation of $\mathcal{Q}$ in superposition, then

$$\sum_{i=1}^{t} u_S^{(i)} = 0 \qquad \text{for every } S.$$

Recall $A = \sum_{i=1}^{t} u^{(i)} u^{(i)\top}$. Therefore

$$A_{S,S} = \sum_{i=1}^{t} (u_S^{(i)})^2 = \sum_{i=1}^{t} u_S^{(i)} = 0.$$

Since A is nonzero, there exists $A_{S,T} \neq 0$ for some $S \neq T$.

Equal-Union Constraints

To argue that this is impossible, we add the equal-union constraints

$$A_{S,T} = A_{S',T'} \qquad \text{whenever} \qquad S \cup T = S' \cup T'.$$

We can verify the constraints hold in the YES case since

$$A_{S,T} = y_S y_T = \prod_{i \in S \cup T} x_i = y_{S'} y_{T'} = A_{S',T'}.$$

Equal-Union Constraints

To argue that this is impossible, we add the equal-union constraints

$$A_{S,T} = A_{S',T'} \qquad \text{whenever} \qquad S \cup T = S' \cup T'.$$

We can verify the constraints hold in the YES case since

$$A_{S,T} = y_S y_T = \prod_{i \in S \cup T} x_i = y_{S'} y_{T'} = A_{S',T'}.$$

If $|S \cup T| \leq d$, then $S \cup T$ is also an index. Since the diagonal is zero,

$$A_{S,T} = A_{S \cup T, S \cup T} = 0.$$

Equal-Union Constraints

To argue that this is impossible, we add the equal-union constraints

$$A_{S,T} = A_{S',T'} \qquad \text{whenever} \qquad S \cup T = S' \cup T'.$$

We can verify the constraints hold in the YES case since

$$A_{S,T} = y_S y_T = \prod_{i \in S \cup T} x_i = y_{S'} y_{T'} = A_{S',T'}.$$

If $|S \cup T| \leq d$, then $S \cup T$ is also an index. Since the diagonal is zero,

$$A_{S,T} = A_{S \cup T, S \cup T} = 0.$$

If $A \neq 0$, choose $A_{S,T} \neq 0$ so that $R := S \cup T$ has minimum cardinality. Then $d < |R| \leq 2d$.

Structural Lemma

Assume $|R|$ is even. Let

$$\mathcal{P} = \{F \subseteq R : |F| = |R|/2\},$$

For $F, G \in \mathcal{P}$,

$$A_{F,G} \neq 0 \quad \Longleftrightarrow \quad G = R \setminus F.$$

Structural Lemma

Assume $|R|$ is even. Let

$$\mathcal{P} = \{F \subseteq R : |F| = |R|/2\},$$

For $F, G \in \mathcal{P}$,

$$A_{F,G} \neq 0 \quad \Longleftrightarrow \quad G = R \setminus F.$$

The submatrix $A|_{\mathcal{P},\mathcal{P}}$ is a permutation matrix, so

$$\operatorname{rank}(A) \geq \binom{|R|}{|R|/2} \geq \binom{d+1}{(d+1)/2} > k.$$

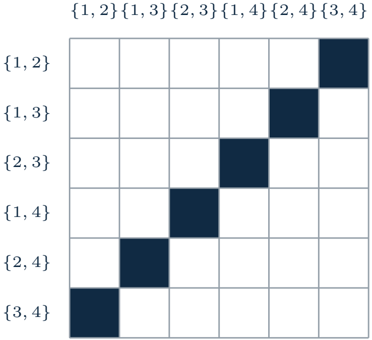

Figure: An example for $R = \{1, 2, 3, 4\}$.

NO Case Summary

For a nonzero matrix $A \in \mathcal{L}$ in the NO case,

$$\begin{aligned}
\operatorname{rank}(A) \leq k &\Longrightarrow A = \sum_{i=1}^{t} u^{(i)} u^{(i)\top} \\
&\Longrightarrow u^{(1)}, \ldots, u^{(t)} \text{ satisfy } \mathcal{Q} \text{ in superposition} \\
&\Longrightarrow \sum_i u^{(i)} = 0 \\
&\Longrightarrow A_{S,T} = 0 \text{ whenever } |S \cup T| \leq d \\
&\Longrightarrow \operatorname{rank}(A) \geq \binom{d+1}{(d+1)/2} > k.
\end{aligned}$$

This completes the soundness proof.

Thank You!

Questions and Comments?