Matrix Rigidity

Friedman's Lower Bound

Sasha Golovnev

September 7, 2020

Recap

- Rigid $\neq$ Sparse $+$ Low-Rank

Recap

- Rigid $\neq$ Sparse $+$ Low-Rank
- Moderately rigid matrices would imply circuit lower bounds

Recap

- Rigid $\neq$ Sparse $+$ Low-Rank
- Moderately rigid matrices would imply circuit lower bounds
- Extremely rigid matrices exist

Recap

- Rigid $\neq$ Sparse $+$ Low-Rank
- Moderately rigid matrices would imply circuit lower bounds
- Extremely rigid matrices exist

We need explicit constructions of rigid matrices

Explicit Constructions

Bounds on Rigidity

- Know a simple explicit matrix with rigidity

$$\mathcal{R}^{\mathbb{F}}_{M_n}(r) = \Omega\left(\frac{n^2}{r}\right) .$$

$$M = \begin{bmatrix} I_{2R} & \cdots & I_{2R} \\ & & \\ I_{2R} & & I_{2R} \end{bmatrix}$$

$$R_M(R) \geq \frac{n^2}{8R}$$

Bounds on Rigidity

- Know a simple explicit matrix with rigidity

$$\mathcal{R}^{\mathbb{F}}_{M_n}(r) = \Omega\left(\frac{n^2}{r}\right).$$

$R = \Theta(n)$

$R^{\mathbb{F}}_{M}(r) = \Omega(n)$

- What we need (for circuit lower bounds) is

$$\mathcal{R}^{\mathbb{F}}_{M_n}(r) = n^{1+\delta} \text{ for } r = \Omega(n).$$

Bounds on Rigidity

- Know a simple explicit matrix with rigidity

$$\mathcal{R}^{\mathbb{F}}_{M_n}(r) = \Omega\left(\frac{n^2}{r}\right).$$

- What we need (for circuit lower bounds) is

$$\mathcal{R}^{\mathbb{F}}_{M_n}(r) = n^{1+\delta} \text{ for } r = \Omega(n).$$

- The best known explicit bound

$R = \Theta(n)$
doesn't even matter

$$\mathcal{R}^{\mathbb{F}}_{M_n}(r) = \Omega\left(\frac{n^2}{r} \cdot \log \frac{n}{r}\right).$$

Explicit Lower Bound

Theorem

Let F be a fixed finite field, and $G \in \mathbb{F}^{n \times k}$ *be a generator matrix of a good linear code, then for every* $\Omega(\log n) < r < O(n)$,

$$\mathcal{R}_G^{\mathbb{F}}(r) \geq \Omega\left(\frac{n^2}{r} \cdot \log \frac{n}{r}\right) .$$

Error-Correcting Codes

- A code C of length n is a subset of $\mathbb{F}^n$

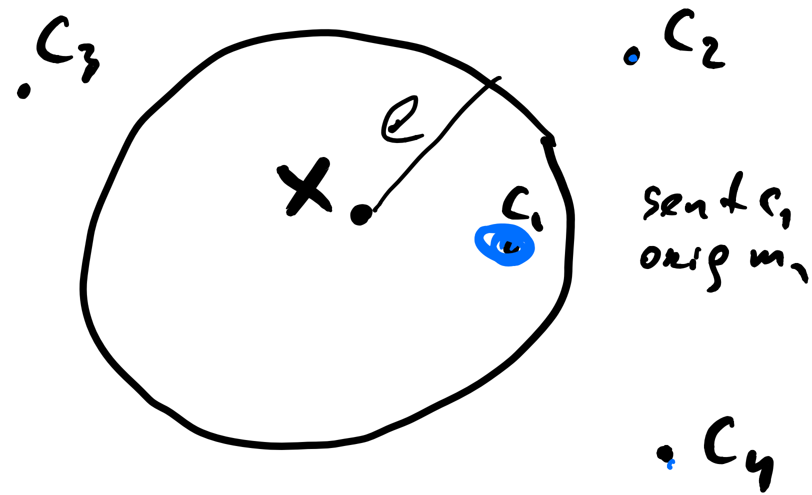
$$\begin{array}{ccccl} m_1 & & \cdots & m_K & \text{— messages} \\ \downarrow & & & \downarrow & \\ c_1 & & & c_K & \text{— codewords} \end{array}$$

$$C = \{c_1, \ldots, c_K\}$$

Even if several bits of c_i are flipped, then you still can recover c_i & m_i.

Error-Correcting Codes

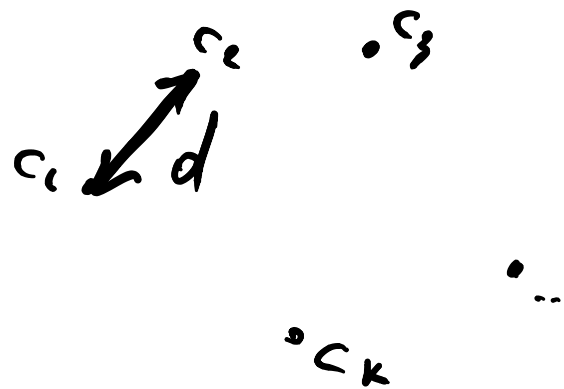
- A code C of length n is a subset of $\mathbb{F}^n$
- Code corrects e errors if for every $\boxed{x \in \mathbb{F}^n}$ there is at most one $c \in C$ with $\|x - c\|_1 \leq e$



Error-Correcting Codes

- A code C of length n is a subset of $\mathbb{F}^n$
- Code corrects e errors if for every $x \in \mathbb{F}^n$ there is at most one $c \in C$ with $\|x - c\|_1 \leq e$
- The minimum distance of a code is

$$d(C) = \min\left(\|u - v\|_1 \colon u, v \in C, u \neq v\right) .$$

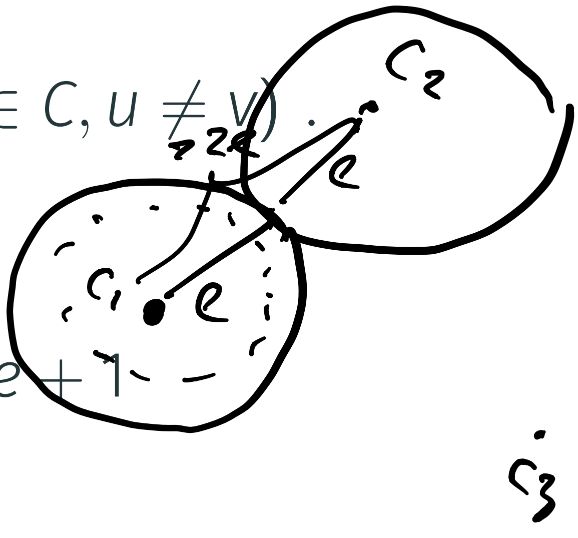


Error-Correcting Codes

- A code C of length n is a subset of $\mathbb{F}^n$
- Code corrects e errors if for every $x \in \mathbb{F}^n$ there is at most one $c \in C$ with $\|x - c\|_1 \leq e$
- The minimum distance of a code is

$$d(C) = \mathbf{min}\left(\|u - v\|_1 : u, v \in C, u \neq v\right).$$

- C corrects e errors IFF $d(C) \geq 2e + 1$



Linear Codes

- A linear code C is a subspace of $\mathbb{F}^n$

$\dim(C) = k$ $\qquad$ $|C| = |F|^k$

LINEAR CODES

- A linear code C is a subspace of $\mathbb{F}^n$

- For a linear code,

$$d(C) = \min\left(\|w\|_1 : w \in C, w \neq \mathbf{0}\right)$$

C - subspace, $0^n \in C$.

$\|w - 0\|_1 = \|w\| \geq d(C)$

$d = \min_{\substack{w_1 \neq w_2 \\ w_1, w_2 \in C}} \|w_1 - w_2\|$

C - subspace

$w_1 - w_2 \in C$

$w = w_1 - w_2 \in C$

$d = \min_{\substack{w \neq 0 \\ w \in C}} \|w\|_1$

Specifying Linear Code

- Two ways to specify a linear code $C \in \mathbb{F}^n$ of $\dim(C) = k$:

Specifying Linear Code

- Two ways to specify a linear code $C \in \mathbb{F}^n$ od $\dim(C) = k$:

- By a basis: give a generator matrix $G \in \mathbb{F}^{n \times k}$ whose columns form a basis of C

linear combinations of columns G $\equiv$ codewords of C, i.e.,

$w \in C \iff w = G \cdot x,\ x \in \mathbb{F}^k$

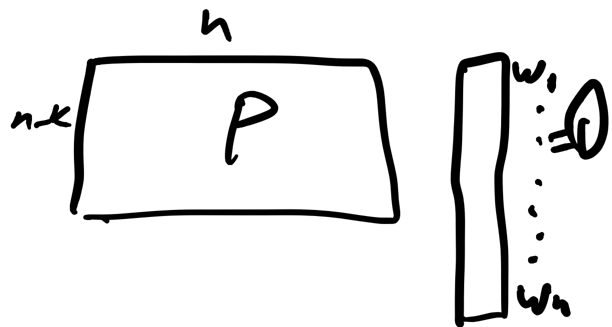
Specifying Linear Code

- Two ways to specify a linear code $C \in \mathbb{F}^n$ od $\dim(C) = k$:

- By a basis: give a generator matrix $G \in \mathbb{F}^{n \times k}$ whose columns form a basis of C

- By a system of linear equations: give a parity-check matrix $P \in \mathbb{F}^{(n-k)\times n}$ s.t. $Pw = 0$ iff $w \in C$

$w = (w_1, \ldots, w_n)$ $Pw = 0$
$\iff w \in C$.



Constructions of Linear Codes

HW1: $\exists$ exist linear codes with good parameters

Proposition

For any finite field $\mathbb{F}$, there exists an explicit family of linear error correcting codes over $\mathbb{F}$ of dimension $k = n/4$ and minimum distance $d = \delta n$ for a constant $\delta > 0$.

Constructions of Linear Codes

Proposition

For any finite field $\mathbb{F}$, there exists an explicit family of linear error correcting codes over $\mathbb{F}$ of dimension $k = n/4$ and minimum distance $d = \delta n$ for a constant $\delta > 0$.

Such codes are called good. Both dimension and minimum distance are $\Theta(n)$.

Friedman's Lower Bound

Series-parallel circuits require $R = \Theta(n)$

$R_G(R) = \omega(n$

Theorem

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of size q. Let $G \in \mathbb{F}^{n\times k}$ be a generator matrix of a code of dimension k and distance δn for a constant $0 < \delta < 1$. Then for any $\frac{\log_q k}{2} \le r \le \frac{k}{8}$,

$k = \Theta(n)$

$q = \Theta(1)$

$\log n \le R \le n$

$$\mathcal{R}_G^{\mathbb{F}}(r) \ge \frac{\delta k n \log_q \frac{k}{2r}}{8r} . \quad = \Omega\left(\frac{n^2}{R} \log \frac{n}{R}\right)$$

Proof Outline

- $G \in \mathbb{F}^{n\times k}$—generator matrix of a good code

Proof Outline

- $G \in \mathbb{F}^{n \times k}$—generator matrix of a good code

- Step 1. Show G has high "column" rigidity

$G \neq$ Low-rank + B

every column of B
is sparse

Proof Outline

- $G \in \mathbb{F}^{n \times k}$—generator matrix of a good code
- Step 1. Show G has high "column" rigidity
- Step 2. Column rigidity $\Rightarrow$ rigidity

Proof Outline

- $G \in \mathbb{F}^{n \times k}$—generator matrix of a good code
- Step 1. Show G has high "column" rigidity
- Step 2. Column rigidity $\Rightarrow$ rigidity

G HAS HIGH "COLUMN" RIGIDITY

Theorem

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of size q. Let $G \in \mathbb{F}^{n \times k}$ be a generator matrix of a code of dimension k and distance δn for a constant $0 < \delta < 1$. For any $\log_q k \leq r \leq \frac{k}{4}$, if every column of $B \in \mathbb{F}^{n \times k}$ contains at most $\frac{\delta n}{4r} \log_q \frac{k}{r}$ non-zero entries, then

$$\mathrm{rank}(G + B) > r\,. \quad \Longleftrightarrow G \neq \text{Low rank} + B$$

Theorem

Let $\mathbb{F} = \mathbb{F}_q$ *be a finite field of size q. Let* $G \in \mathbb{F}^{n\times k}$ *be a generator matrix of a code of dimension k and distance* δn *for a constant* $0 < \delta < 1$*. For any* $\log_q k \le r \le \frac{k}{4}$*, if every column of* $B \in \mathbb{F}^{n\times k}$ *contains at most* $\frac{\delta n}{4r}\log_q \frac{k}{r}$ *non-zero entries, then*

$$\mathrm{rank}(G+B) > r\,.$$

Assume, $\exists B$, every col of B has $\le \frac{\delta n}{4R} \log_q \frac{k}{R}$ non-zeros AND $\mathrm{Rank}(G+B) \le R$

$G + B \in F^{n\times k}$

$x \in F^k \qquad G+B : F^k \to F^n$

$\qquad\qquad x \longmapsto (G+B)x$

$\ker(G+B) = \{y \in F^k : (G+B)y = 0\}$

subspace.

<u>Proof outline.</u>

1. $x \in \ker(G+B)$, x is sparse.

2. $(G+B)x = \underline{Gx} + Bx = 0$

codeword $\|Gx\| \ge \delta n$

$Bx = -Gx$ - codeword $\Rightarrow \underline{\|Bx\| \ge \delta n}$

x - sparse, B is sparse

<u>Bx is sparse</u>

$x \in \ker(G+B)$, x is sparse

$\ker(G+B)$, draw Ham. ball of radius $d/2$ around every point

(parameter, choose later.

Rank-Nullity Theorem:

Rank + null = dim

$G+B : \mathbb{F}^k \to \mathbb{F}^n$

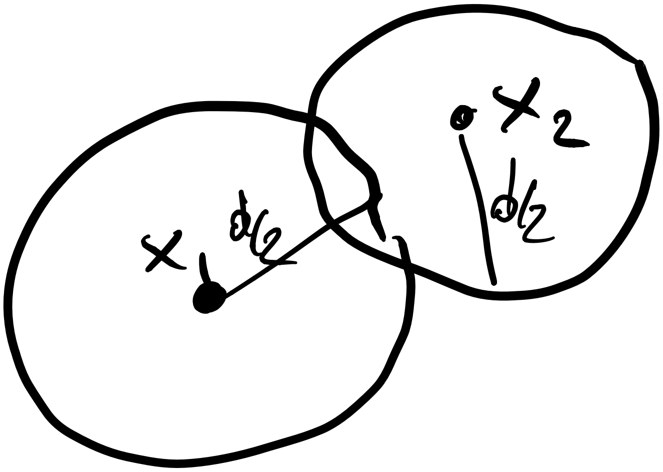
$$\underbrace{\operatorname{Rank}(G+B)}_{\leq R} + \operatorname{Rank}(\ker(G+B)) = k$$

$\Rightarrow \operatorname{Rank}(\ker(G+B)) \geq k-R$

$|\ker(G+B)| \geq |\mathbb{F}|^{k-R}$

$|\mathbb{F}|^{k-R} \cdot |\text{Ham ball of radius } \frac{d}{2}| \geq$

$\geq |\mathbb{F}|^k$ $\Rightarrow$ 2 balls must intersect.



$\Rightarrow$ Ham dist between x_1 & x_2 $\le d$.

$$x = x_1 - x_2 \in \ker R$$

$$\|x\|_1 = \| x_1 - x_2 \| \le d$$

$$\underbrace{|F|^{k-R} \cdot |\text{Ham ball of } R\ d/2| \ge |F|^k}$$

$$\ge |F|^{k-R} \cdot \binom{k}{d/2} \cdot \cancel{(|F|-1)}^{d/2}$$

$$\ge |F|^{k-R}\ k^{d/2} =$$

$$= |F|^{\frac{d}{2}\log_{|F|}\left(\frac{2k}{d}(|F|-1)\right)} \ge$$

$$\ge |F|^k$$

$$\boxed{d = \frac{2R}{\log_{1A}\frac{k}{R}}}$$

$x \in \ker(G+B)$, $\|x\|_1 \le d$

$(G+B)x = 0$

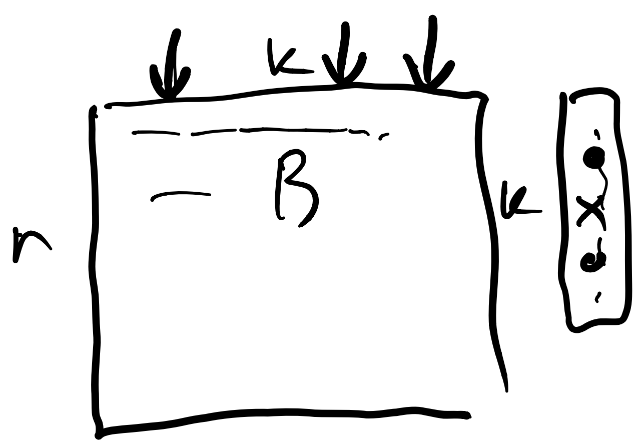
$Gx = -Bx$

codeword $\Rightarrow \|Gx\|_1 \geq \delta n$

$Bx = -Gx \Rightarrow \|Gx\|_1 \geq \boxed{\delta n}$

$\|x\|_1 \le d$

every col of B $\le \frac{\delta n}{4R} \log_{1A} \frac{k}{R}$ non-zeros



= lin comb of cols B.

$\le d$ cols

$\|Bx\|_1 \leq \|x\|_1 \cdot$ sparsity of col.

$\leq d \cdot \frac{\delta n}{4R} \log_{|F|} \frac{K}{R}$

$$d \approx \frac{2R}{\log_q \frac{K}{R}}$$

$\|Bx\|_1 < \delta n$

Proof Outline

- $G \in \mathbb{F}^{n \times k}$—generator matrix of a good code
- Step 1. Show G has high "column" rigidity
- Step 2. Column rigidity $\Rightarrow$ rigidity

Column rigidity $\Rightarrow$ rigidity

Theorem

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of size q. Let $G \in \mathbb{F}^{n \times k}$ be a generator matrix of a code of dimension k and distance δn for a constant $0 < \delta < 1$. Then for any $\frac{\log_q k}{2} \leq r \leq \frac{k}{8}$,

$$\mathcal{R}^{\mathbb{F}}_G(r) \geq \frac{\delta k n \log_q \frac{k}{2r}}{8r}. = \Omega\left(\frac{n^2}{R} \log \frac{n}{R}\right)$$

$k = \Theta(n)$

$q = \Theta(1)$

$\delta = \Theta(1)$

— $\log n \leq R \leq n$

$$G = L + S$$

$$\|S\|_0 \leq \frac{\delta k n \log_q \frac{k}{2R}}{8R}$$

Choose $\frac{k}{2}$ sparsest cols of S.

By Markov's inequality:

every col (of $k/2$) has

$$\leq \|S\|_0 / (k/2) = \frac{\delta n}{4R} \log \frac{k}{2R}$$

non-zeros.

$s_1 \ldots\ s_k$ — sparsities of cols

$s_1 \leq \ldots \leq s_k$

$s_1 + \ldots + s_k = \|S\|_0$

$$\underbrace{s_{k/2}} \leq \|S\|_0 / (k/2)$$

J = set of (indices of) $k/2$ sparsest cols

$$\boxed{G_J} = L_J + \boxed{S_J}$$

sparse in every col.

G is a good code

$k = \Theta(n)$, $d = \Theta(n)$

G_J $k' = \frac{k}{2} = \Theta(n)$, $d = \Theta(n)$

good code

By prev Thm: $(k \Rightarrow k/2)$

$G_J \neq L_J + S_J$ column-sparse

$\square$

Friedman

G – linear code

$$R_G^F(r) \geq \Omega\left(\frac{n^2}{r}\log\left(\frac{n}{r}\right)\right)$$

I. G high col rig

II Markov: col rig $\Rightarrow$ rig.