16. Seeded Lossless Rank Extractors

Sunday, October 15, 2023 7:01 PM

Let $\mathbb{F} = \overline{\mathbb{F}}$ (e.g. $\mathbb{F} = \mathbb{C}$). Let $\mathcal{M} = (M_i)_{i \in I}$ be a finite collection of matrices $M_i \in \mathbb{F}^{m \times n}$, where $m \le n$.

Def We say $\mathcal{M}$ is an (m', ε)-(seeded) lossless rank condenser if for every $A \in \mathbb{F}^{n \times m'}$ of rank m',

$$\Pr_{i \in_u I}[\operatorname{rank}(M_i \cdot A) = m'] \ge 1 - \varepsilon.$$

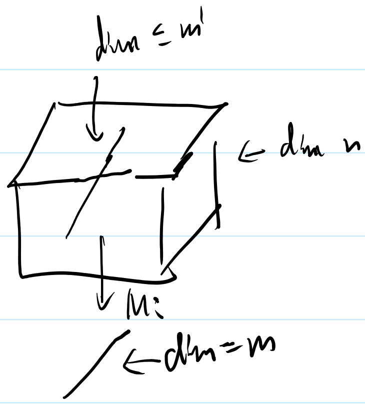
If $m = m'$, we say $\mathcal{M}$ is an ε-(seeded) lossless rank extractor.

Let $V \subseteq \mathbb{F}^n$ be the column span of A. Then $\dim V = \operatorname{rank}(A) = m'$.

View M_i as a linear map $\mathbb{F}^n \to \mathbb{F}^m$. Then $\operatorname{rank}(M_i \cdot A) = m' \iff \dim(M_i(V)) = m'$.

So A is an (m', ε)-lossless rank condenser iff all but $\le \varepsilon$-fraction of M_i preserve the dimension of V (i.e. $\dim V = \dim M_i(V)$) for all linear subspace $V \subseteq \mathbb{F}^n$ of dimension (at most) m'.

If M_i is injective on V of dim m', then it is also injective on subspaces of V.



"seeded" means we consider M_i chosen from a family $\mathcal{M}$, not a single matrix M_i.

A single matrix can't work (why?)

"lossless" means $\operatorname{rank}(A) = \operatorname{rank}(M_i A)$, or equivalently, $\dim V = \dim(M_i(V))$.

A construction of ε-lossless rank extractors. (Forbes - Shpilka '12)

Let $I \subseteq \mathbb{F} \setminus \{0\}$ finite. Let $\omega \in \mathbb{F}$ s.t. the multiplicative order of ω is at least n, i.e., $1, \omega, \dots, \omega^{n-1}$ are distinct.

For $a \in I$, let $M_a = \left(\omega^{i-1} a\right)^{j-1}_{1 \le i \le m,\ 1 \le j \le n} \in \mathbb{F}^{m \times n}$.

finite

For $a \in I$, let $M_a = \left(\omega^{(i-1)} a \right)^{j-1}_{1 \le i \le m,\, 1 \le j \le n} \in \mathbb{F}^{m \times n}$.

<u>Thm</u> (Forbes–Shpilka '12, Forbes–Saptharishi–Shpilka '13)

$\mathcal{M} = (M_a)_{a \in I}$ is an ε-lossless rank extractor with $\varepsilon = \dfrac{m(n-m)}{|I|}$.

i.e. for every $A \in \mathbb{F}^{n \times m}$, the number of $a \in I$ s.t. $\operatorname{rank}(M_a \cdot A) < m$ is at most $m(n-m)$.

To prove the theorem, we need:

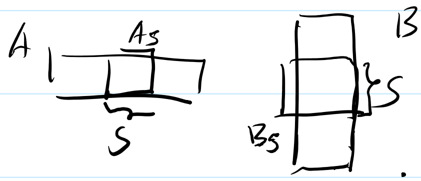
<u>Lemma</u> (Cauchy–Binet) Let $A \in \mathbb{F}^{m \times n}$ and $B \in \mathbb{F}^{n \times m}$, where $m \le n$. Then

$$\det(A \cdot B) = \sum_{\substack{S \subseteq [n] \\ |S| = m}} \det(A_S) \cdot \det(B_S)$$

$\leftarrow$ i.e. S ranges over m-subsets of $[n] = \{1, \dots, n\}$.

where A_S is the $m \times m$ submatrix with cols selected by S,

and B_S is the $m \times m$ submatrix with rows selected by S.



<u>Pf of the lemma</u>: Let $a_1, \dots, a_m$ be the rows of A & $b_1, \dots, b_m$ the columns of B.

Note $A \cdot B = \begin{pmatrix} a_1 B \\ \vdots \\ a_m B \end{pmatrix} = \begin{pmatrix} Ab_1 & \cdots & Ab_m \end{pmatrix}$.

As det is multilinear in its rows and columns, $\det(A \cdot B)$ is multilinear in $a_1, \dots, a_m$, $b_1, \dots, b_m$ (over $\mathbb{F}$).

i.e. let $f(a_1, \dots, a_m, b_1, \dots, b_m) = \det(A \cdot B)$.

Then $f(a_1, \dots, r a_i + s a_i', \dots, b_1, \dots, b_m) = r f(\cdots a_i \cdots) + s f(\cdots a_i' \cdots)$ $\quad r, s \in \mathbb{F}$

and similarly for b_i's.

Write each a_i and b_i^T as a linear combination of the standard basis $e_1, \dots, e_n$.

By multilinearity, we may assume $a_i, b_i^T \in \{e_1, \dots, e_n\}$.

Say $a_i = e_{j_i}$, $b_i^T = e_{j_i'}$, $S_A = \{j_1, \dots, j_m\}$, $S_B = \{j_1', \dots, j_m'\}$.

If $|S_A| < m$ or $|S_B| < m$, $\det(AB) = 0$ and $\sum_S \det(A_S) \cdot \det(B_S) = 0$.

If $S_A \ne S_B$, again $\det(AB) = 0$ and $\sum_S \det(A_S) \cdot \det(B_S) = 0$.

If $S_A \neq S_B$, again $\det(AB) = 0$ and $\sum_S \det(A_S) \cdot \det(B_S) = 0$.

So we may assume $S_A = S_B$ and $|S_A| = |S_B| = m$.

Then $A \cdot B = A_{S_A} \cdot B_{S_B}$. So the claim holds.

zero outside S_A zero outside S_B

$\square$

Proof of Thm: Consider $M(X) = \left((\omega^{i-1} X)^{j-1} \right)_{1 \le i \le m,\, 1 \le j \le n} \in (\mathbb{F}[X])^{m \times n}$. So $M_a = M(a)$.

substitute X by a within each entry.

Consider $A = (a_{ij})_{1 \le i \le n,\, 1 \le j \le m} \in \mathbb{F}^{n \times m}$. Let $P(X) = \det(M(X) \cdot A) \in \mathbb{F}[X]$.

Claim: $P(X) \neq 0$, $\deg(P) \le \sum_{i=n-m+1}^{n} (i-1)$, and $X^{\sum_{i=1}^{m}(i-1)}$ divides $P(X)$.

Pf of the claim: By Cauchy-Binet,

$$P(X) = \sum_S \det\left((M(X))_S\right) \cdot \det(A_S)$$

$$= \sum_{\substack{1 \le d_1 < \cdots < d_m \le n \\ S = \{d_1, \cdots, d_m\}}} \det\left(\left((\omega^{i-1} X)^{d_j - 1}\right)_{1 \le i \le m,\, 1 \le j \le m}\right) \cdot \det(A_S)$$

$$= \sum_{1 \le d_1 < \cdots < d_m \le n} \det\left((\omega^{i-1})^{d_j - 1}\right) \cdot \det(A_S) \cdot X^{\sum_{j=1}^{m}(d_j - 1)} \qquad (*)$$

Choose $1 \le d_1 < \cdots < d_m \le n$ s.t. $\det(A_S) \neq 0$ and $\sum_{j=1}^{m} (d_j - 1)$ is minimized.

By exchangeability, $(d_1, \cdots, d_m)$ is unique. The corresponding $\det\left((\omega^{i-1})^{d_j - 1}\right)$

$= \det\left((\omega^{d_j - 1})^{i-1}\right) \neq 0$

$\leftarrow$ Vandermonde matrix

$1, \omega, \cdots, \omega^{n-1}$ are distinct.

So $P(X) \neq 0$, $\deg(P) \le \sum_{i=n-m+1}^{n} (i-1)$, and $X^{\sum_{i=1}^{m}(i-1)}$ divides $P(X)$ by $(*)$.

This proves the claim.

$\Rightarrow$ $P(X)$ has at most $\underbrace{\left(\sum_{i=n-m+1}^{n} (i-1)\right) - \left(\sum_{i=1}^{m} (i-1)\right)}_{= m(n-m)}$ roots in $\mathbb{F} \setminus \{0\} \supseteq I$.

$\Rightarrow P[\operatorname{rank}(M_a \cdot A) = m] = P_a[\det(M(X) \cdot A)| \quad \neq 0]$

So $\Pr_{a \in_u I}\left[\operatorname{rank}(M_a \cdot A) = m\right] = \Pr_{a \in_u I}\left[\det(M(x) \cdot A)|_{x=a} \neq 0\right]$

$$= \Pr_{a \in_u I}\left[P(a) \neq 0\right] \leq \frac{m(n-m)}{|I|}. \quad \square.$$

By the theorem, if $|I| > m(n-m)$, then for every $A \in \mathbb{F}^{n \times m}$, $\exists M_a \in \mathcal{M}$ s.t.

$$\operatorname{rank}(M_a A) = \operatorname{rank}(A).$$

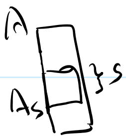
This is tight:

<u>Thm</u>: If $|I| \leq m(n-m)$, for any collection $\mathcal{M} = (M_a)_{a \in I}$ of matrices $M_a \in \mathbb{F}^{m \times n}$,

$\exists A \in \mathbb{F}^{n \times m}$ of rank m s.t. $\operatorname{rank}(M_a A) < m$ for all $a \in I$

<u>Pf sketch</u>: The set of m-dimensional subspaces of $\mathbb{F}^n$ is called the Grassmannian $Gr_{\mathbb{F}}(m, n) = Gr(m, n)$

It embeds in the projective space $\mathbb{P}^{\binom{n}{m}}$:



$$V \mapsto (A_S)_{S \subseteq \binom{[n]}{m}}, \text{ where } A \in \mathbb{F}^{n \times m} \text{ s.t. } V \text{ is the column space of } A.$$

For each $a \in I$, $\operatorname{rank}(M_a A) < m \iff \det(M_a A) = 0 \iff \sum_S \det((M_a)_S) \cdot \det(A_S) = 0$

Cauchy-Binet

This gives a linear constraint C_a in the coordinates A_S.

As $\dim Gr(m, n) = m(n-m) \geq |I|$, there exists $V \in Gr(m, n)$ satisfying C_a for all $a \in I$, i.e., $\operatorname{rank}(M_a A) < m$ for all $a \in I$. $\square$