On Lower Bounds for Multiplicative Circuits and Linear Circuits in Noncommutative Domains

V. Arvind , S. Raja
The Institute of Mathematical Sciences, Chennai
&
A.V. Sreejith
Tata Institute of Fundamental Research, Mumbai

CSR 2014

Outline

1. Lower Bounds for Multiplicative Circuits.
   1.1 lower bounds for Circuits over free monoids.
   1.2 lower bounds for Circuits over permutation groups.
2. Lower Bounds for Linear Circuits over Noncommutative Rings

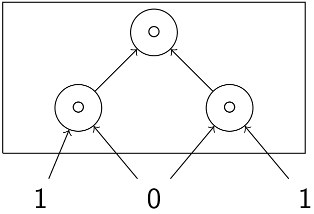
Multiplicative Circuits

- Let $T = \{0,1\}^*$ and $\circ =$ string concatenation operation
- $(T, \circ)$ is a monoid

Multiplicative Circuits

- Let $T = \{0,1\}^*$ and $\circ$ = string concatenation operation
- $(T,\circ)$ is a monoid

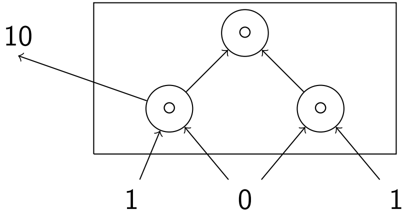
Circuit over monoid $(T,\circ)$:



Multiplicative Circuits

- Let $T = \{0,1\}^*$ and $\circ =$ string concatenation operation
- $(T,\circ)$ is a monoid

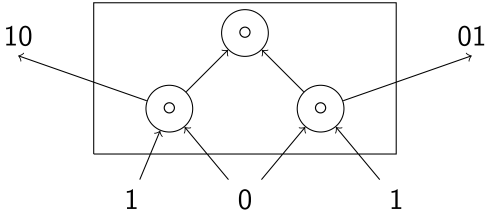
Circuit over monoid $(T,\circ)$:



Multiplicative Circuits

- Let $T = \{0, 1\}^*$ and $\circ =$ string concatenation operation
- $(T, \circ)$ is a monoid

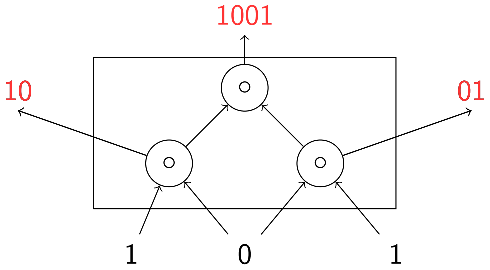
Circuit over monoid $(T, \circ)$:



Multiplicative Circuits

- Let $T = \{0,1\}^*$ and $\circ =$ string concatenation operation
- $(T,\circ)$ is a monoid

Circuit over monoid $(T,\circ)$:



- fanin $= 2$

- size $=$ number of gates in the circuit

- multi-output circuit

Our Results

Theorem (Lower Bounds for Circuits over free Monoids)

Let $S = \{y_1, ..., y_n\} \subseteq \{0,1\}^n$ be the explicit set of n strings. Any concatenation circuit that takes $X = \{0,1\}$ as input and outputs $y_1, ..., y_n$ will require size $\Omega(\frac{n^2}{\log^2 n})$.

Our Results

Theorem (Lower Bounds for Circuits over free Monoids)

Let $S = \{y_1, \ldots, y_n\} \subseteq \{0,1\}^n$ *be the explicit set of n strings. Any concatenation circuit that takes* $X = \{0,1\}$ *as input and outputs* $y_1, \ldots, y_n$ *will require size* $\Omega(\frac{n^2}{\log^2 n})$.

Theorem (Lower Bounds for Circuits over permutation group)

Any composition circuit over the permutation group $(S_N, \cdot)$, *with domain size* $N = 2^{\frac{n^2}{\log^2 n}}$, *that takes as input* π_0, π_1 *and computes* $G_S = \{\pi_{y_i} | y_i \in S\} \subseteq S_N$ *as output is of size* $\Omega(\frac{n^2}{\log^2 n})$.

Lower Bounds for Circuits over free Monoids

Circuits over free Monoids: $T = \{0,1\}^*$ and monoid operation is string concatenation.

Definition (Construction of S)

- Let $D = \{1, 2, ..., n^2\}$.
- Each $i \in [n^2]$ requires $\lceil 2\log_2 n \rceil$ bits to represent it in binary

Lower Bounds for Circuits over free Monoids

Circuits over free Monoids: $T = \{0,1\}^*$ and monoid operation is string concatenation.

Definition (Construction of S)

- Let $D = \{1, 2, ..., n^2\}$.
- Each $i \in [n^2]$ requires $\lceil 2\log_2 n \rceil$ bits to represent it in binary

for $i = 1, ..., n$ do

1. pick first $\frac{n}{2\log n}$ numbers from the current set D
2. concatenate their binary representation to obtain y_i
3. remove these numbers from D

end for

Lower Bounds for Circuits over free Monoids

Circuits over free Monoids: $T = \{0,1\}^*$ and monoid operation is string concatenation.

Definition (Construction of S)

- Let $D = \{1, 2, ..., n^2\}$.
- Each $i \in [n^2]$ requires $\lceil 2\log_2 n \rceil$ bits to represent it in binary

for $i = 1, ..., n$ do

1. pick first $\frac{n}{2\log n}$ numbers from the current set D
2. concatenate their binary representation to obtain y_i
3. remove these numbers from D

end for

- Each $y_i \in \{0,1\}^n$ constructed has the property that y_i has $\geq \frac{n}{2\log n}$ distinct substrings of length $2\log n$.

Lower Bounds for Circuits over free Monoids, contd

Lemma

Let $s \in X^n$ be any string where $|X| \geq 2$, such that the number of distinct substrings of s of length ℓ is N. Then any concatenation circuit for s will require $\Omega(\frac{N}{\ell})$ gates.

Lower Bounds for Circuits over free Monoids, contd

Lemma

Let $s \in X^n$ be any string where $|X| \geq 2$, such that the number of distinct substrings of s of length ℓ is N. Then any concatenation circuit for s will require $\Omega(\frac{N}{\ell})$ gates.

Proof Let C be a concatenation circuit computing s.

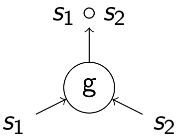
Lower Bounds for Circuits over free Monoids, contd

Lemma

Let $s \in X^n$ be any string where $|X| \geq 2$, such that the number of distinct substrings of s of length ℓ is N. Then any concatenation circuit for s will require $\Omega(\frac{N}{\ell})$ gates.

Proof Let C be a concatenation circuit computing s.

k_1 distinct substrings of length ℓ



k_2 distinct substrings of length ℓ

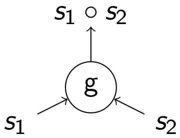
Lower Bounds for Circuits over free Monoids, contd

Lemma

Let $s \in X^n$ be any string where $|X| \geq 2$, such that the number of distinct substrings of s of length ℓ is N. Then any concatenation circuit for s will require $\Omega(\frac{N}{\ell})$ gates.

Proof Let C be a concatenation circuit computing s.

$k_1 + k_2 + \ell - 1$ distinct substrings of length ℓ



k_1 distinct substrings of length ℓ

k_2 distinct substrings of length ℓ

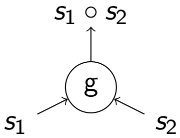
Lower Bounds for Circuits over free Monoids, contd

Lemma

Let $s \in X^n$ be any string where $|X| \geq 2$, such that the number of distinct substrings of s of length ℓ is N. Then any concatenation circuit for s will require $\Omega(\frac{N}{\ell})$ gates.

Proof Let C be a concatenation circuit computing s.

$k_1 + k_2 + \ell - 1$ distinct substrings of length ℓ



k_1 distinct substrings of length ℓ

k_2 distinct substrings of length ℓ

- \# of **new** substrings of length ℓ generated at any g is $\leq \ell - 1$

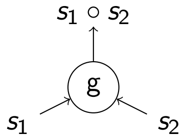
Lower Bounds for Circuits over free Monoids, contd

Lemma

Let $s \in X^n$ be any string where $|X| \geq 2$, such that the number of distinct substrings of s of length ℓ is N. Then any concatenation circuit for s will require $\Omega(\frac{N}{\ell})$ gates.

Proof Let C be a concatenation circuit computing s.

$k_1 + k_2 + \ell - 1$ distinct substrings of length ℓ



k_1 distinct substrings of length ℓ

k_2 distinct substrings of length ℓ

- $\#$ of **new** substrings of length ℓ generated at any g is $\leq \ell - 1$ and this gives, $|C| = \Omega(\frac{N}{\ell})$. $\blacksquare$

Lower Bounds for Circuits over free Monoids, contd

Theorem

Let $S = \{y_1, ..., y_n\} \subseteq \{0,1\}^n$ be the explicit set of n strings defined above. Any concatenation circuit that takes $X = \{0,1\}$ as input and outputs S at its n output gates will require size $\Omega(\frac{n^2}{\log^2 n})$.

Lower Bounds for Circuits over free Monoids, contd

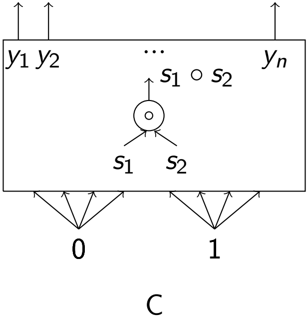
Theorem

Let $S = \{y_1, ..., y_n\} \subseteq \{0,1\}^n$ be the explicit set of n strings defined above. Any concatenation circuit that takes $X = \{0,1\}$ as input and outputs S at its n output gates will require size $\Omega(\frac{n^2}{\log^2 n})$.

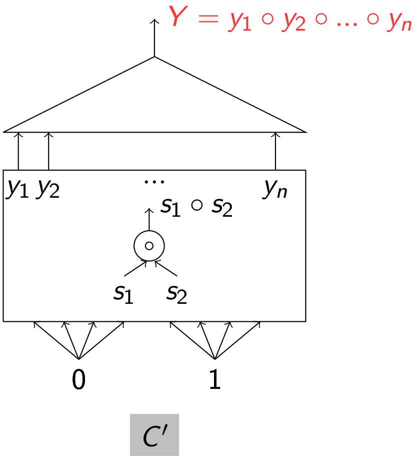
Proof

- Let C be a concatenation circuit computing S.
- Note that each $y_i \in S$ have $\Omega(\frac{n}{\log n})$ distinct substrings of length $O(\log n)$.
- In total $y_1, y_2, ..., y_n$ have $\Omega(\frac{n^2}{\log n})$ distinct substrings of length $O(\log n)$.

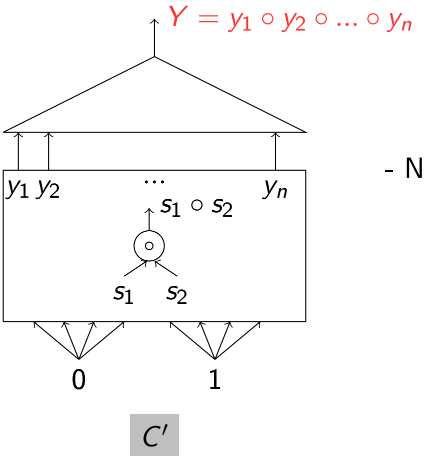
Lower Bounds for Circuits over free Monoids, contd



Lower Bounds for Circuits over free Monoids, contd

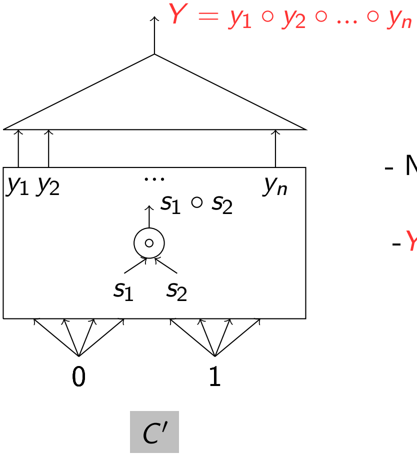


Lower Bounds for Circuits over free Monoids, contd



- Note that $|C'| \leq |C| + n - 1$

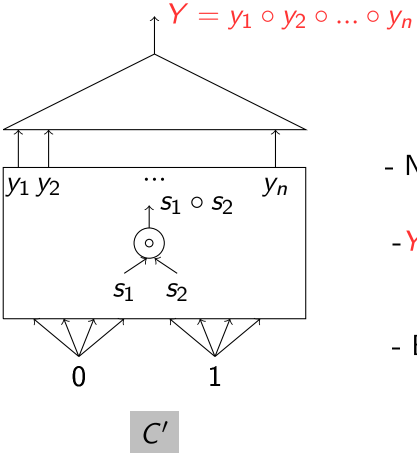
Lower Bounds for Circuits over free Monoids, contd



- Note that $|C'| \leq |C| + n - 1$

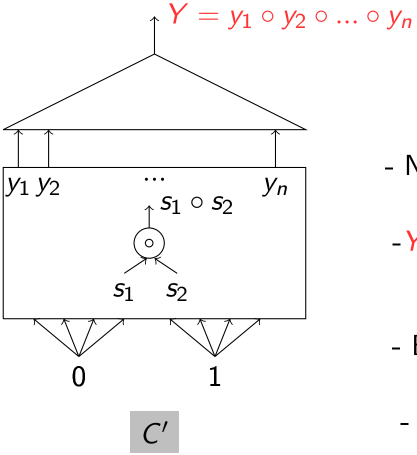
- Y have $\Omega(\frac{n^2}{\log n})$ distinct substrings of length $O(\log n)$

Lower Bounds for Circuits over free Monoids, contd



- Note that $|C'| \leq |C| + n - 1$
- Y have $\Omega(\frac{n^2}{\log n})$ distinct substrings of length $O(\log n)$
- By Lemma, $|C'| = \Omega(\frac{n^2}{\log^2 n})$

Lower Bounds for Circuits over free Monoids, contd



- Note that $|C'| \leq |C| + n - 1$

- Y have $\Omega(\frac{n^2}{\log n})$ distinct substrings of length $O(\log n)$

- By Lemma, $|C'| = \Omega(\frac{n^2}{\log^2 n})$

- This gives, $|C| = \Omega(\frac{n^2}{\log^2 n})$ ■

2. Circuits over permutation groups

Circuits over permutation groups:

- $S = S_N$ where S_N is a permutation group with domain size N
- operation is composition

2. Circuits over permutation groups

Circuits over permutation groups:

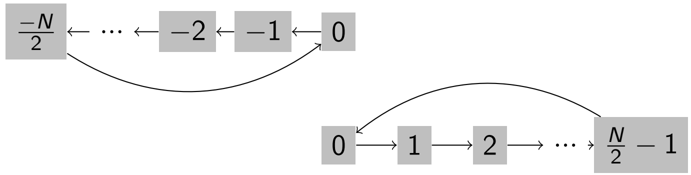
- $S = S_N$ where S_N is a permutation group with domain size N
- operation is composition

Definition of generating elements: π_0 and π_1

- Let $D = \{-\frac{N}{2}, -(\frac{N}{2}-1), ..., -1, 0, 1, ..., \frac{N}{2}-1\}$

π_0

π_1



- Let $y = 101$. By π_y we mean the permutation $\pi_1\pi_0\pi_1$.

Definition: $G_S = \{\pi_{y_i} | y_i \in S\}$, where the set S be the explicit set of n strings defined before.

Goal: To compute G_S using composition circuits

Theorem

Any composition circuit over the permutation group $(S_N, \cdot)$, with domain size $N = 2^{\frac{n^2}{\log^2 n}}$, that takes as input π_0, π_1 and computes $G_S = \{\pi_{y_i} | y_i \in S\} \subseteq S_N$ as output is of size $\Omega(\frac{n^2}{\log^2 n})$.

Theorem

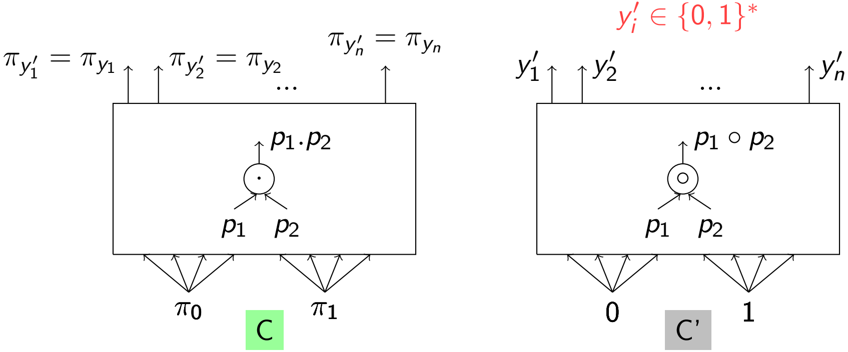
Any composition circuit over the permutation group $(S_N, \cdot)$*, with domain size* $N = 2^{\frac{n^2}{\log^2 n}}$*, that takes as input* π_0, π_1 *and computes* $G_S = \{\pi_{y_i} | y_i \in S\} \subseteq S_N$ *as output is of size* $\Omega(\frac{n^2}{\log^2 n})$*.*

Proof:- Let C be a composition circuit computing G_S.

Theorem

Any composition circuit over the permutation group $(S_N, \cdot)$, with domain size $N = 2^{\frac{n^2}{\log^2 n}}$, that takes as input π_0, π_1 and computes $G_S = \{\pi_{y_i} | y_i \in S\} \subseteq S_N$ as output is of size $\Omega(\frac{n^2}{\log^2 n})$.

Proof:- Let C be a composition circuit computing G_S.



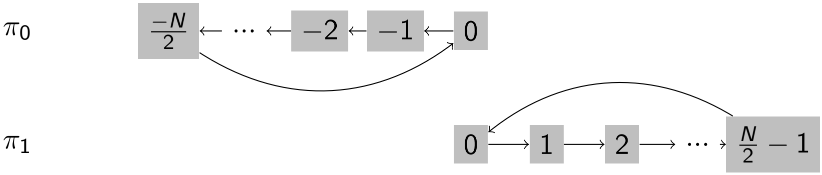
- Note that $|C| = |C'|$.

- Suppose in C', if $\forall i \in [n]$, $y_i' = y_i \in S$ then C' is a concatenation circuit computing $S = \{y_1, ..., y_n\}$.
- By Theorem, $|C'| = \Omega(\frac{n^2}{\log^2 n}) \implies |C| = \Omega(\frac{n^2}{\log^2 n})$.

- Suppose in C', if $\forall i \in [n]$, $y'_i = y_i \in S$ then C' is a concatenation circuit computing $S = \{y_1, ..., y_n\}$.
- By Theorem, $|C'| = \Omega(\frac{n^2}{\log^2 n}) \implies |C| = \Omega(\frac{n^2}{\log^2 n})$.
- Otherwise in C', $\exists i \in [n]$, $y'_i \neq y_i$.
- Let $\pi_{y_i} = v.b_1.s$, $\pi_{y'_i} = u.b_2.s$, where $b_1 \neq b_2$.
- w.l.o.g, assume that $b_1 = \pi_0$ and $b_2 = \pi_1$.

- Suppose in C', if $\forall i \in [n]$, $y'_i = y_i \in S$ then C' is a concatenation circuit computing $S = \{y_1, ..., y_n\}$.
- By Theorem, $|C'| = \Omega(\frac{n^2}{\log^2 n}) \implies |C| = \Omega(\frac{n^2}{\log^2 n})$.
- Otherwise in C', $\exists i \in [n]$, $y'_i \neq y_i$.
- Let $\pi_{y_i} = v.b_1.s$, $\pi_{y'_i} = u.b_2.s$, where $b_1 \neq b_2$.
- w.l.o.g, assume that $b_1 = \pi_0$ and $b_2 = \pi_1$.
- $D = \{-\frac{N}{2}, -(\frac{N}{2} - 1), ..., -1, 0, 1, ..., \frac{N}{2} - 1\}$

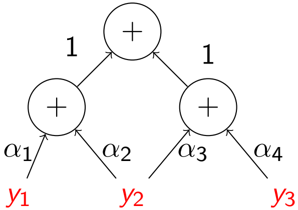
- Suppose in C', if $\forall i \in [n]$, $y'_i = y_i \in S$ then C' is a concatenation circuit computing $S = \{y_1, \dots, y_n\}$.
- By Theorem, $|C'| = \Omega(\frac{n^2}{\log^2 n}) \implies |C| = \Omega(\frac{n^2}{\log^2 n})$.
- Otherwise in C', $\exists i \in [n]$, $y'_i \neq y_i$.
- Let $\pi_{y_i} = v.b_1.s$, $\pi_{y'_i} = u.b_2.s$, where $b_1 \neq b_2$.
- w.l.o.g, assume that $b_1 = \pi_0$ and $b_2 = \pi_1$.
- $D = \{-\frac{N}{2}, -(\frac{N}{2} - 1), \dots, -1, 0, 1, \dots, \frac{N}{2} - 1\}$



- Thus, u have at least $(\frac{N}{2} - 1)$ copies of π_1 and since fanin is 2, $|C| \geq \Omega(\log(\frac{N}{2} - 1))$, where $N = 2^{\frac{n^2}{\log^2 n}}$. $\blacksquare$

Linear Circuits over Rings

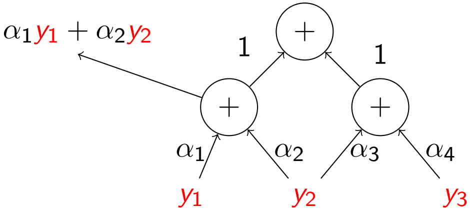
Example: Linear circuit over noncommutative ring R



where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in R$.

Linear Circuits over Rings

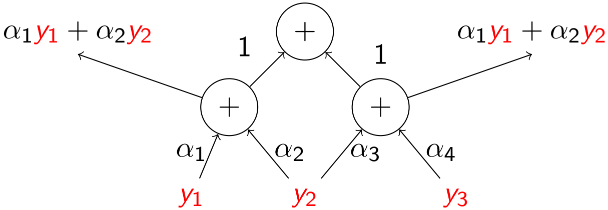
Example: Linear circuit over noncommutative ring R



where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in R$.

Linear Circuits over Rings

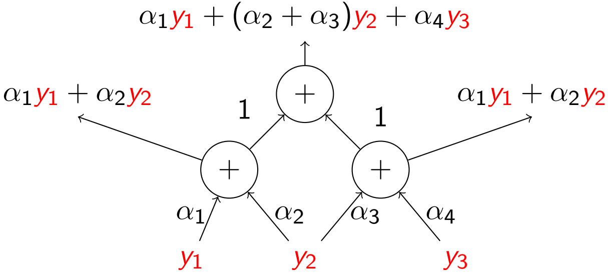
Example: Linear circuit over noncommutative ring R



where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in R$.

Linear Circuits over Rings

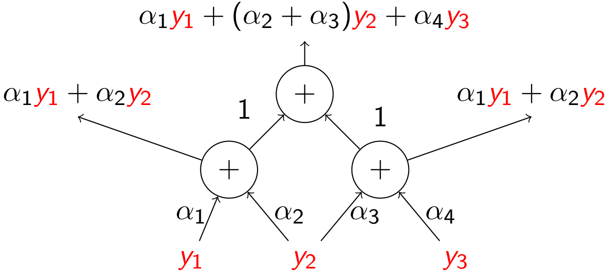
Example: Linear circuit over noncommutative ring R



where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in R$.

Linear Circuits over Rings

Example: Linear circuit over noncommutative ring R



- fanin $= 2$
- size $=$ number of gates in the circuit
- multi-output circuit

where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in R$.

Linear Circuits over Rings , contd

- When R is a field, we get the well-studied linear circuits model (see Satya Lokam's 2009 survey).
- No explicit superlinear size lower bounds are known for this model over fields (except for some special cases like the bounded coefficient model [Morgenstern'73])
- When the coefficients to come from a *noncommutative* ring $R = \mathbb{F}\langle x_0, x_1 \rangle$, we prove lower bounds for certain restricted linear circuits.

Linear Circuits over Rings, contd

Definition (Homogeneous polynomials)

A polynomial $P \in \mathbb{F}\langle x_0, x_1 \rangle$ is called homogeneous if degree of each monomial in P is the same.

Linear Circuits over Rings, contd

Definition (Homogeneous polynomials)

A polynomial $P \in \mathbb{F}\langle x_0, x_1\rangle$ is called homogeneous if degree of each monomial in P is the same.

Example:

- Homogeneous polynomials: $x_1^{10} + x_0^5 x_1^5$

Linear Circuits over Rings, contd

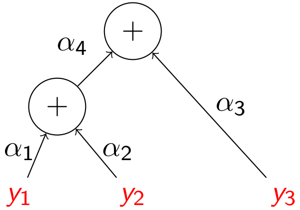
Definition (Homogeneous polynomials)

A polynomial $P \in \mathbb{F}\langle x_0, x_1 \rangle$ is called homogeneous if degree of each monomial in P is the same.

Example:

- Homogeneous polynomials: $x_1^{10} + x_0^5 x_1^5$
- Non-homogeneous polynomials: $x_1^2 + x_0$

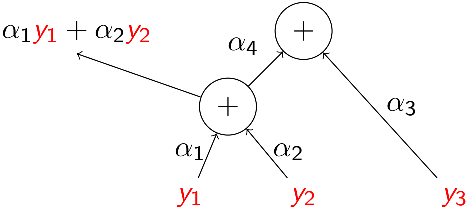
Homogeneous Linear Circuits over $\mathbb{F}\langle x_0, x_1 \rangle$



where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}\langle x_0, x_1 \rangle$.

- each gate g of the circuit computes a linear form $\sum_{i=1}^{n} \beta_i y_i$, where the $\beta_i \in \mathbb{F}\langle x_0, x_1 \rangle$ are all homogeneous polynomials of the same degree.

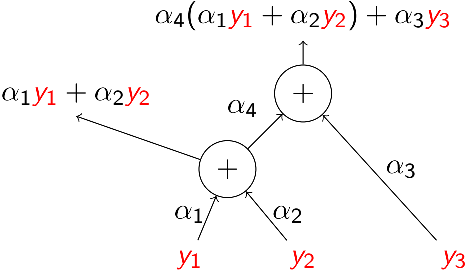
Homogeneous Linear Circuits over $\mathbb{F}\langle x_0, x_1 \rangle$



where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}\langle x_0, x_1 \rangle$.

- each gate g of the circuit computes a linear form $\sum_{i=1}^{n} \beta_i y_i$, where the $\beta_i \in \mathbb{F}\langle x_0, x_1 \rangle$ are all homogeneous polynomials of the same degree.

Homogeneous Linear Circuits over $\mathbb{F}\langle x_0, x_1\rangle$



where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}\langle x_0, x_1\rangle$.

- each gate g of the circuit computes a linear form $\sum_{i=1}^{n} \beta_i y_i$, where the $\beta_i \in \mathbb{F}\langle x_0, x_1\rangle$ are all homogeneous polynomials of the same degree.

Linear Circuits over Rings, contd

- Our goal is to construct an explicit matrix $M \in \mathbb{F}^{n\times n}\langle x_0, x_1\rangle$ such that MY, where $Y = (y_1, y_2, \ldots, y_n)^T$ is a column vector of input variables, can not be computed by any homogeneous linear circuit C with size $O(n)$ and depth $O(\log n)$.

Linear Circuits over Rings, contd

- Our goal is to construct an explicit matrix $M \in \mathbb{F}^{n \times n}\langle x_0, x_1 \rangle$ such that MY, where $Y = (y_1, y_2, \ldots, y_n)^T$ is a column vector of input variables, can not be computed by any homogeneous linear circuit C with size $O(n)$ and depth $O(\log n)$.
- proved by suitably generalizing Valiant's matrix rigidity method.

Linear Circuits over Rings, contd

- Our goal is to construct an explicit matrix $M \in \mathbb{F}^{n\times n}\langle x_0, x_1\rangle$ such that MY, where $Y = (y_1, y_2, \ldots, y_n)^T$ is a column vector of input variables, can not be computed by any homogeneous linear circuit C with size $O(n)$ and depth $O(\log n)$.
- proved by suitably generalizing Valiant's matrix rigidity method.

Notation

Consider $n \times n$ matrices $\mathbb{F}^{n\times n}$ over field $\mathbb{F}$. The support of a matrix $A \in \mathbb{F}^{n\times n}$ is the set of locations $\mathrm{supp}(A) = \{(i,j) \mid A_{ij} \neq 0\}$.

Definition (Rigidity of a matrix)

Let $\mathbb{F}$ be any field. The rigidity of a matrix $A \in \mathbb{F}^{n \times n}$, denoted by $\mathcal{R}_r(A)$, is the smallest number t for which there are set of t positions $S \subseteq [n] \times [n]$ and a matrix E such that:

- $\mathrm{supp}(E) \subseteq S$
- rank of $A + E$ is upper bounded by r.

Linear Circuits over Rings, contd

Definition (Rigidity of a deck of matrices)

Let $\mathbb{F}$ be any field. The rigidity $\rho_r(D)$ of a deck of matrices $D = \{A_1, A_2, \ldots, A_N\} \subseteq \mathbb{F}^{n \times n}$ is the smallest number t for which there are set of t positions $S \subseteq [n] \times [n]$ and a deck of matrices $E = \{E_1, E_2, \ldots, E_N\}$ such that for all i:

- $\mathrm{supp}(E_i) \subseteq S$
- rank of $A_i + E_i$ is upper bounded by r.

Linear Circuits over Rings, contd

Definition (Rigidity of a deck of matrices)

Let $\mathbb{F}$ be any field. The rigidity $\rho_r(D)$ of a deck of matrices $D = \{A_1, A_2, \ldots, A_N\} \subseteq \mathbb{F}^{n \times n}$ is the smallest number t for which there are set of t positions $S \subseteq [n] \times [n]$ and a deck of matrices $E = \{E_1, E_2, \ldots, E_N\}$ such that for all i:

- $\mathrm{supp}(E_i) \subseteq S$
- rank of $A_i + E_i$ is upper bounded by r.

Definition (Rigid deck)

A deck of matrices $D = \{A_1, A_2, \ldots, A_N\} \subseteq \mathbb{F}^{n \times n}$ is called *rigid deck* if $\rho_{\epsilon \cdot n}(D) = \Omega(n^{2-o(1)})$, where $\epsilon > 0$ is a constant.

Linear Circuits over Rings, contd

Definition (Rigidity of a deck of matrices)

Let $\mathbb{F}$ be any field. The rigidity $\rho_r(D)$ of a deck of matrices $D = \{A_1, A_2, \ldots, A_N\} \subseteq \mathbb{F}^{n \times n}$ is the smallest number t for which there are set of t positions $S \subseteq [n] \times [n]$ and a deck of matrices $E = \{E_1, E_2, \ldots, E_N\}$ such that for all i:

- $\mathrm{supp}(E_i) \subseteq S$
- rank of $A_i + E_i$ is upper bounded by r.

Definition (Rigid deck)

A deck of matrices $D = \{A_1, A_2, \ldots, A_N\} \subseteq \mathbb{F}^{n \times n}$ is called *rigid deck* if $\rho_{\epsilon \cdot n}(D) = \Omega(n^{2-o(1)})$, where $\epsilon > 0$ is a constant.

- Notice that for $N = 1$, this is the notion of rigid matrices.

Linear Circuits over Rings, contd

Definition (Construction of a Rigid deck)

Let $D = \{A_m \mid m \in \{x_0, x_1\}^{n^2}\}$ with matrices A_m indexed by string m of length n^2. The matrix A_m is defined as follows: $1 \leq i, j \leq n$

$$A_m[i,j] = \begin{cases} 1 & \text{if } m_{ni+j} = x_1 \\ 0 & \text{if } m_{ni+j} = x_0 \end{cases}$$

Linear Circuits over Rings, contd

Definition (Construction of a Rigid deck)

Let $D = \{A_m \mid m \in \{x_0, x_1\}^{n^2}\}$ with matrices A_m indexed by string m of length n^2. The matrix A_m is defined as follows: $1 \leq i, j \leq n$

$$A_m[i,j] = \begin{cases} 1 & \text{if } m_{ni+j} = x_1 \\ 0 & \text{if } m_{ni+j} = x_0 \end{cases}$$

- For each $k \in \{x_0, x_1\}^{n^2}$ and each $1 \leq i, j \leq n$ there is a polynomial (in n) time algorithm that outputs the $(i,j)^{th}$ entry of A_k. We call such a deck D as an explicit deck.

Linear Circuits over Rings, contd

Definition (Construction of a Rigid deck)

Let $D = \{A_m \mid m \in \{x_0, x_1\}^{n^2}\}$ with matrices A_m indexed by string m of length n^2. The matrix A_m is defined as follows: $1 \leq i, j \leq n$

$$A_m[i,j] = \begin{cases} 1 & \text{if } m_{ni+j} = x_1 \\ 0 & \text{if } m_{ni+j} = x_0 \end{cases}$$

- For each $k \in \{x_0, x_1\}^{n^2}$ and each $1 \leq i, j \leq n$ there is a polynomial (in n) time algorithm that outputs the $(i,j)^{th}$ entry of A_k. We call such a deck D as an explicit deck.

Lemma

The above deck $D = \{A_m \mid m \in \{x_0, x_1\}^{n^2}\}$ is an explicit rigid deck for any field $\mathbb{F}$.

Linear Circuits over Rings, contd

- We now turn to the lower bound result for homogeneous linear circuits where the coefficient ring is $\mathbb{F}\langle x_0, x_1\rangle$.

- WANT: an explicit matrix $M \in \mathbb{F}^{n\times n}\langle x_0, x_1\rangle$ such that MY, where Y is a vector of input variables, can not be computed by any homogeneous linear circuits C with size $O(n)$ and depth $O(\log n)$.

Linear Circuits over Rings, contd

- We now turn to the lower bound result for homogeneous linear circuits where the coefficient ring is $\mathbb{F}\langle x_0, x_1\rangle$.
- WANT: an explicit matrix $M \in \mathbb{F}^{n\times n}\langle x_0, x_1\rangle$ such that MY, where Y is a vector of input variables, can not be computed by any homogeneous linear circuits C with size $O(n)$ and depth $O(\log n)$.

Definition (of matrix M)

We define an explicit $n \times n$ matrix M as $M = \sum_{m\in\{x_0,x_1\}^{n^2}} A_m m$, where $D = \{A_m \mid m \in \{x_0, x_1\}^{n^2}\}$ is the deck defined before

- each entry of matrix M can be expressed as

$$M_{ij} = (x_0 + x_1)^{(i-1)n+j-1} \cdot x_1 \cdot (x_0 + x_1)^{n^2-((i-1)n+j)}.$$

Theorem

Any homogeneous linear circuit C over the coefficient ring $\mathbb{F}\langle x_0, x_1 \rangle$ computing MY, for M defined before, requires either size $\omega(n)$ or depth $\omega(\log n)$.

Theorem

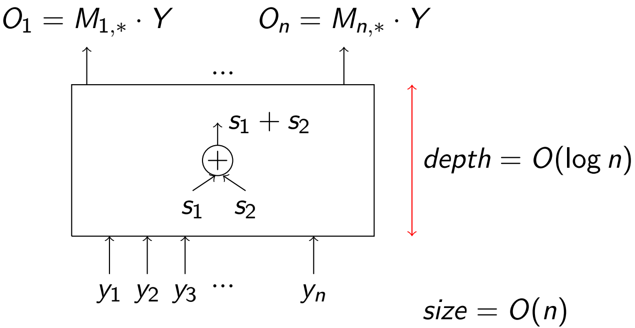
Any homogeneous linear circuit C over the coefficient ring $\mathbb{F}\langle x_0, x_1\rangle$ computing MY, for M defined before, requires either size $\omega(n)$ or depth $\omega(\log n)$.

Proof Proof by contradiction. Let C is a homogeneous linear circuit of size $O(n)$ and depth $O(\log n)$ computing MY.

Theorem

Any homogeneous linear circuit C over the coefficient ring $\mathbb{F}\langle x_0, x_1 \rangle$ computing MY, for M defined before, requires either size $\omega(n)$ or depth $\omega(\log n)$.

Proof Proof by contradiction. Let C is a homogeneous linear circuit of size $O(n)$ and depth $O(\log n)$ computing MY.



C computing $M \cdot Y$

- By Valiant's graph-theoretic argument, in the circuit C there is a set of gates V of cardinality $s = \frac{c_1 n}{\log \log n} = o(n)$ such that at least $n^2 - n^{1+\delta}$, for $\delta < 1$, input-output pairs have all their paths going through V.

- By Valiant's graph-theoretic argument, in the circuit C there is a set of gates V of cardinality $s = \frac{c_1 n}{\log \log n} = o(n)$ such that at least $n^2 - n^{1+\delta}$, for $\delta < 1$, input-output pairs have all their paths going through V.
- Thus, we can write $M = B_1 B_2 + E$, where
  - $B_1 \in \mathbb{F}^{n \times s}\langle x_0, x_1 \rangle$ and
  - $B_2 \in \mathbb{F}^{s \times n}\langle x_0, x_1 \rangle$
  - $E \in \mathbb{F}^{n \times n}\langle x_0, x_1 \rangle$ and $|\mathrm{supp}(E)| \leq n^{1+\delta}$

- Write matrices M, E and B_1B_2 as a polynomial with matrix coefficients.

Example:

$$\begin{pmatrix} 6x_0 + x_1 & x_0 \\ 8x_1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 0 & 0 \end{pmatrix} x_0 + \begin{pmatrix} 1 & 0 \\ 8 & 0 \end{pmatrix} x_1$$

- $M = \sum_{m \in \{x_0, x_1\}^{n^2}} A_m \cdot m$, where $A_m \in \mathcal{A}$
- $B_1B_2 = \sum_{m \in \{x_0, x_1\}^{n^2}} B_m \cdot m$
- $E = \sum_{m \in \{x_0, x_1\}^{n^2}} E_m \cdot m$, $|\cup_{m \in \{x_0, x_1\}^{n^2}} \mathrm{supp}(E_m)| \leq n^{1+\delta}$

- Write matrices M,E and B_1B_2 as a polynomial with matrix coefficients.

Example:

$$\begin{pmatrix} 6x_0 + x_1 & x_0 \\ 8x_1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 0 & 0 \end{pmatrix} x_0 + \begin{pmatrix} 1 & 0 \\ 8 & 0 \end{pmatrix} x_1$$

- $M = \sum_{m \in \{x_0,x_1\}^{n^2}} A_m \cdot m$, where $A_m \in \mathcal{A}$
- $B_1B_2 = \sum_{m \in \{x_0,x_1\}^{n^2}} B_m \cdot m$
- $E = \sum_{m \in \{x_0,x_1\}^{n^2}} E_m \cdot m$, $|\cup_{m \in \{x_0,x_1\}^{n^2}} \mathrm{supp}(E_m)| \leq n^{1+\delta}$
- Note that, $A_m = B_m + E_m \implies B_m = A_m - E_m$.

- Write matrices M,E and B_1B_2 as a polynomial with matrix coefficients.

Example:

$$\begin{pmatrix} 6x_0+x_1 & x_0 \\ 8x_1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 0 & 0 \end{pmatrix} x_0 + \begin{pmatrix} 1 & 0 \\ 8 & 0 \end{pmatrix} x_1$$

- $M = \sum_{m \in \{x_0,x_1\}^{n^2}} A_m \cdot m$, where $A_m \in \mathcal{A}$
- $B_1B_2 = \sum_{m \in \{x_0,x_1\}^{n^2}} B_m \cdot m$
- $E = \sum_{m \in \{x_0,x_1\}^{n^2}} E_m \cdot m$, $|\cup_{m \in \{x_0,x_1\}^{n^2}} \mathrm{supp}(E_m)| \leq n^{1+\delta}$
- Note that, $A_m = B_m + E_m \implies B_m = A_m - E_m$.

Rest of the proof:

- We show that for each m, rank of B_m is $\leq s = o(n)$.

- Write matrices M,E and B_1B_2 as a polynomial with matrix coefficients.

Example:

$$\begin{pmatrix} 6x_0 + x_1 & x_0 \\ 8x_1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 0 & 0 \end{pmatrix} x_0 + \begin{pmatrix} 1 & 0 \\ 8 & 0 \end{pmatrix} x_1$$

- $M = \sum_{m \in \{x_0,x_1\}^{n^2}} A_m \cdot m$, where $A_m \in \mathcal{A}$
- $B_1B_2 = \sum_{m \in \{x_0,x_1\}^{n^2}} B_m \cdot m$
- $E = \sum_{m \in \{x_0,x_1\}^{n^2}} E_m \cdot m$, $|\cup_{m \in \{x_0,x_1\}^{n^2}} \mathrm{supp}(E_m)| \leq n^{1+\delta}$
- Note that, $A_m = B_m + E_m \implies B_m = A_m - E_m$.

Rest of the proof:

- We show that for each m, rank of B_m is $\leq s = o(n)$.
- we know that, $|\mathrm{supp}(E_m)| \leq n^{1+\delta}$.

- Write matrices M,E and B_1B_2 as a polynomial with matrix coefficients.

Example:

$$\begin{pmatrix} 6x_0 + x_1 & x_0 \\ 8x_1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 0 & 0 \end{pmatrix} x_0 + \begin{pmatrix} 1 & 0 \\ 8 & 0 \end{pmatrix} x_1$$

- $M = \sum_{m \in \{x_0,x_1\}^{n^2}} A_m \cdot m$, where $A_m \in \mathcal{A}$
- $B_1B_2 = \sum_{m \in \{x_0,x_1\}^{n^2}} B_m \cdot m$
- $E = \sum_{m \in \{x_0,x_1\}^{n^2}} E_m \cdot m$, $|\cup_{m \in \{x_0,x_1\}^{n^2}} \mathrm{supp}(E_m)| \leq n^{1+\delta}$
- Note that, $A_m = B_m + E_m \implies B_m = A_m - E_m$.

Rest of the proof:

- We show that for each m, rank of B_m is $\leq s = o(n)$.
- we know that, $|\mathrm{supp}(E_m)| \leq n^{1+\delta}$. This contradicts the fact that $\mathcal{A}$ is a rigid deck. ■

Summary:-

- We have shown lower bounds for
  - multiplicative circuits over monoids, permutation groups, free groups, matrix semigroups
  - linear circuit over noncommutative rings

Summary:-

- We have shown lower bounds for
  - multiplicative circuits over monoids, permutation groups, free groups, matrix semigroups
  - linear circuit over noncommutative rings

Open Problems

- To give explicit constructions for smaller rigid decks of $n \times n$ matrices, say, $poly(n)$ sized decks.

Summary:-

- We have shown lower bounds for
  - multiplicative circuits over monoids, permutation groups, free groups, matrix semigroups
  - linear circuit over noncommutative rings

Open Problems

- To give explicit constructions for smaller rigid decks of $n \times n$ matrices, say, $poly(n)$ sized decks. Or
  is the construction of rigid decks of smaller size equivalent to the original matrix rigidity problem?

Summary:-

- We have shown lower bounds for
  - multiplicative circuits over monoids, permutation groups, free groups, matrix semigroups
  - linear circuit over noncommutative rings

Open Problems

- To give explicit constructions for smaller rigid decks of $n \times n$ matrices, say, $poly(n)$ sized decks. Or
  is the construction of rigid decks of smaller size equivalent to the original matrix rigidity problem?

Thank you.

Linear Circuits over Rings, contd

Lemma

The deck $\mathcal{A} = \{A_m \mid m \in \{x_0, x_1\}^{n^2}\}$ *is an explicit rigid deck for any field* $\mathbb{F}$.

Linear Circuits over Rings, contd

Lemma

The deck $\mathcal{A} = \{A_m \mid m \in \{x_0, x_1\}^{n^2}\}$ *is an explicit rigid deck for any field* $\mathbb{F}$.

Proof:-

- Valiant showed that almost all $n \times n$ 0-1 matrices A over any field $\mathbb{F}$ have rigidity $\rho_r(A) = \Omega(\frac{(n-r)^2}{\log n})$ for target rank r.
- In particular, for $r = \epsilon \cdot n$, over any field $\mathbb{F}$, there is a 0-1 matrix R for which we have $\rho_r(R) \geq \frac{\delta \cdot n^2}{\log n}$ for some constant $\delta > 0$ depending on ϵ.

Linear Circuits over Rings, contd

Lemma

The deck $\mathcal{A} = \{A_m \mid m \in \{x_0, x_1\}^{n^2}\}$ *is an explicit rigid deck for any field* $\mathbb{F}$*.*

Proof:-

- Valiant showed that almost all $n \times n$ 0-1 matrices A over any field $\mathbb{F}$ have rigidity $\rho_r(A) = \Omega(\frac{(n-r)^2}{\log n})$ for target rank r.
- In particular, for $r = \epsilon \cdot n$, over any field $\mathbb{F}$, there is a 0-1 matrix R for which we have $\rho_r(R) \geq \frac{\delta \cdot n^2}{\log n}$ for some constant $\delta > 0$ depending on ϵ.
- We claim that for the deck $\mathcal{A}$ we have $\rho_{\epsilon n}(\mathcal{A}) \geq \frac{\delta \cdot n^2}{\log n}$.

- To see this, $S \subseteq [n] \times [n]$ such that $|S| < \frac{\delta n^2}{\log n}$
- Let $E = \{E_m \in \mathbb{F}^{n \times n} | m \in \{x_0, x_1\}^{n^2}\}$ be any collection of matrices such that:
  - $\mathrm{supp}(E_m) \subseteq S$
  - Thus, we have for each m, $|\mathrm{supp}(E_m)| < \frac{\delta n^2}{\log n}$
- Since the deck $\mathcal{A}$ contains all 0-1 matrices, in particular $R \in \mathcal{A}$ and $R = A_m$ for some monomial m.
- From the rigidity of R we know that the rank of $R + E_m$ is at least ϵn.

This proves the claim and the lemma follows. ■

Rank of B_m is $\leq s$

- We now analyze the matrices B_m.

Rank of B_m is $\leq s$

- We now analyze the matrices B_m.
- By the homogeneity condition on the circuit C, we can partition $V = V_1 \cup V_2 \cup \ldots V_\ell$, where each gate g in V_i computes a linear form $\sum_{j=1}^{n} \gamma_j y_j$ and $\gamma_j \in \mathbb{F}\langle x_0, x_1 \rangle$ is a homogeneous degree d_i polynomial.
- Let $s_i = |V_i|, 1 \leq i \leq \ell$. Then we have $s = s_1 + s_2 + \ldots s_\ell$.

Rank of B_m is $\leq s$

- We now analyze the matrices B_m.
- By the homogeneity condition on the circuit C, we can partition $V = V_1 \cup V_2 \cup \dots V_\ell$, where each gate g in V_i computes a linear form $\sum_{j=1}^{n} \gamma_j y_j$ and $\gamma_j \in \mathbb{F}\langle x_0, x_1 \rangle$ is a homogeneous degree d_i polynomial.
- Let $s_i = |V_i|, 1 \leq i \leq \ell$. Then we have $s = s_1 + s_2 + \dots s_\ell$.
- Every monomial m has a unique prefix of length d_i for each degree d_i.
  - Thus, we can write $B_m = \sum_{j=1}^{\ell} B_{m,j,1} B_{m,j,2}$, where
    - $B_{m,j,1}$ is the $n \times s_j$ matrix corresponding to the d_j-prefix of m
    - $B_{m,j,2}$ is the $s_j \times n$ matrix corresponding to the $n^2 - d_j$-suffix of m.

Rank of B_m is $\leq s$

- We now analyze the matrices B_m.
- By the homogeneity condition on the circuit C, we can partition $V = V_1 \cup V_2 \cup \ldots V_\ell$, where each gate g in V_i computes a linear form $\sum_{j=1}^{n} \gamma_j y_j$ and $\gamma_j \in \mathbb{F}\langle x_0, x_1 \rangle$ is a homogeneous degree d_i polynomial.
- Let $s_i = |V_i|, 1 \leq i \leq \ell$. Then we have $s = s_1 + s_2 + \ldots s_\ell$.
- Every monomial m has a unique prefix of length d_i for each degree d_i.
  - Thus, we can write $B_m = \sum_{j=1}^{\ell} B_{m,j,1} B_{m,j,2}$, where
    - $B_{m,j,1}$ is the $n \times s_j$ matrix corresponding to the d_j-prefix of m
    - $B_{m,j,2}$ is the $s_j \times n$ matrix corresponding to the $n^2 - d_j$-suffix of m.
- It follows that for each monomial m the rank of B_m is bounded by s.

Rank of B_m is $\leq s$

- We now analyze the matrices B_m.
- By the homogeneity condition on the circuit C, we can partition $V = V_1 \cup V_2 \cup \ldots V_\ell$, where each gate g in V_i computes a linear form $\sum_{j=1}^{n} \gamma_j y_j$ and $\gamma_j \in \mathbb{F}\langle x_0, x_1 \rangle$ is a homogeneous degree d_i polynomial.
- Let $s_i = |V_i|, 1 \leq i \leq \ell$. Then we have $s = s_1 + s_2 + \ldots s_\ell$.
- Every monomial m has a unique prefix of length d_i for each degree d_i.
  - Thus, we can write $B_m = \sum_{j=1}^{\ell} B_{m,j,1} B_{m,j,2}$, where
    - $B_{m,j,1}$ is the $n \times s_j$ matrix corresponding to the d_j-prefix of m
    - $B_{m,j,2}$ is the $s_j \times n$ matrix corresponding to the $n^2 - d_j$-suffix of m.
- It follows that for each monomial m the rank of B_m is bounded by s.

Putting it together, for each monomial m we have $A_m = B_m + E_m$, where B_m is rank s and $|\cup_{m \in \{x_0, x_1\}^{n^2}} \mathrm{supp}(E_m)| \leq n^{1+\delta}$.

Rank of B_m is $\leq s$

- We now analyze the matrices B_m.
- By the homogeneity condition on the circuit C, we can partition $V = V_1 \cup V_2 \cup \ldots V_\ell$, where each gate g in V_i computes a linear form $\sum_{j=1}^{n} \gamma_j y_j$ and $\gamma_j \in \mathbb{F}\langle x_0, x_1 \rangle$ is a homogeneous degree d_i polynomial.
- Let $s_i = |V_i|, 1 \leq i \leq \ell$. Then we have $s = s_1 + s_2 + \ldots s_\ell$.
- Every monomial m has a unique prefix of length d_i for each degree d_i.
  - Thus, we can write $B_m = \sum_{j=1}^{\ell} B_{m,j,1} B_{m,j,2}$, where
    - $B_{m,j,1}$ is the $n \times s_j$ matrix corresponding to the d_j-prefix of m
    - $B_{m,j,2}$ is the $s_j \times n$ matrix corresponding to the $n^2 - d_j$-suffix of m.
- It follows that for each monomial m the rank of B_m is bounded by s.

Putting it together, for each monomial m we have $A_m = B_m + E_m$, where B_m is rank s and $|\cup_{m \in \{x_0,x_1\}^{n^2}} \mathrm{supp}(E_m)| \leq n^{1+\delta}$. This contradicts the fact that $\mathcal{A}$ is a rigid deck. ∎