

Classical and quantum streaming complexity of Max- Cut

Qualifying Oral Exam

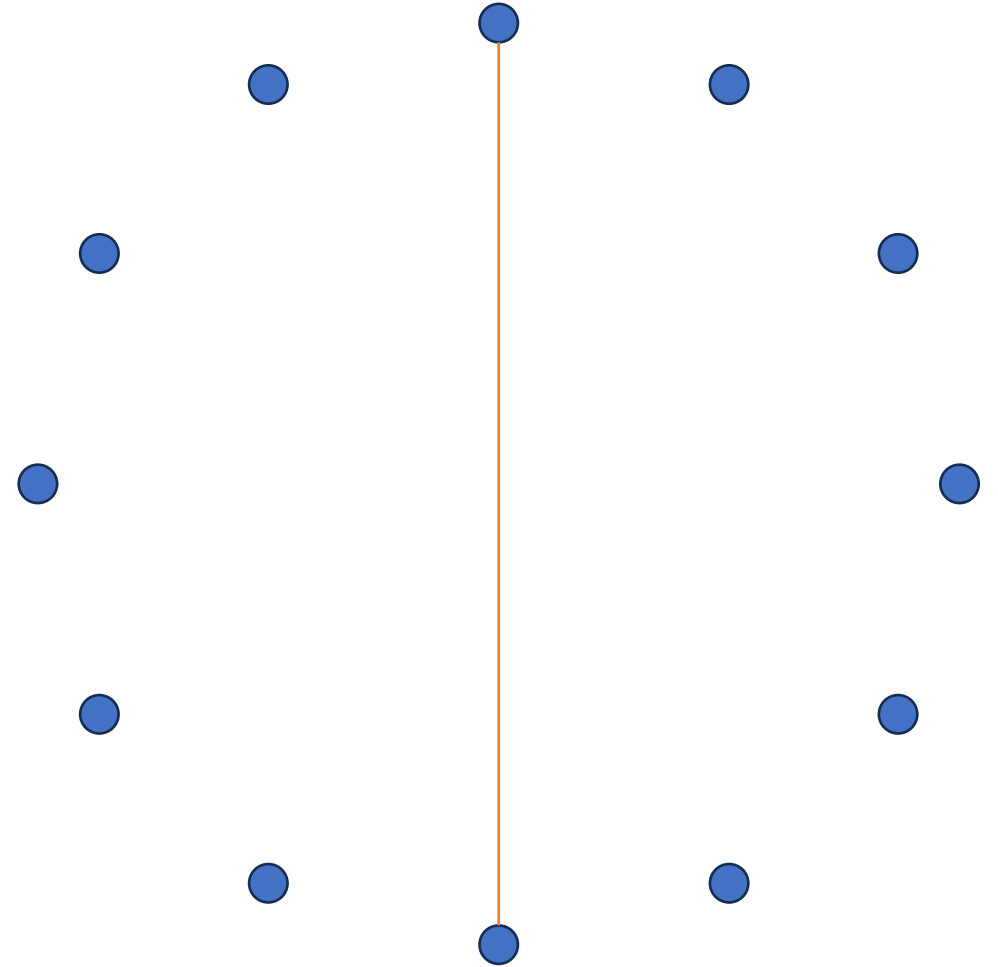
Nadya Voronova

This talk is based on

1. Kapralov, Krachun, STOC 2019
“An Optimal Space Lower Bound for Approximating MAX-CUT”
2. Kallaugher, Parekh, FOCS 2022
“The Quantum and Classical Streaming Complexity of Quantum and Classical Max-Cut”

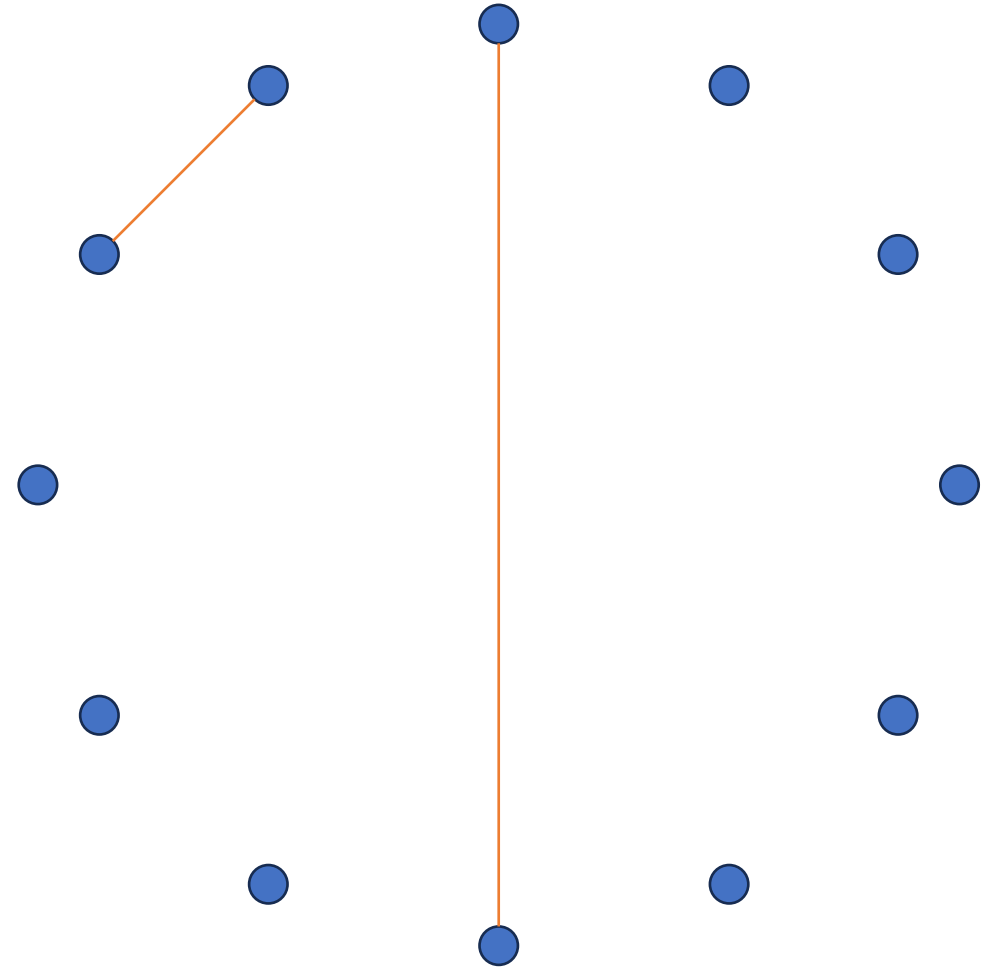
Streaming model

- Graph is given edge by edge
- Arbitrary order of the input
- Access to random bits
- Goal is to minimize the space complexity: compute in $\tilde{O}(n)$ space



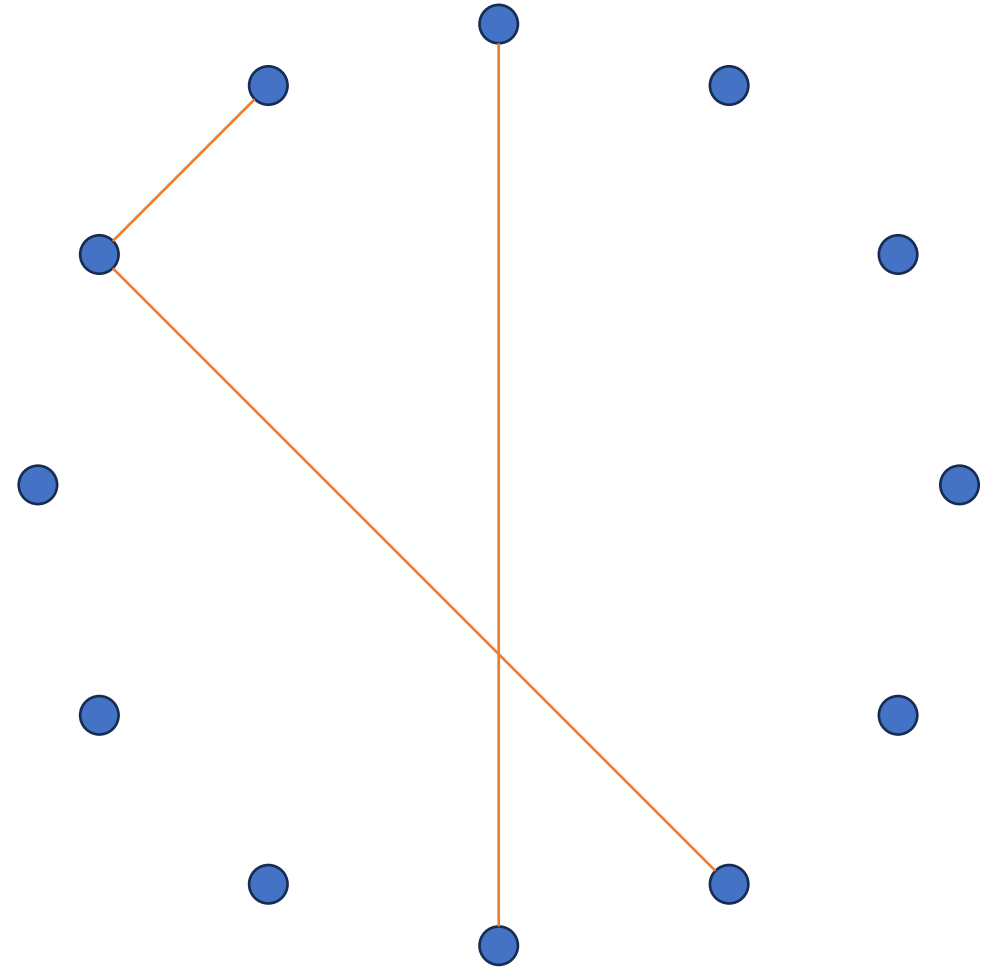
Streaming model

- Graph is given edge by edge
- Arbitrary order of the input
- Access to random bits
- Goal is to minimize the space complexity: compute in $\tilde{O}(n)$ space



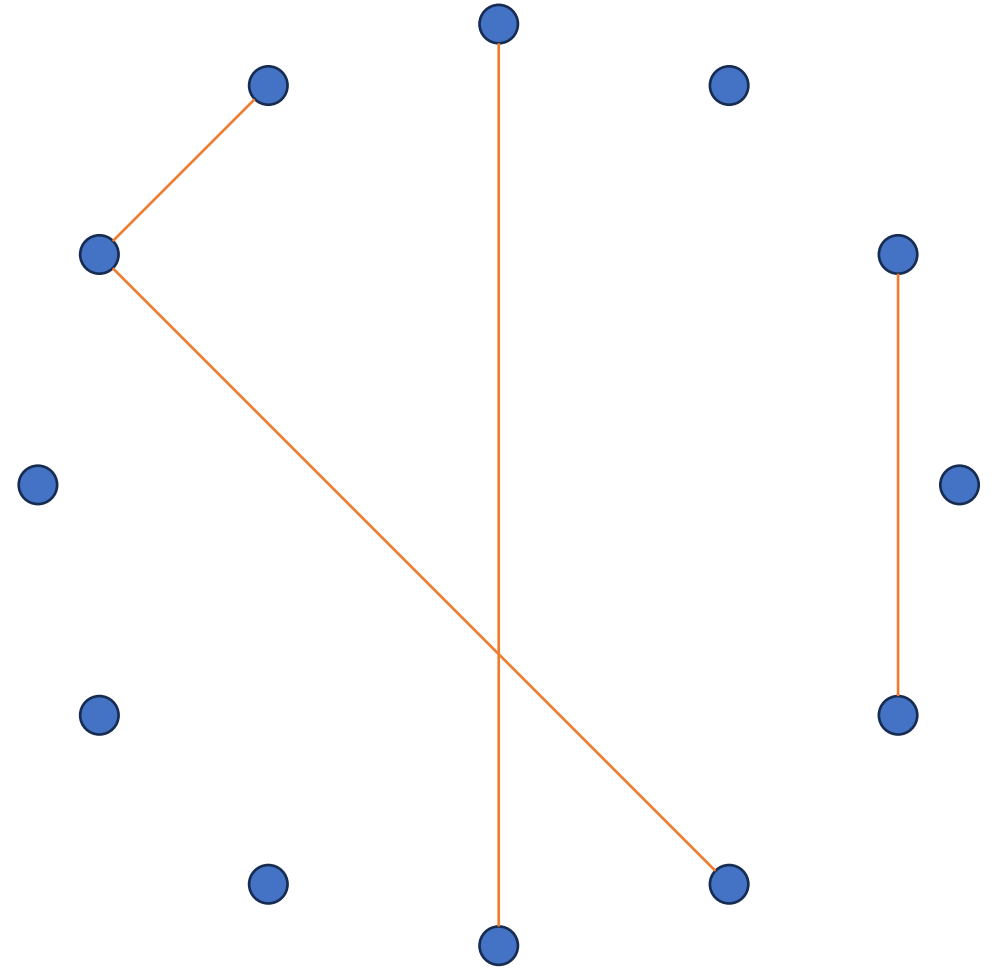
Streaming model

- Graph is given edge by edge
- Arbitrary order of the input
- Access to random bits
- Goal is to minimize the space complexity: compute in $\tilde{O}(n)$ space



Streaming model

- Graph is given edge by edge
- Arbitrary order of the input
- Access to random bits
- Goal is to minimize the space complexity: compute in $\tilde{O}(n)$ space

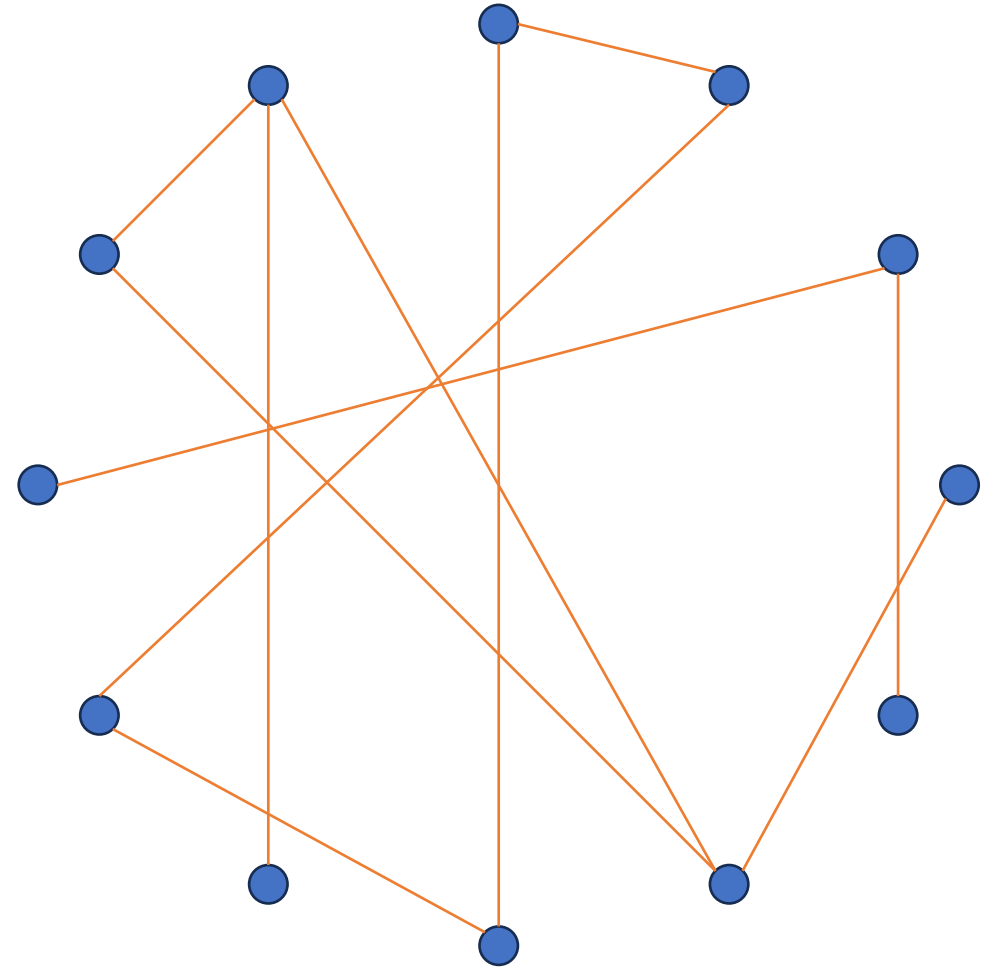


Streaming model

- Graph is given edge by edge
- Arbitrary order of the input
- Access to random bits
- Goal is to minimize the space complexity: compute in $\tilde{O}(n)$ space

$\Omega(n)$ space is often needed:

- Output size often $\Omega(n)$ (e.g. matching)
- Even if the output is a number: e.g. testing connectivity



Max-Cut

Given:

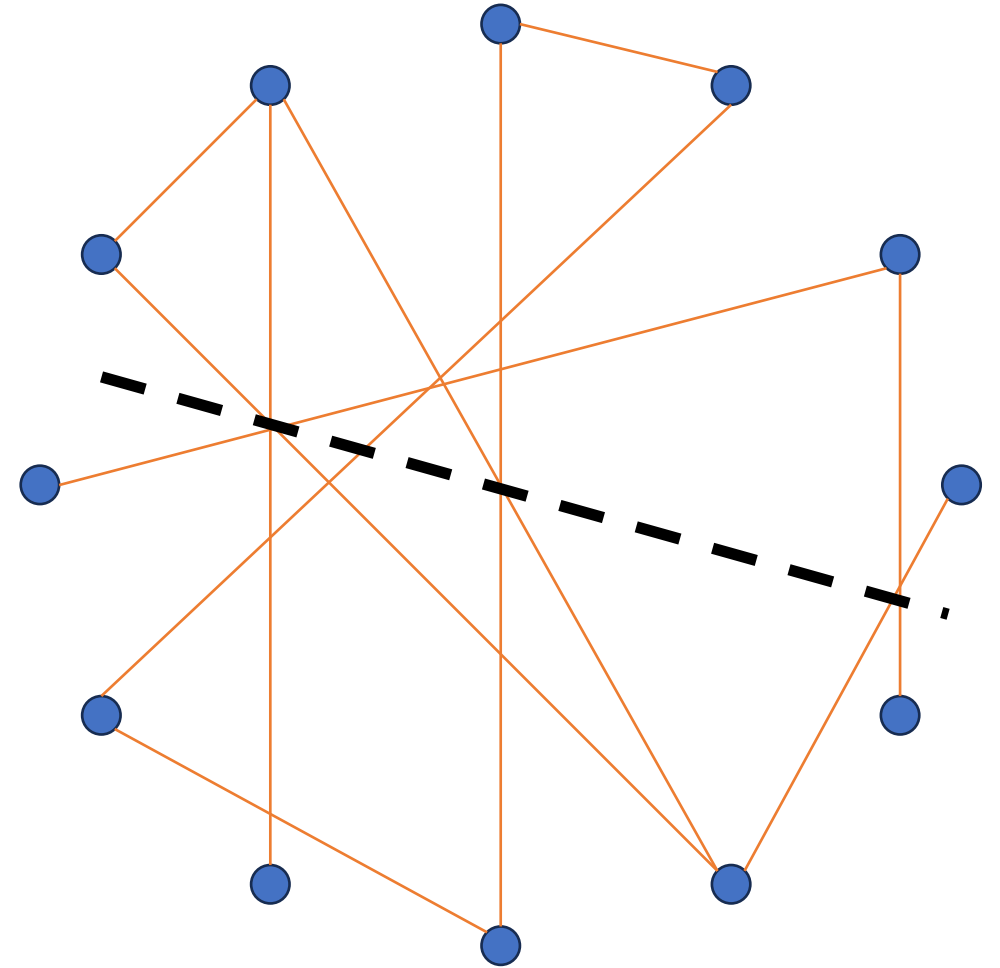
A graph $G = (V, E)$ on n vertices

Goal:

Find the maximal value of $|\{(a, b) \in E \mid a \in V_1, b \in V_2\}|$ over partitions $V = V_1 \cup V_2$

RAM model:

- Trivial 2-approximation: output $\frac{|E|}{2}$
- ~ 1.14 -approximation due to Goemans-Williamson'95



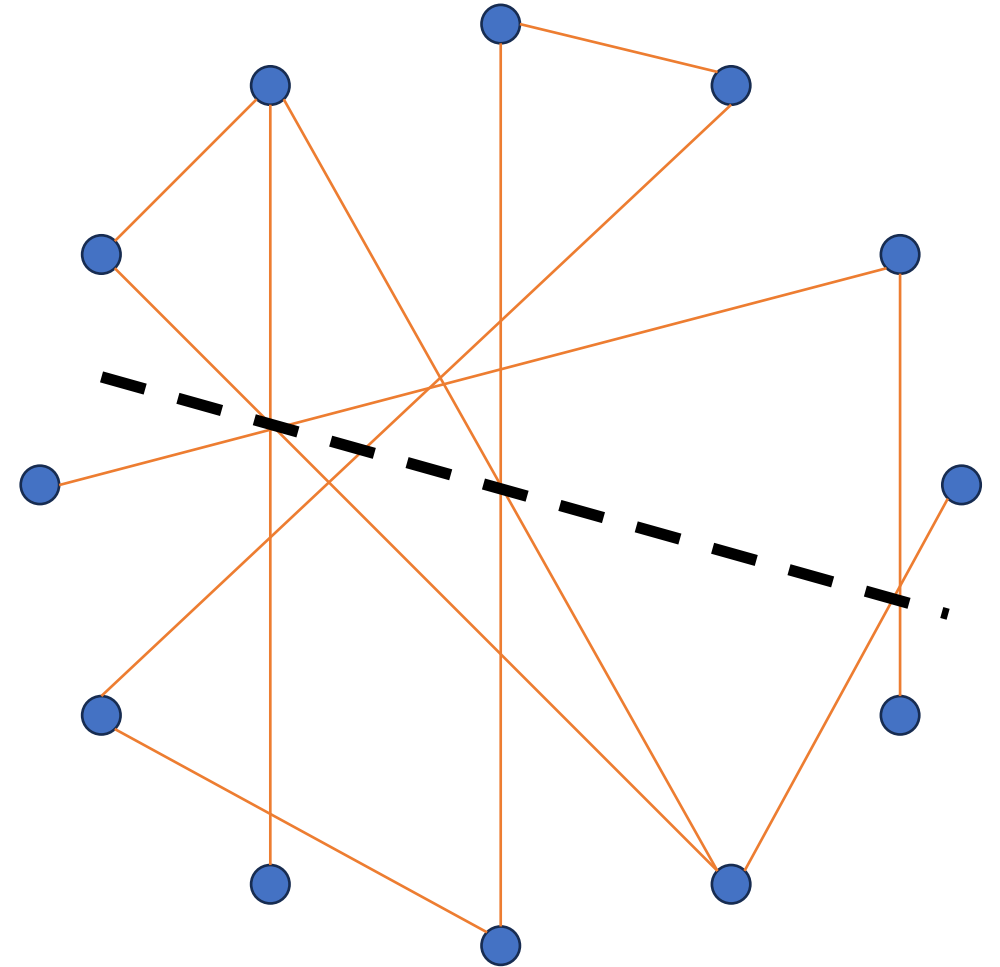
Streaming model: Max-Cut

- Graph is given edge by edge
- Arbitrary order of the input
- Access to random bits
- Goal is to approximate the value of Max-Cut

Upper bounds:

- 2-approximation in $O(\log n)$ space.
- $(1 + \varepsilon)$ -approximation in $\tilde{O}(\frac{n}{\varepsilon^2})$ space (store a sample of edges).

Is there something in between?



Streaming Max-Cut: state-of-the-art

1. [Kapralov, Krachun, 2019]

Any $(2 - \varepsilon)$ -approximation algorithm requires $\Omega(n)$ space for any ε .

2. [Kallaugher, Parekh, 2022]

Any $(2 - \varepsilon)$ -approximation quantum algorithm requires $\Omega(n)$ qubits for any ε .

Ideas:

- Reduction from communication problem in the sequential model
- Fourier analysis
- Sparseness of Fourier spectrum
- Bounding l_1 norm instead of l_2

Plan

1. Communication model and streaming lower bounds
2. DIHP problem, reduction from DIHP to Max-Cut
3. Simple protocol for DIHP
4. Fourier analysis of the protocol
5. Generalization of the analysis
6. Intro to quantum
7. How is the quantum result achieved?

Plan

1. **Communication model and streaming lower bounds**
2. DIHP problem, reduction from DIHP to Max-Cut
3. Simple protocol for DIHP
4. Fourier analysis of the protocol
5. Generalization of the analysis
6. Intro to quantum
7. How is the quantum result achieved?

One-way communication model



$x \in X$

Message m



$y \in Y$

Compute $f(x, y)$

How many bits of communication are required?

Streaming lower bounds

Algorithm $\mathcal{A}$ solves a problem in the streaming model.



$x \in X$

State $\mathcal{A}(S_x)$



$y \in Y$

1. Converts x into a stream S_x .
2. Runs algorithm $\mathcal{A}$ on S_x

1. Converts y into a stream S_y
2. Runs algorithm $\mathcal{A}(S_x)$ on S_y
3. Computes $f(x, y)$ from $\mathcal{A}(S_x S_y)$

Sequential communication model

Inputs:
Public M_1
Private w_1

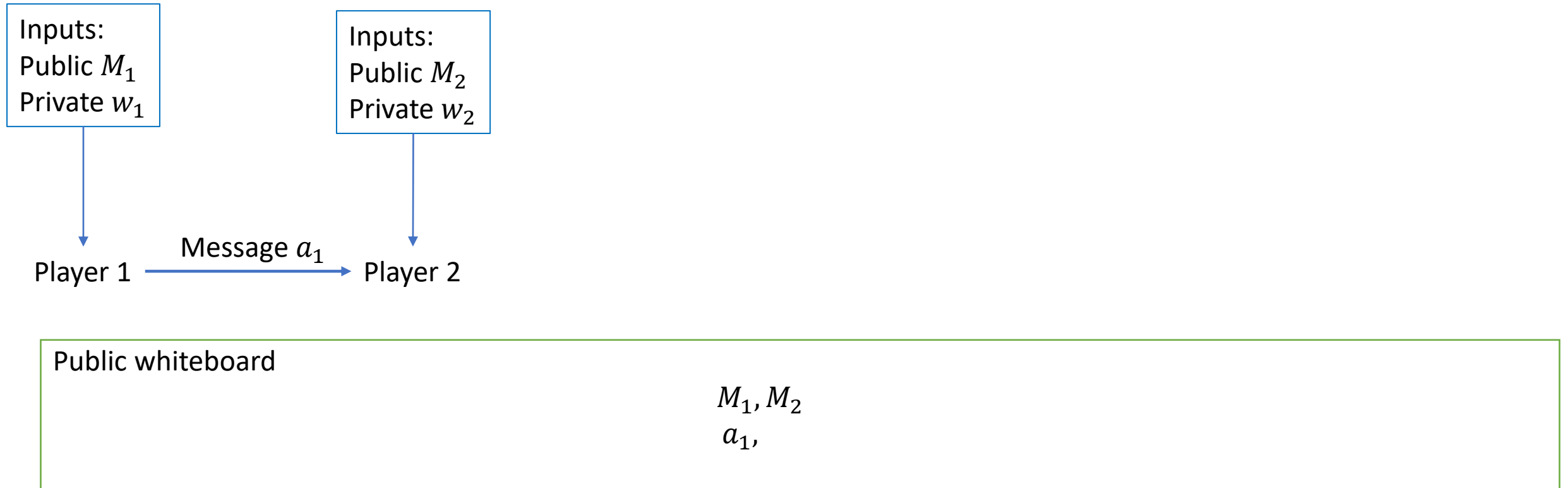


Player 1

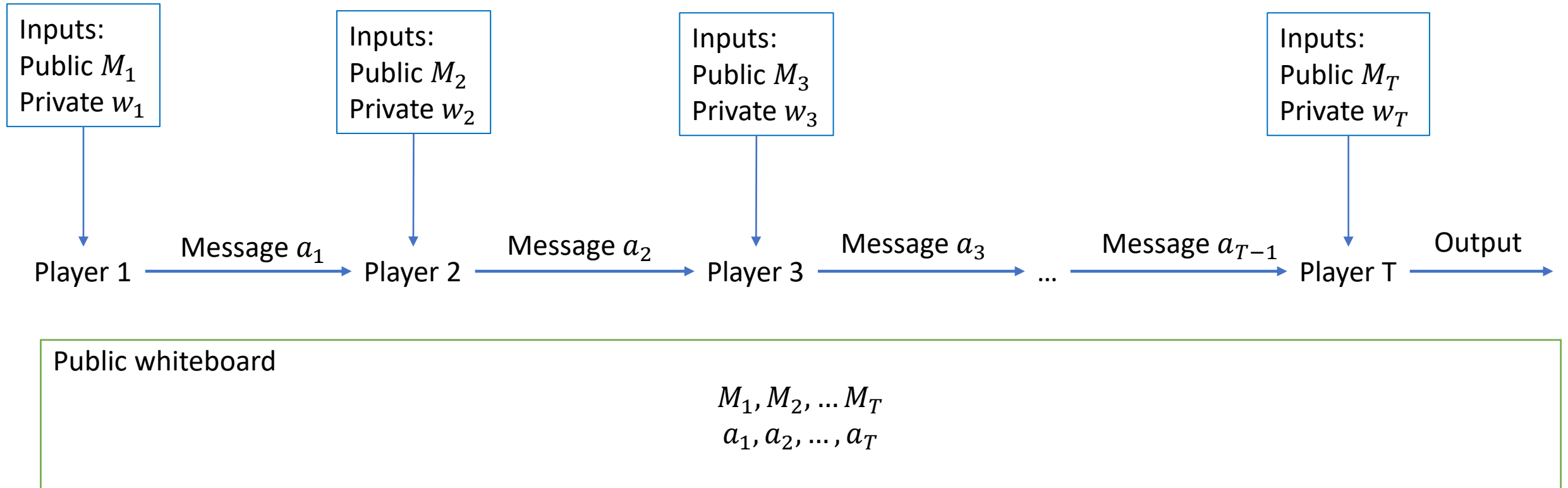
Public whiteboard

M_1

Sequential communication model



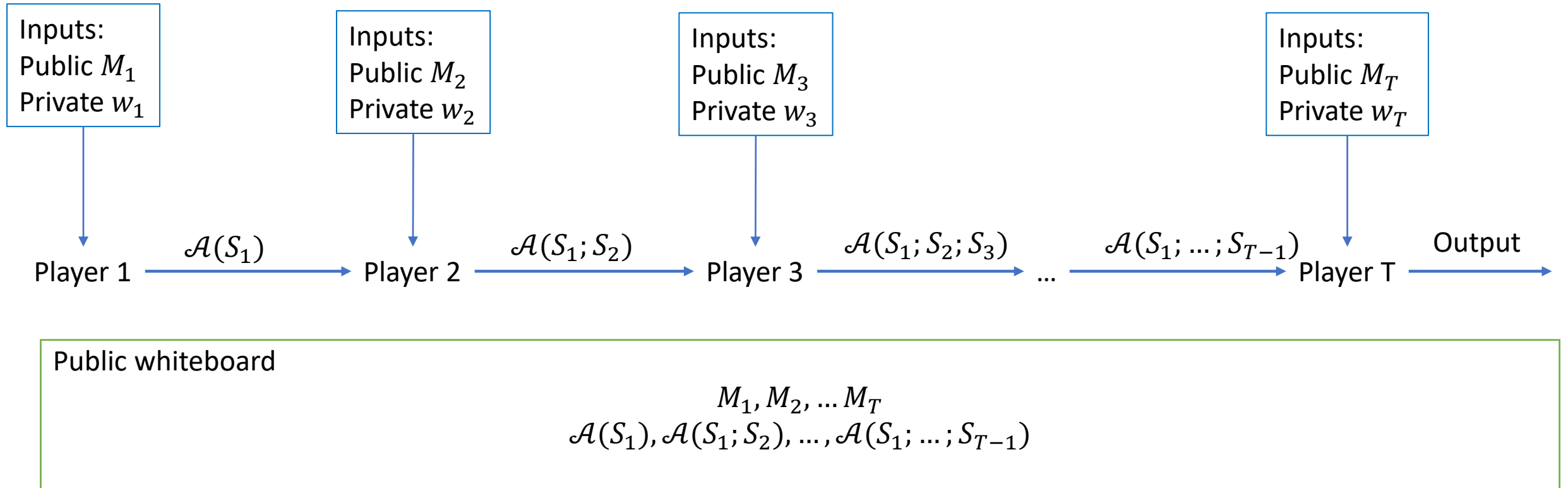
Sequential communication model



Complexity on the protocol: $\max |a_i|$

Sequential communication model vs streaming

Algorithm $\mathcal{A}$ solves a problem in the streaming model.



Complexity on the protocol: $\max |\mathcal{A}(S_1; \dots; S_i)| \leq \text{space complexity of } \mathcal{A}$

Plan

1. Communication model and streaming lower bounds
- 2. DIHP problem, reduction from DIHP to Max-Cut**
3. Simple protocol for DIHP
4. Fourier analysis of the protocol
5. Generalization of the analysis
6. Intro to quantum
7. How is the quantum result achieved?

Distributional Implicit Hidden Partition

DIHP(n, α, T):

Input: **YES** with pr $\frac{1}{2}$, **NO** with pr $\frac{1}{2}$

Goal: distinguish between **YES** and **NO** cases

Distributional Implicit Hidden Partition

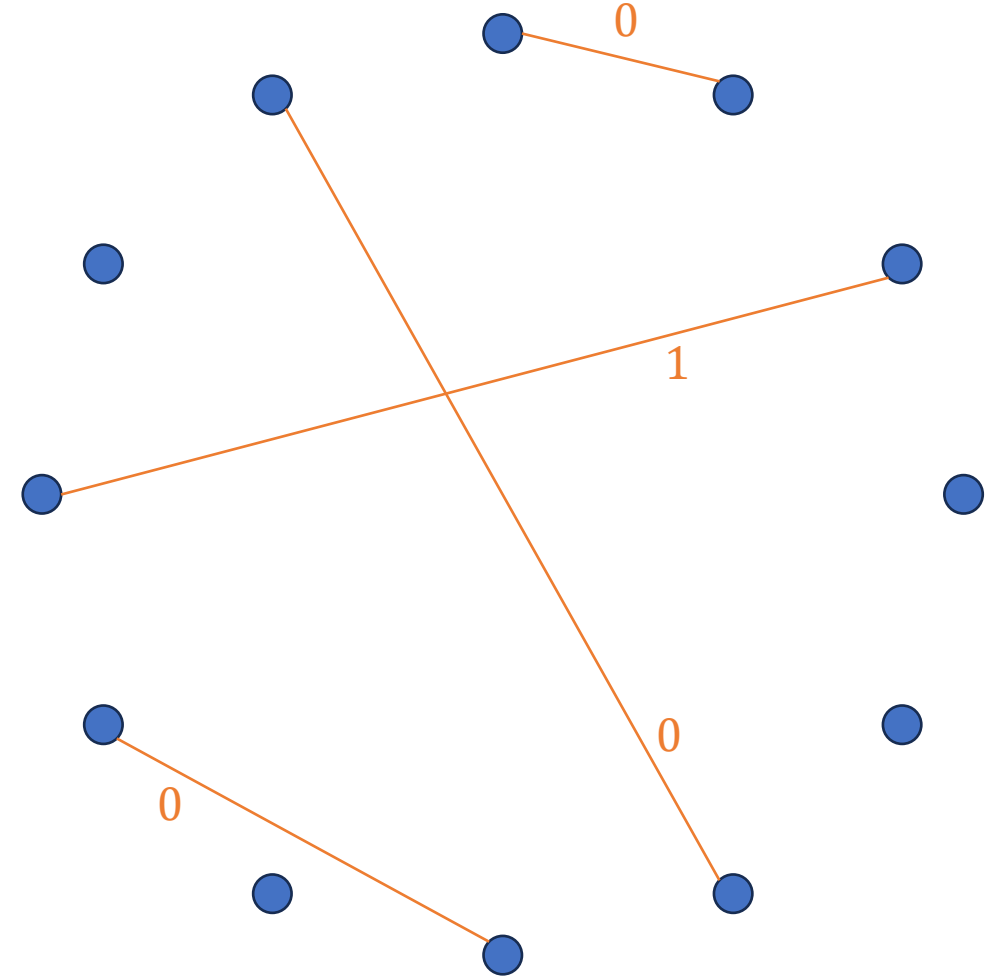
DIHP(n, α, T):

Input: **YES** with pr $\frac{1}{2}$, **NO** with pr $\frac{1}{2}$

NO:

- $M_t \leftarrow$ matching of size αn
- For all t the input $w_t \leftarrow \{0, 1\}^{\alpha n}$

Edges with label 1 form a random (almost Erdős–Rényi) non-bipartite graph.



Goal: distinguish between **YES** and **NO** cases

Distributional Implicit Hidden Partition

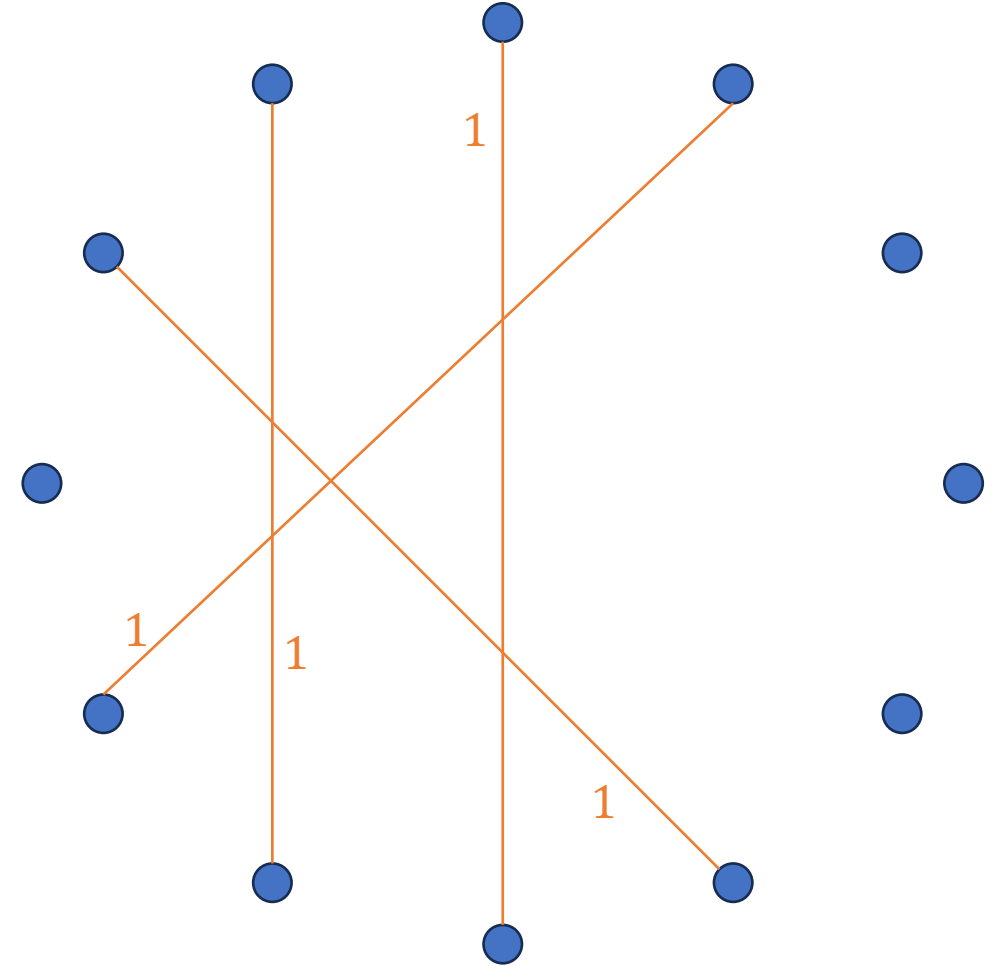
DIHP(n, α, T):

Input: **YES** with pr $\frac{1}{2}$, **NO** with pr $\frac{1}{2}$

NO:

- $M_t \leftarrow$ matching of size αn
- For all t the input $w_t \leftarrow \{0, 1\}^{\alpha n}$

Edges with label 1 form a random (almost Erdős–Rényi) non-bipartite graph.



Goal: distinguish between **YES** and **NO** cases

Distributional Implicit Hidden Partition

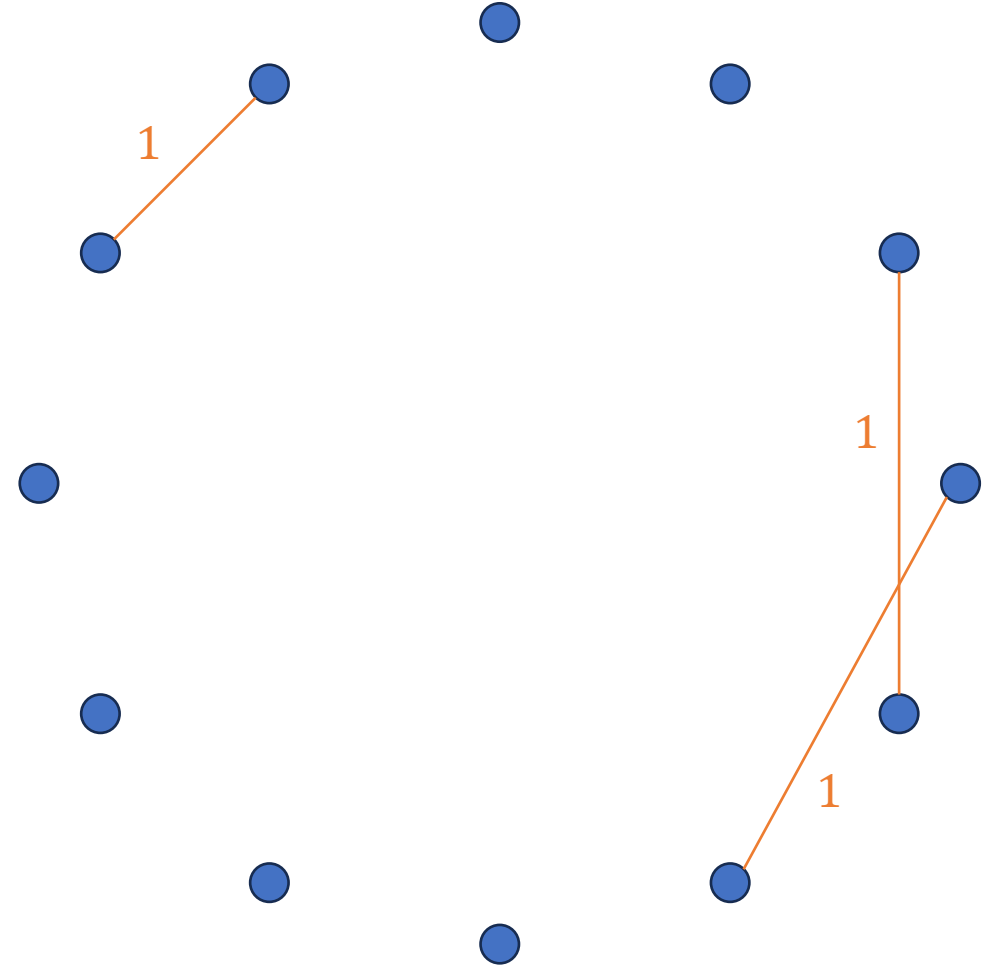
DIHP(n, α, T):

Input: **YES** with pr $\frac{1}{2}$, **NO** with pr $\frac{1}{2}$

NO:

- $M_t \leftarrow$ matching of size αn
- For all t the input $w_t \leftarrow \{0, 1\}^{\alpha n}$

Edges with label 1 form a random (almost Erdős–Rényi) non-bipartite graph.



Goal: distinguish between **YES** and **NO** cases

Distributional Implicit Hidden Partition

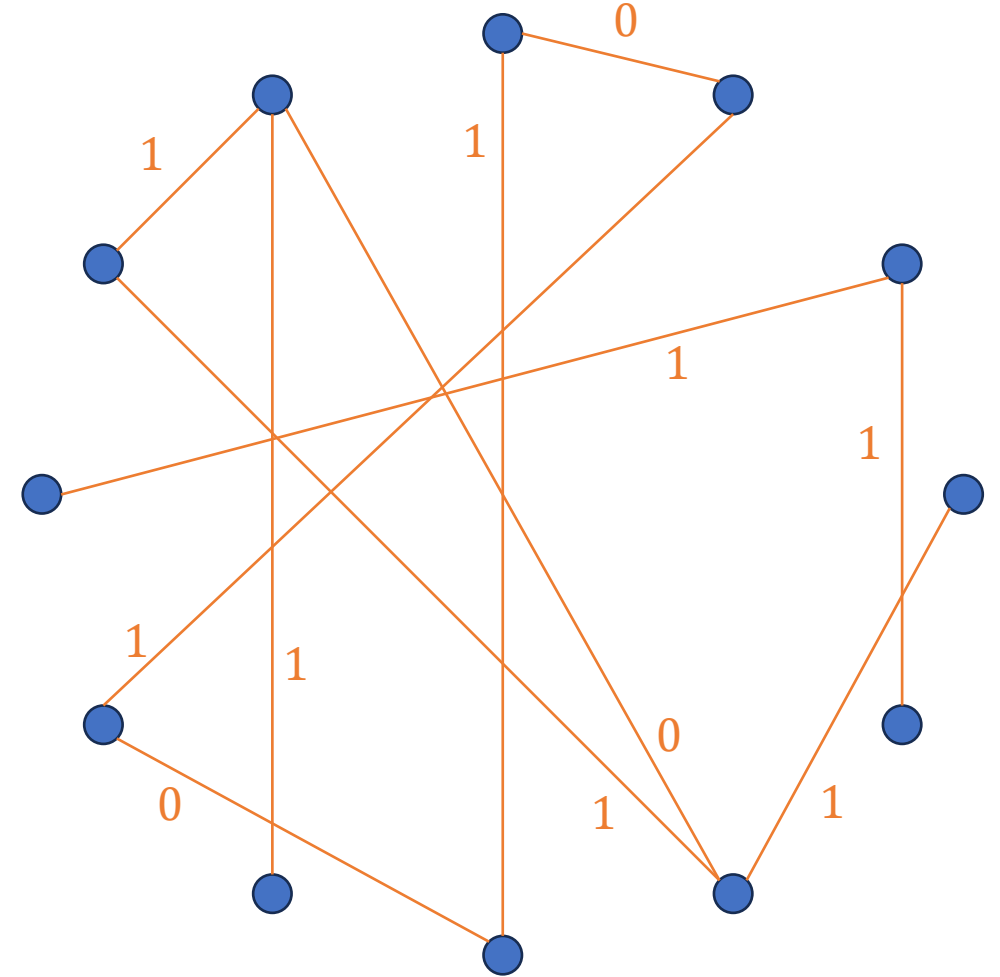
DIHP(n, α, T):

Input: **YES** with pr $\frac{1}{2}$, **NO** with pr $\frac{1}{2}$

NO:

- $M_t \leftarrow$ matching of size αn
- For all t the input $w_t \leftarrow \{0, 1\}^{\alpha n}$

Edges with label 1 form a random (almost Erdős–Rényi) non-bipartite graph.



Goal: distinguish between **YES** and **NO** cases

Distributional Implicit Hidden Partition

DIHP(n, α, T):

Input: YES with pr $\frac{1}{2}$, NO with pr $\frac{1}{2}$

NO:

- $M_t \leftarrow$ matching of size αn
- For all t the input $w_t \leftarrow \{0, 1\}^{\alpha n}$

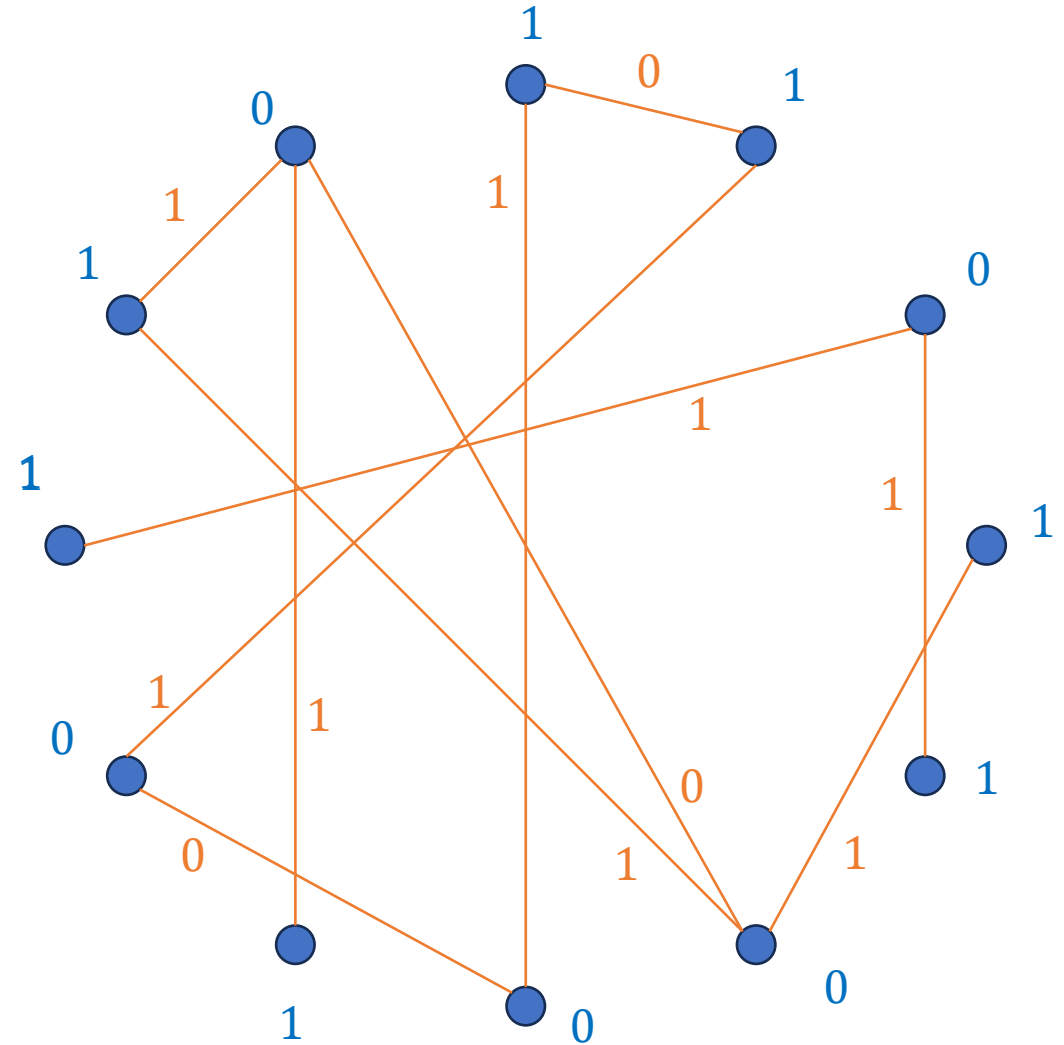
Edges with label 1 form a random (almost Erdős–Rényi) non-bipartite graph.

YES:

- $M_t \leftarrow$ matching of size αn
- $x \leftarrow \{0, 1\}^n$,
- For all t the input $w_t = M_t x$
- $w_{[u,v]} = x_u \oplus x_v$

Edges with label 1 form a random (almost Erdős–Rényi) bipartite graph.

Goal: distinguish between YES and NO cases



Reduction from Max-Cut

There exists constant $C > 0$ such that $\forall \varepsilon \in (0, 1]$:

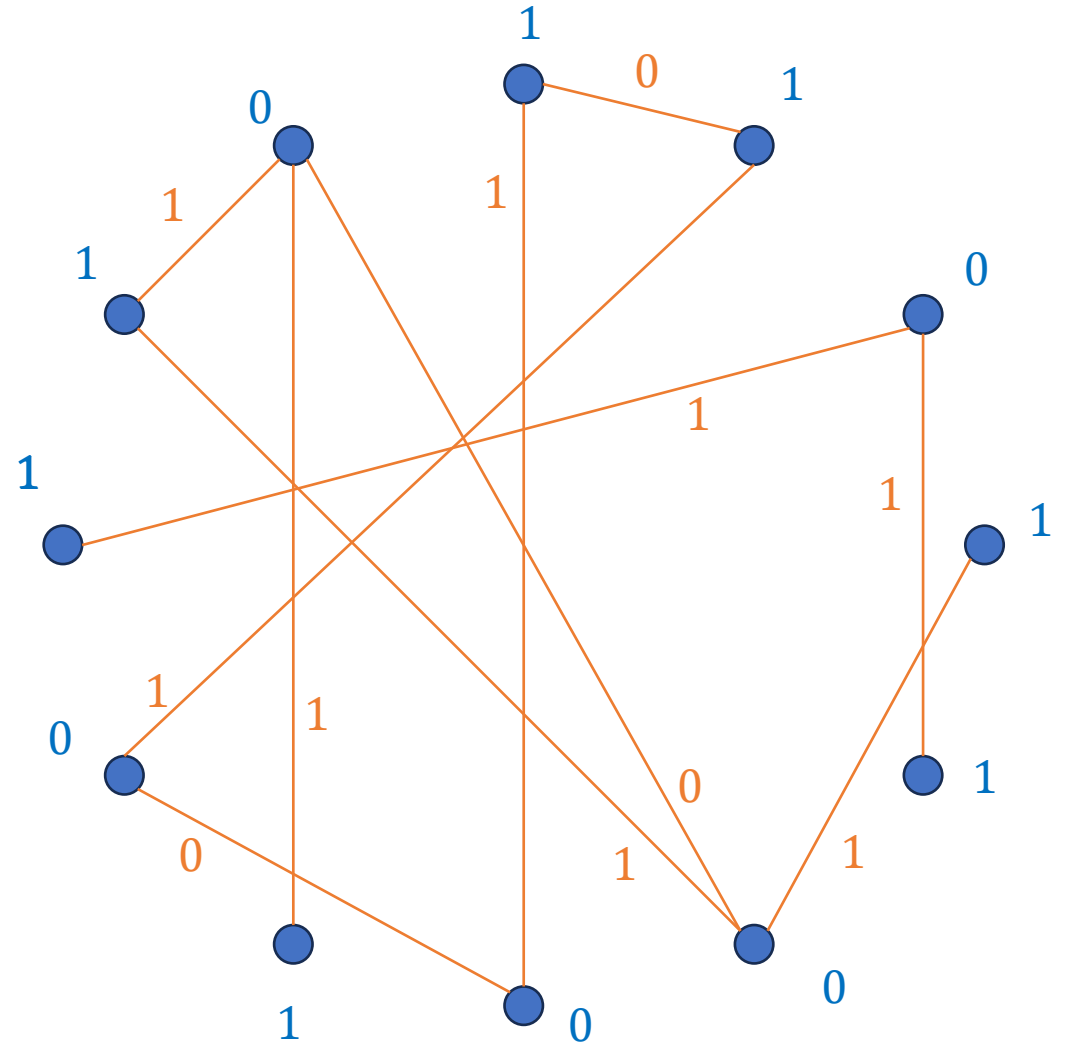
Suppose there is a streaming algorithm for $(2 - \varepsilon)$ -approximation of Max-Cut size of n -vertex graph in space S .

Then $\text{DIHP}(n, \frac{\varepsilon}{C}, \frac{C^3}{\varepsilon^2})$ has a protocol using $O(S)$ communication.

Construction: Player t posts i -th edge from M_t to their part of the stream if

- $(w_t)_i = 1$ and
- The edge is not in M_s for any $s \leq t$

- YES case: Max-Cut size is m . The graph is bipartite.
- NO case: With high probability Max-Cut size is $\leq \frac{m}{2 - O(\frac{1}{n} + \alpha)}$.



Plan

1. Communication model and streaming lower bounds
2. DIHP problem, reduction from DIHP to Max-Cut
- 3. Simple protocols for DIHP**
4. Fourier analysis of the protocol
5. Generalization of the analysis
6. Intro to quantum
7. How is the quantum result achieved?

Distributional Implicit Hidden Partition

DIHP(n, α, T):

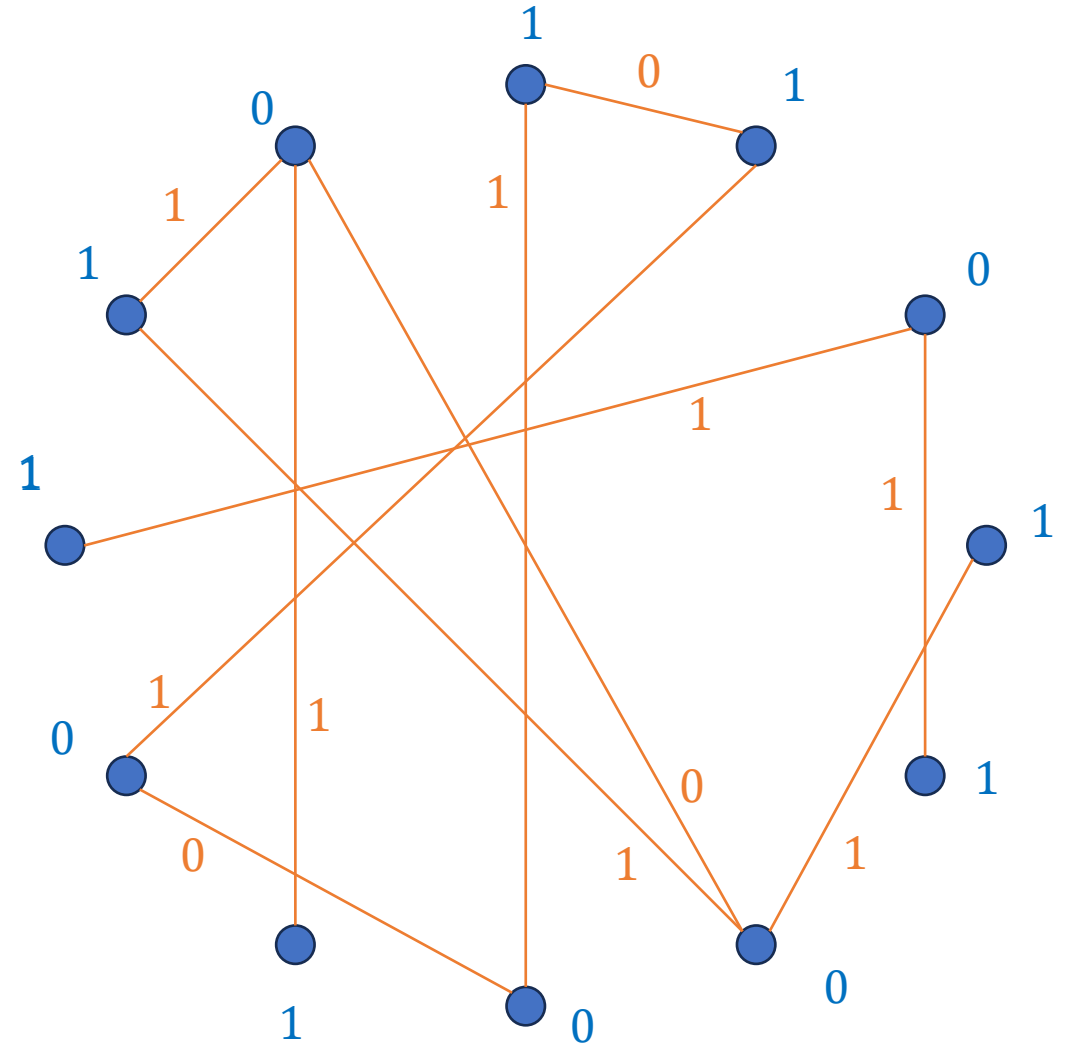
Input: YES with pr $\frac{1}{2}$, NO with pr $\frac{1}{2}$

NO:

- $M_t \leftarrow$ matching of size αn
- For all t the input $w_t \leftarrow \{0, 1\}^{\alpha n}$

YES:

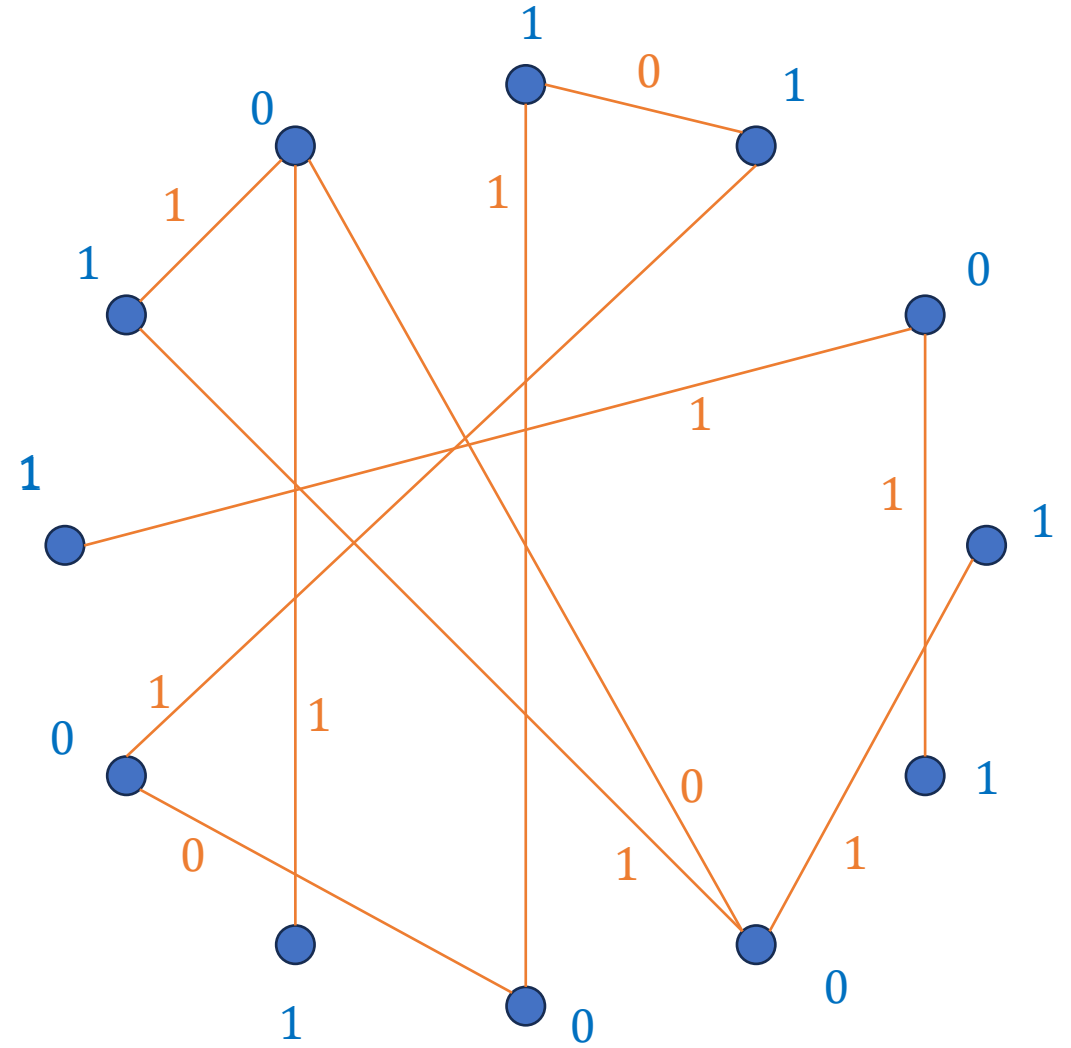
- $M_t \leftarrow$ matching of size αn
- $x \leftarrow \{0, 1\}^n$,
- For all t the input $w_t = M_t x$
- $w_{[u,v]} = x_u \oplus x_v$



Goal: distinguish between YES and NO cases

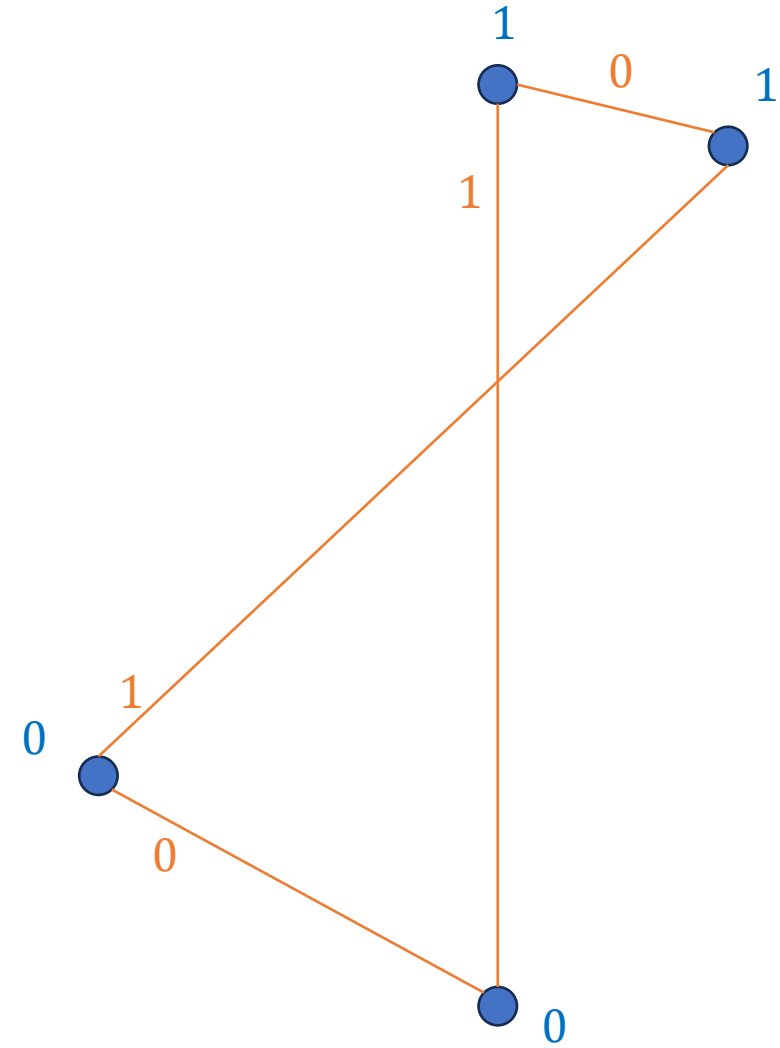
DIHP: component growing protocol

Goal: Find a cycle



DIHP: component growing protocol

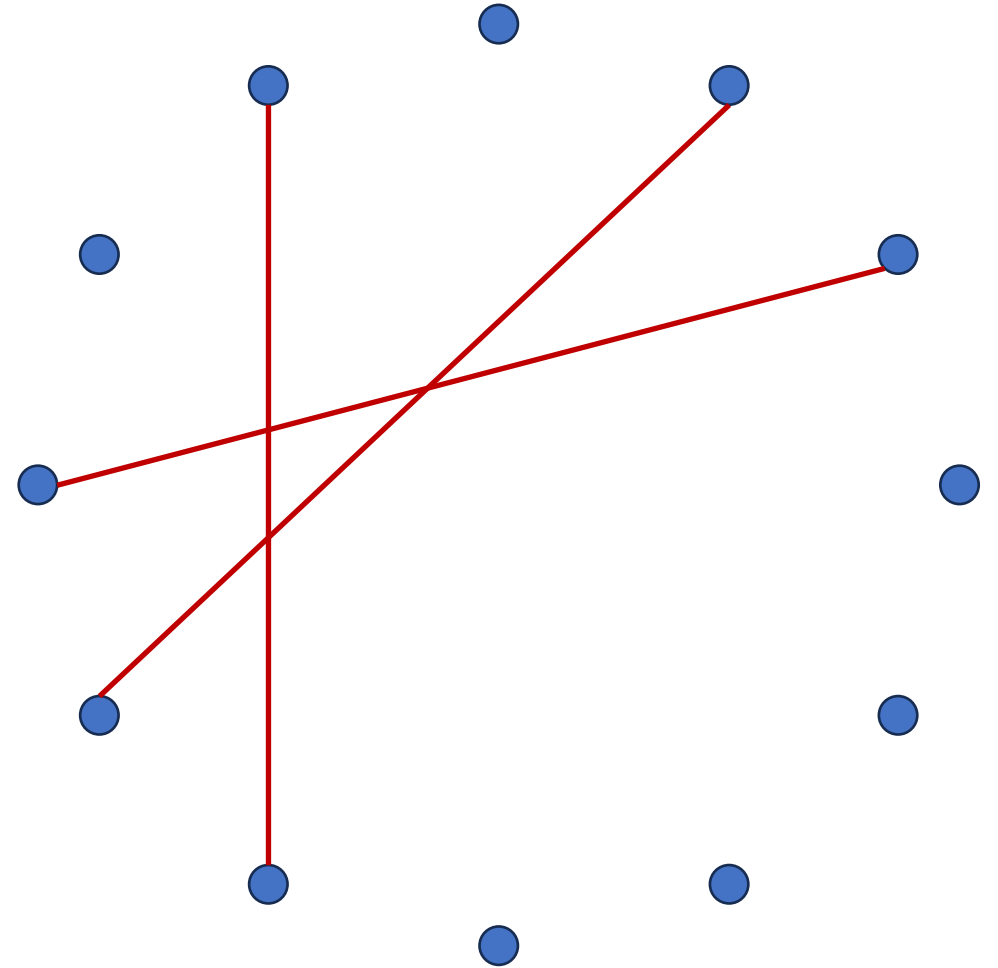
Goal: Find a cycle



DIHP: component growing protocol

Goal: Find a cycle

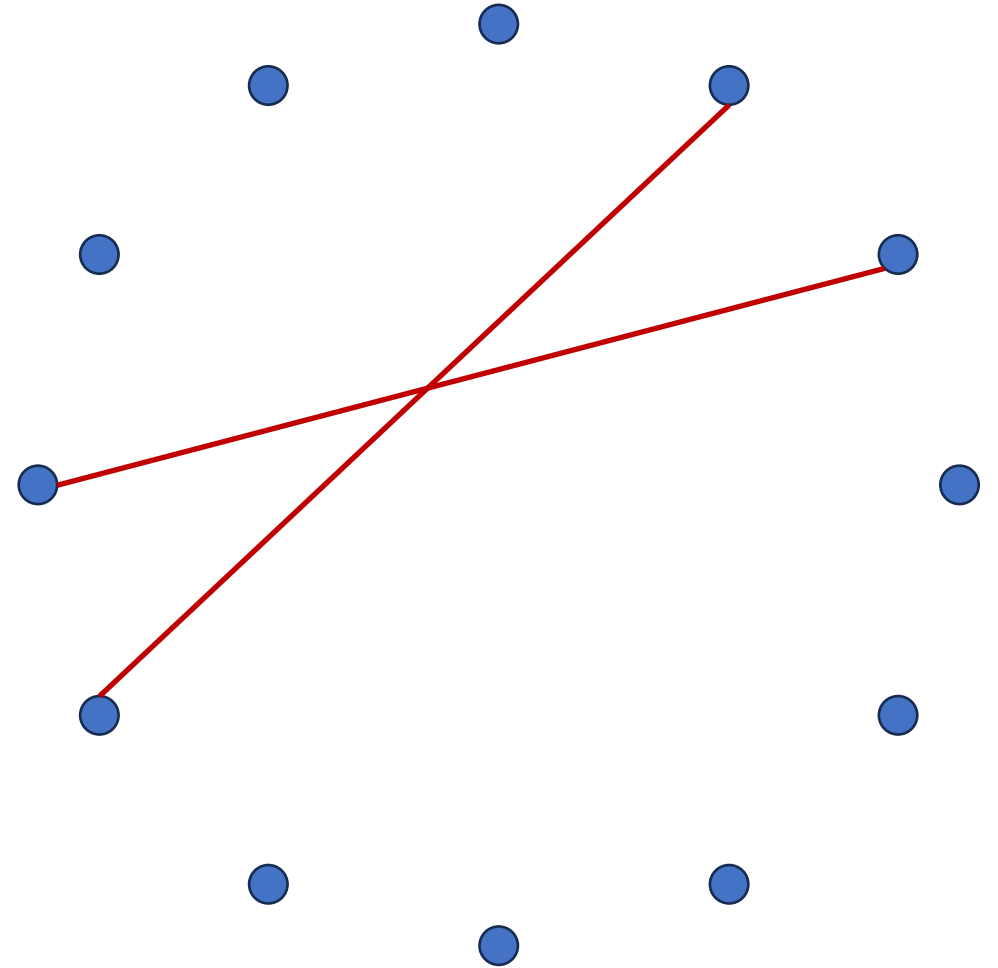
Approach:
Grow a forest



DIHP: component growing protocol

Goal: Find a cycle

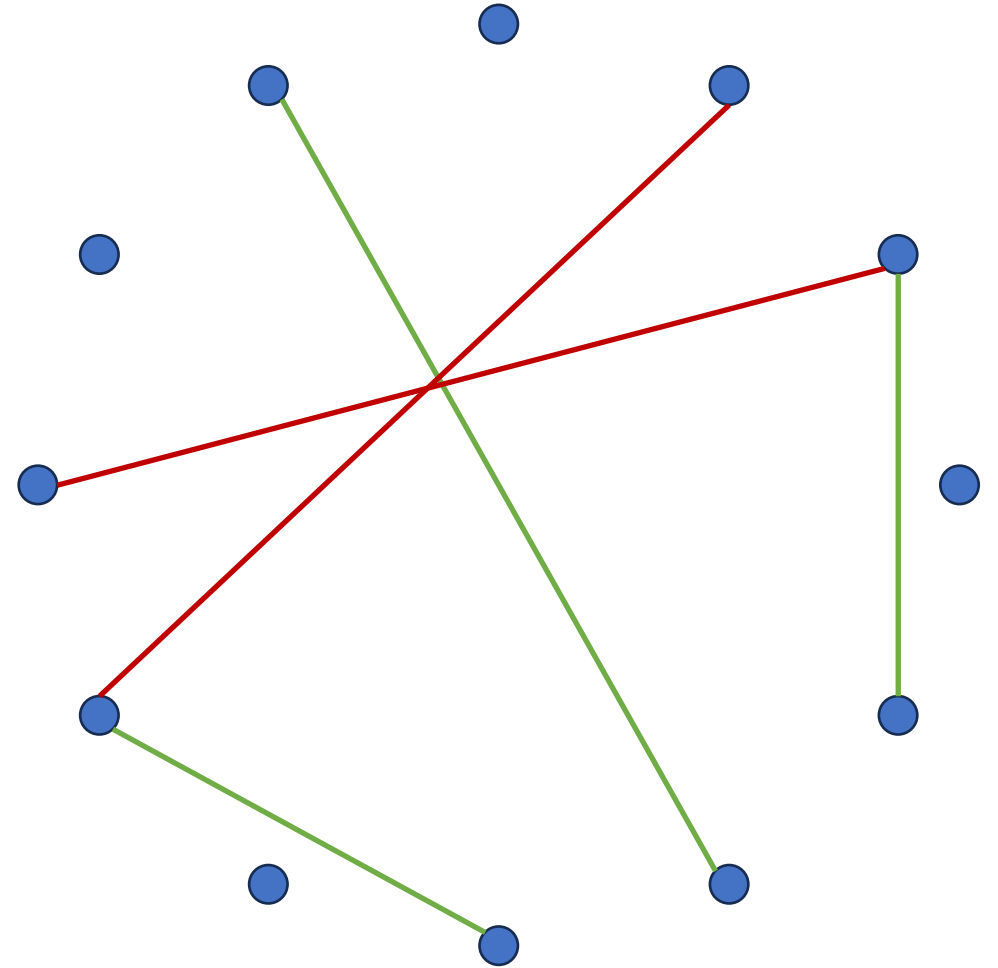
Approach:
Grow a forest



DIHP: component growing protocol

Goal: Find a cycle

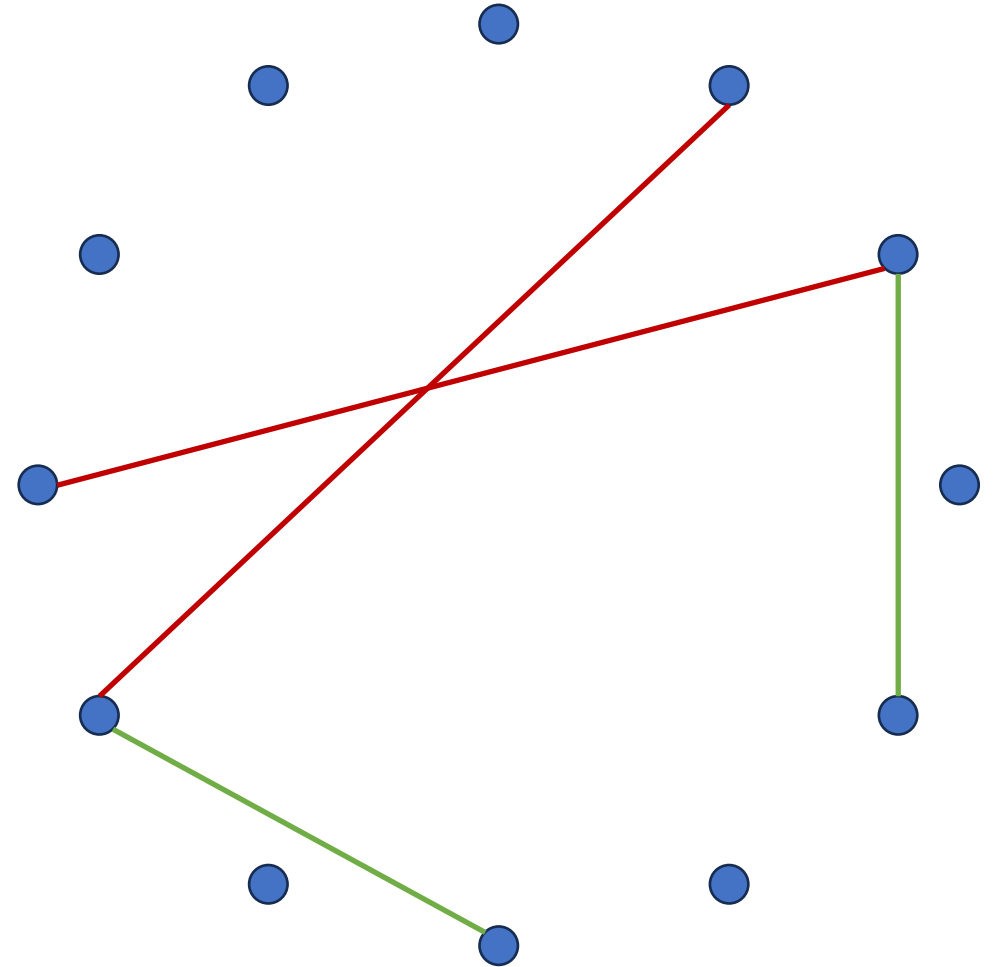
Approach:
Grow a forest



DIHP: component growing protocol

Goal: Find a cycle

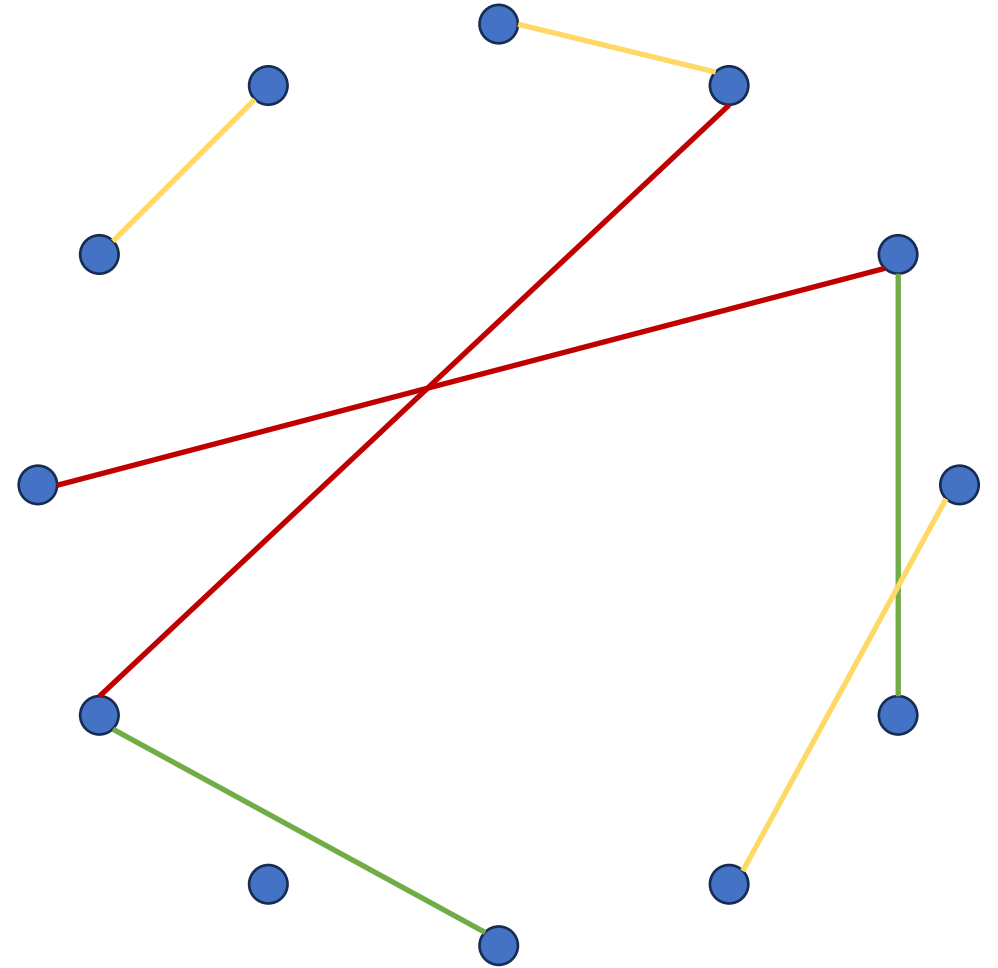
Approach:
Grow a forest



DIHP: component growing protocol

Goal: Find a cycle

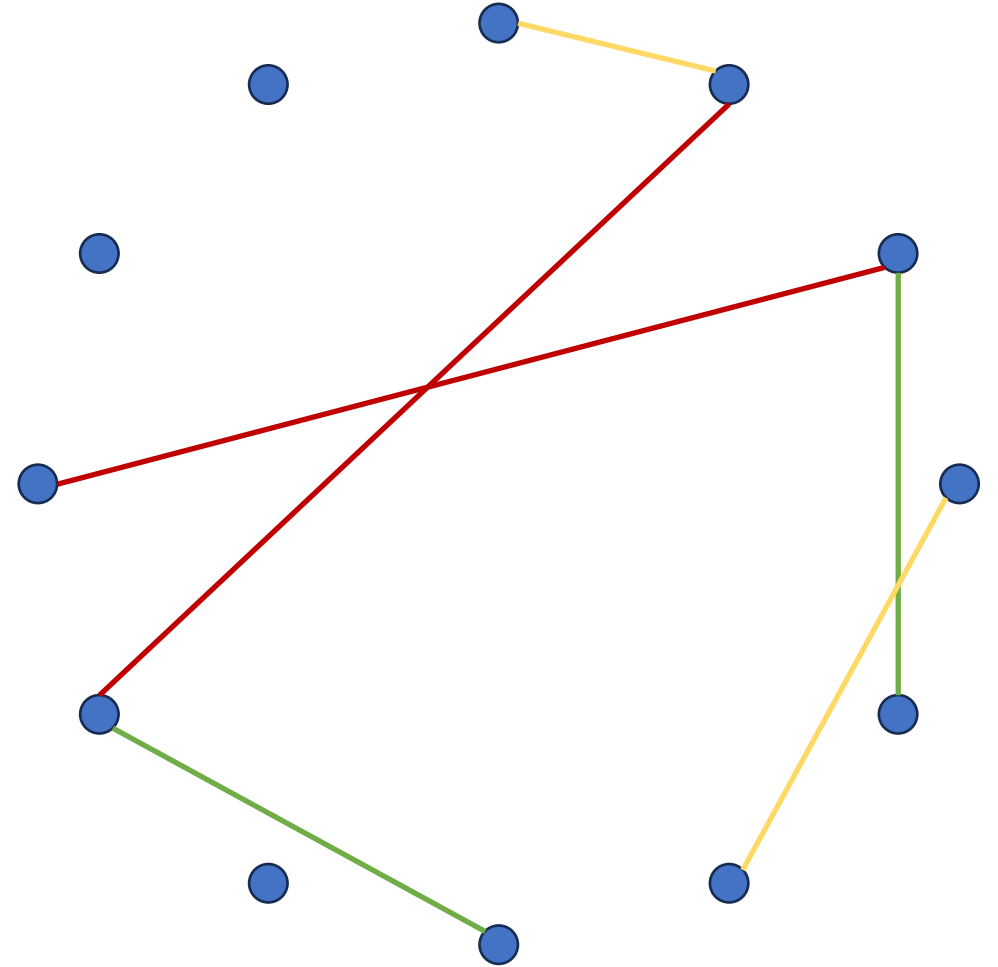
Approach:
Grow a forest



DIHP: component growing protocol

Goal: Find a cycle

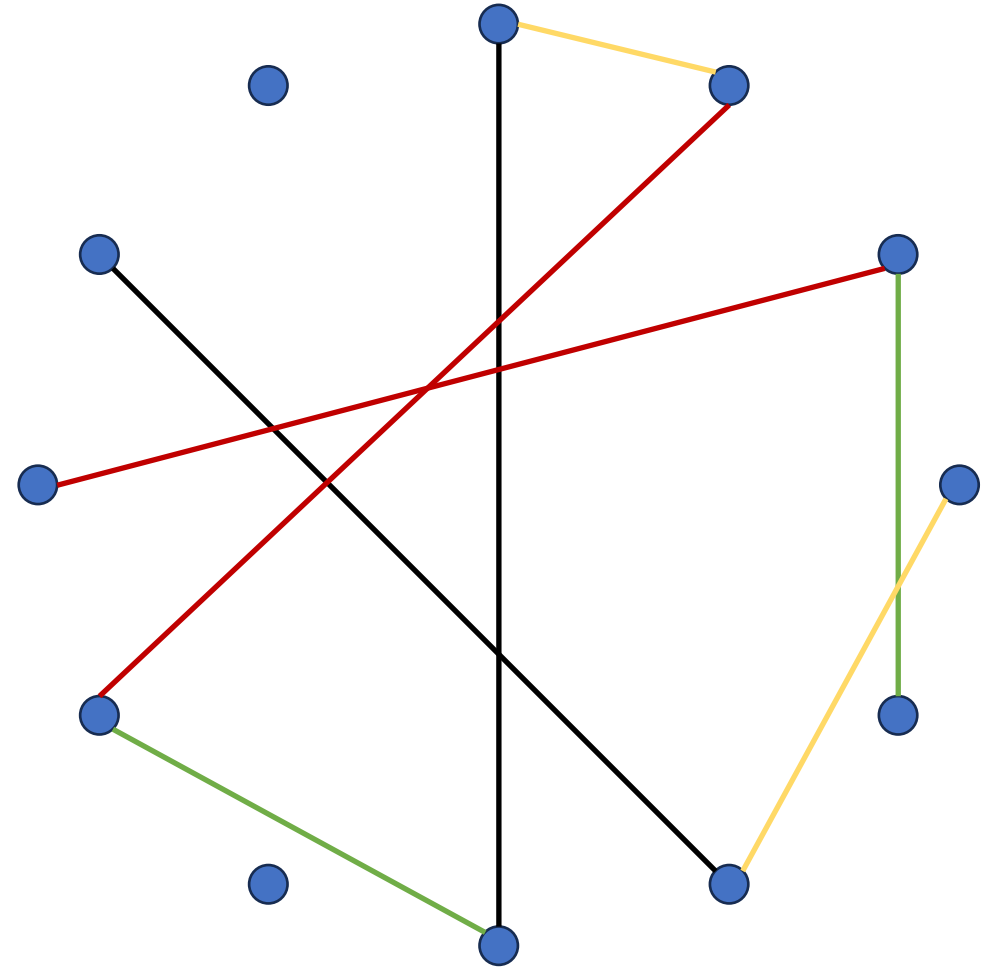
Approach:
Grow a forest



DIHP: component growing protocol

Goal: Find a cycle

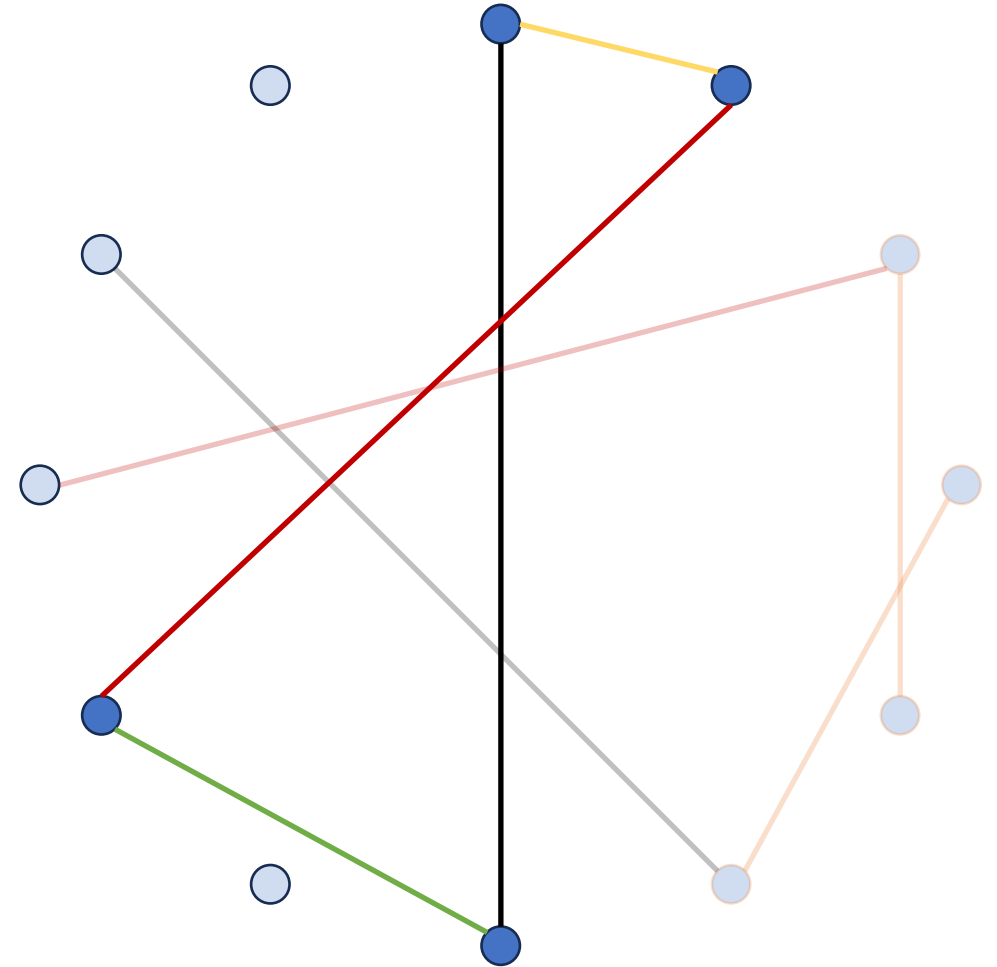
Approach:
Grow a forest



DIHP: component growing protocol

Goal: Find a cycle

Approach:
Grow a forest



DIHP: component growing protocol

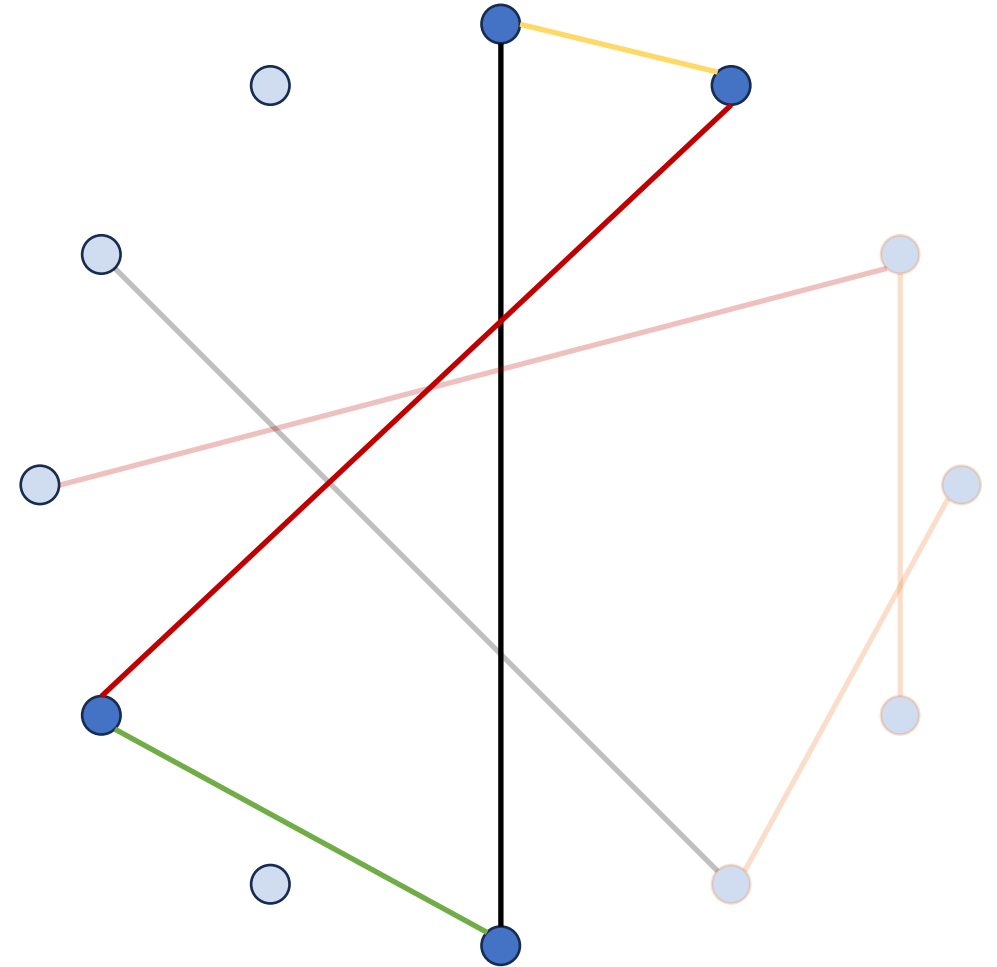
Goal: Find a cycle

Approach:

Grow a forest.

Let β be the communication budget.

1. Each player maintain a collection of connected components $C_1, C_2, \dots, C_k$ and post labels for edges incident to at least one of the connected components.



DIHP: component growing protocol

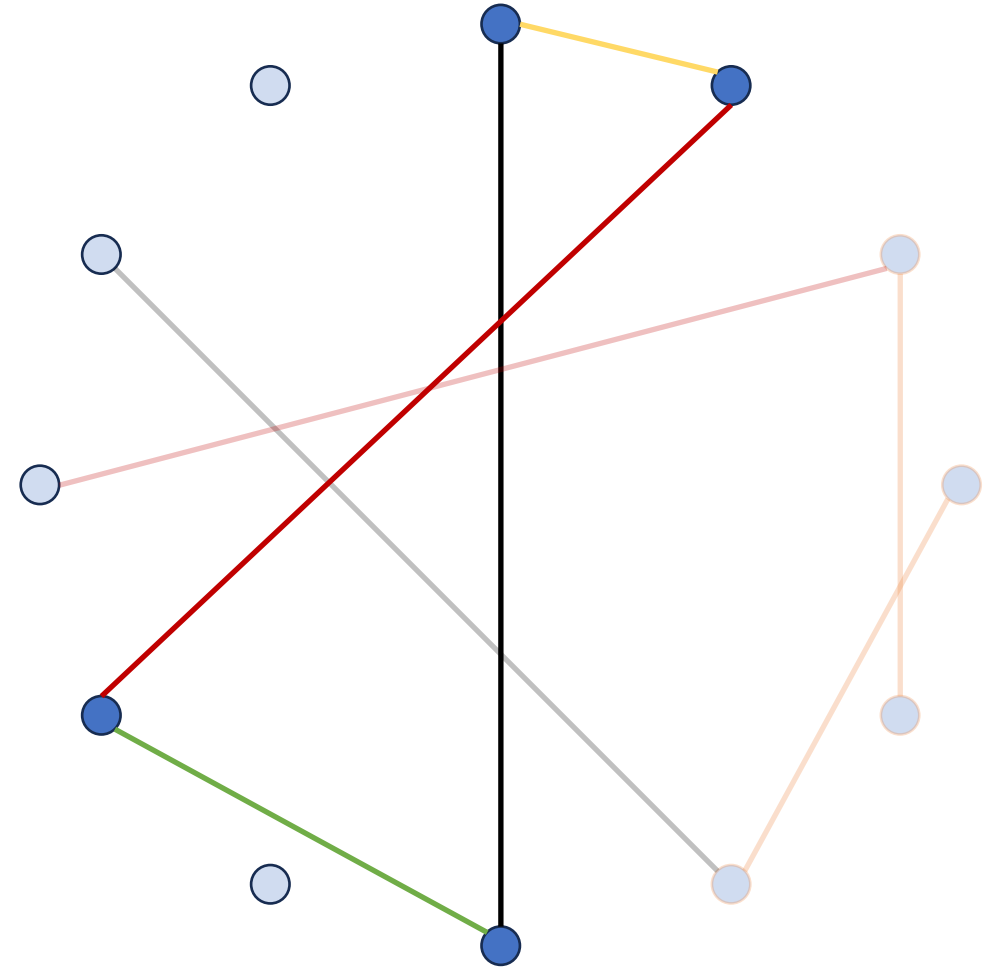
Goal: Find a cycle

Approach:

Grow a forest.

Let β be the communication budget.

1. Each player maintain a collection of connected components $C_1, C_2, \dots, C_k$ and post labels for edges incident to at least one of the connected components.
2. If player hits communication budget β , they dispose smallest components.



DIHP: component growing protocol

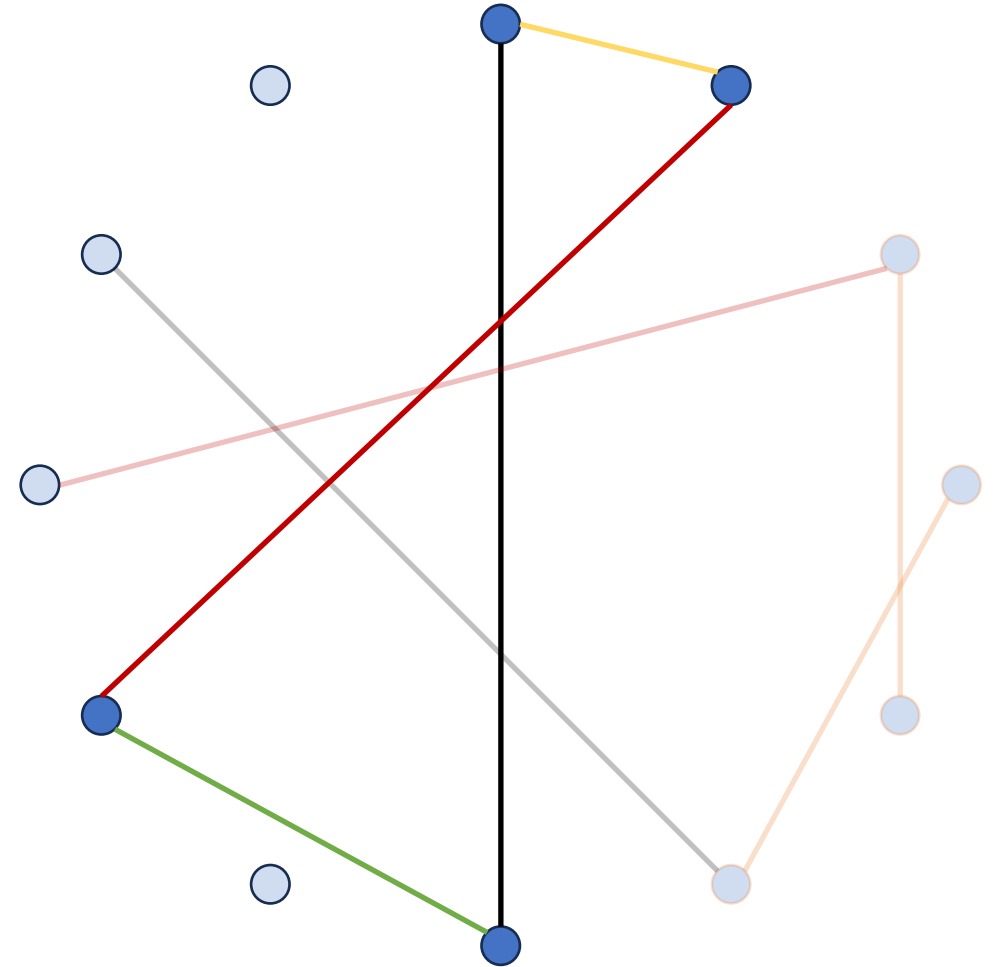
Goal: Find a cycle

Approach:

Grow a forest.

Let β be the communication budget.

1. Each player maintain a collection of connected components $C_1, C_2, \dots, C_k$ and post labels for edges incident to at least one of the connected components.
2. If player hits communication budget β , they dispose smallest components.
3. With high probability most of the components will increase by a constant factor after every step.



DIHP: component growing protocol

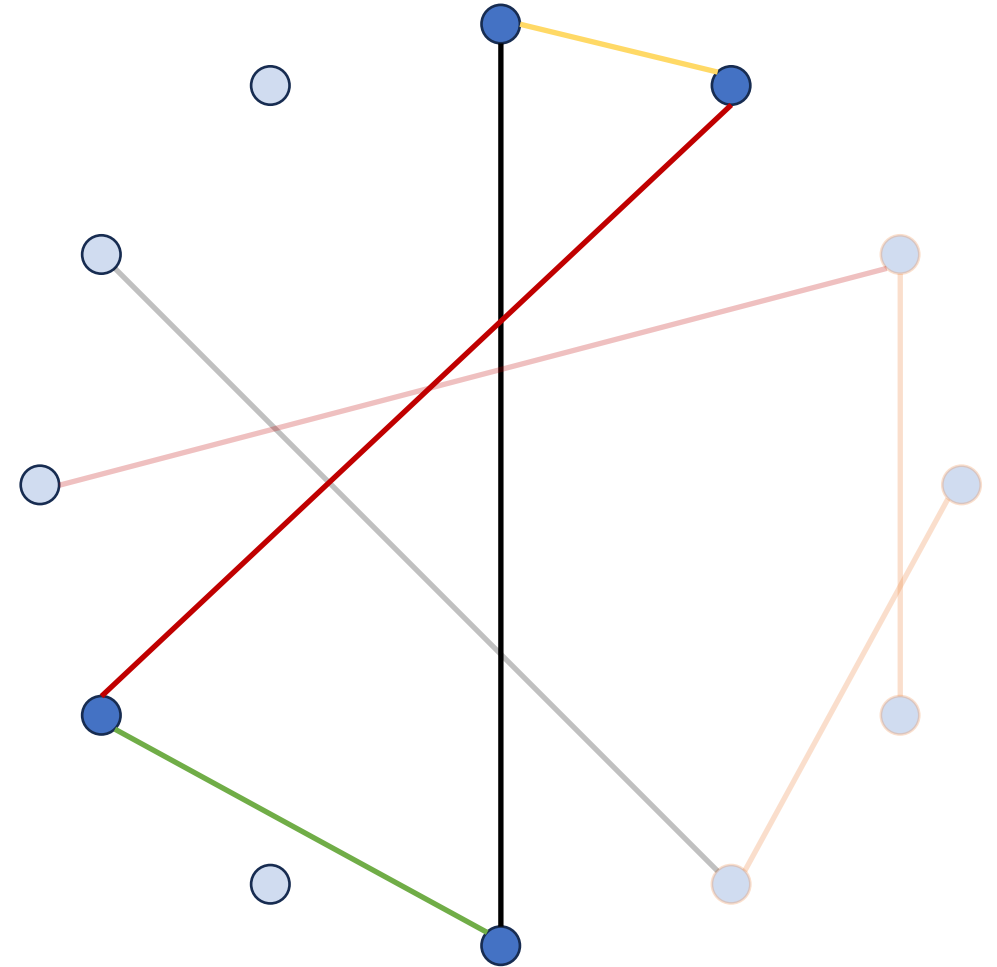
Goal: Find a cycle

Approach:

Grow a forest.

Let β be the communication budget.

1. Each player maintain a collection of connected components $C_1, C_2, \dots, C_k$ and post labels for edges incident to at least one of the connected components.
2. If player hits communication budget β , they dispose smallest components.
3. With high probability most of the components will increase by a constant factor after every step.
4. After T steps we get $\sim \beta / c^T$ connected components of size $\sim c^T$.



DIHP: component growing protocol

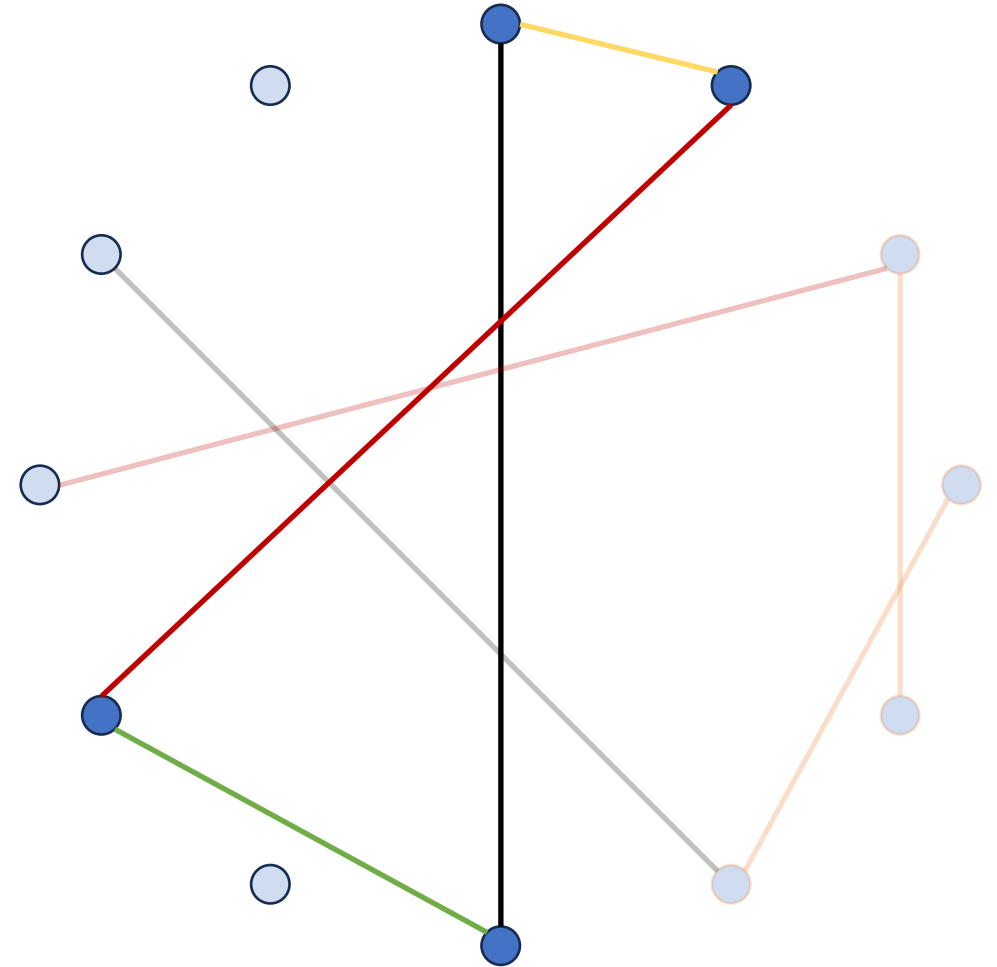
Goal: Find a cycle

Approach:

Grow a forest.

Let β be the communication budget.

1. Each player maintain a collection of connected components $C_1, C_2, \dots, C_k$ and post labels for edges incident to at least one of the connected components.
2. If player hits communication budget β , they dispose smallest components.
3. With high probability most of the components will increase by a constant factor after every step.
4. After T steps we get $\sim \beta / c^T$ connected components of size $\sim c^T$.
5. If $\beta \gg n / c^T$ then with high probability one of the edges will be contained in one of the components.



“Lower bound”

Let the communication budget for each player to be β .

Consider player t . Let $C_1^{t-1}, \dots, C_k^{t-1}$ be the connected components created by previous players.

“Lower bound”

Let the communication budget for each player to be β .

Consider player t . Let $C_1^{t-1}, \dots, C_k^{t-1}$ be the connected components created by previous players.

Then the chance of catching a cycle is

$$\Pr_{u,v \leftarrow [n]} [\exists j, \exists (u, v) \in M_t : u, v \in C_j^{t-1}] \leq \frac{1}{n} \sum_{j=1}^k |C_j^{t-1}|^2$$

“Lower bound”

Let the communication budget for each player to be β .

Consider player t . Let $C_1^{t-1}, \dots, C_k^{t-1}$ be the connected components created by previous players.

Then the chance of catching a cycle is

$$\Pr_{u,v \leftarrow [n]} [\exists j, \exists (u, v) \in M_t : u, v \in C_j^{t-1}] \leq \frac{1}{n} \sum_{j=1}^k |C_j^{t-1}|^2$$

Then the probability of T players succeeding is at most $\sum_{t=1}^T O\left(\frac{\sum_{j=1}^k |C_j^t|^2}{n}\right) = O\left(\frac{T \sum_{j=1}^k |C_j^T|^2}{n}\right)$.

“Lower bound”

Let the communication budget for each player to be β .

Consider player t . Let $C_1^{t-1}, \dots, C_k^{t-1}$ be the connected components created by previous players.

Then the chance of catching a cycle is

$$\Pr_{u,v \leftarrow [n]} [\exists j, \exists (u, v) \in M_t : u, v \in C_j^{t-1}] \leq \frac{1}{n} \sum_{j=1}^k |C_j^{t-1}|^2$$

Then the probability of T players succeeding is at most $\sum_{t=1}^T O\left(\frac{\sum_{j=1}^k |C_j^t|^2}{n}\right) = O\left(\frac{T \sum_{j=1}^k |C_j^T|^2}{n}\right)$.

Every step $\sum_{j=1}^k |C_j^T|^2$ increases by at most constant factor, so $\sum_{j=1}^k |C_j^T|^2 \leq \beta C^T$. So, if $\beta \ll n/(100C)^T$, then the probability of succeeding is at most

$$O\left(\frac{T}{100^T}\right)$$

Plan

1. Communication model and streaming lower bounds
2. DIHP problem, reduction from DIHP to Max-Cut
3. Simple protocol for DIHP
- 4. Fourier analysis of the protocol**
5. Generalization of the analysis
6. Intro to quantum
7. How is the quantum result achieved?

Notation

Fix matchings and messages.

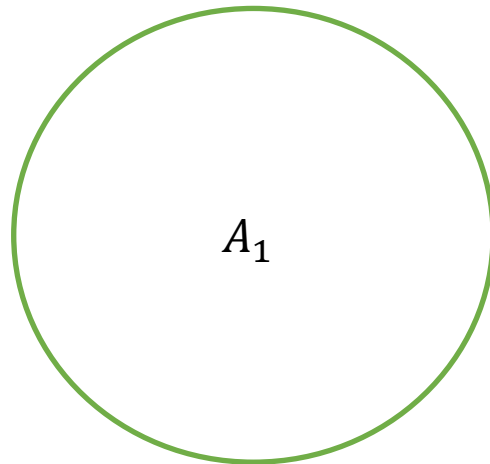
$$B_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with current knowledge}\}$$
$$A_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with the message of player } t\}$$

Notation

Fix matchings and messages.

$$B_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with current knowledge}\}$$

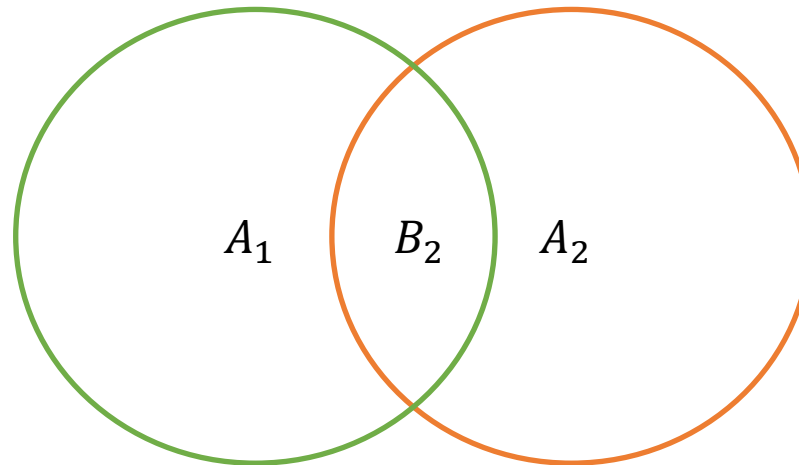
$$A_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with the message of player } t\}$$



Notation

Fix matchings and messages.

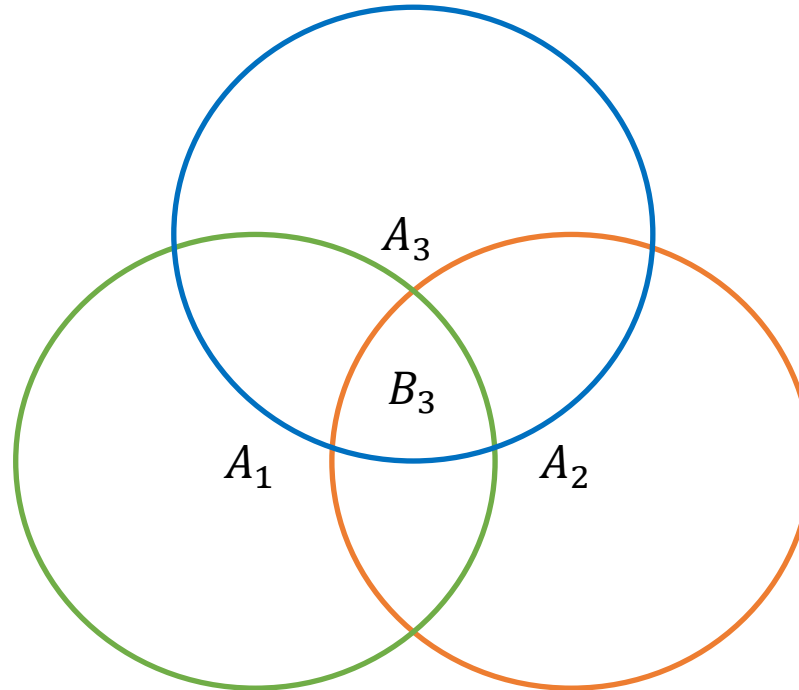
$$B_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with current knowledge}\}$$
$$A_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with the message of player } t\}$$



Notation

Fix matchings and messages.

$$B_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with current knowledge}\}$$
$$A_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with the message of player } t\}$$



Notation

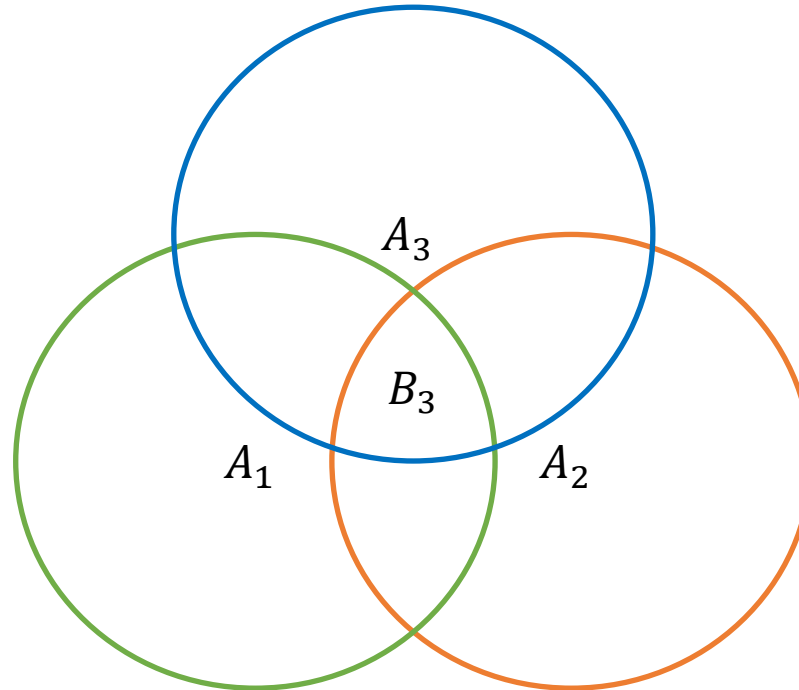
Fix matchings and messages.

$$B_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with current knowledge}\}$$
$$A_t = \{x \in \{0, 1\}^n \mid x \text{ is consistent with the message of player } t\}$$

Let $b_t(x) = \mathbb{1}[x \in B_t]$, $a_t(x) = \mathbb{1}[x \in A_t]$ be indicator functions for these sets.

By definition,

$$B_t = B_{t-1} \cap A_t = A_1 \cap A_2 \cap \dots \cap A_t$$
$$b_t(x) = b_{t-1}(x) \cdot a_t(x) = a_1(x) \cdot a_2(x) \cdot \dots \cdot a_t(x)$$



Fourier analysis

Let $f: \{0,1\}^n \rightarrow \mathbb{R}$. Then Fourier transform $\hat{f}: \{0,1\}^n \rightarrow \mathbb{R}$ is defined

$$\hat{f}(S) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x) \cdot (-1)^{x \cdot S}$$

For $f, g: \{0,1\}^n \rightarrow \mathbb{R}$ define the convolution of them,

$$(f * g)(x) = \sum_{y \in \{0,1\}^n} f(y) \cdot g(x \oplus y)$$

Convolution theorem

$$\widehat{(f \cdot g)} = \hat{f} * \hat{g}$$

Basic facts about the setting

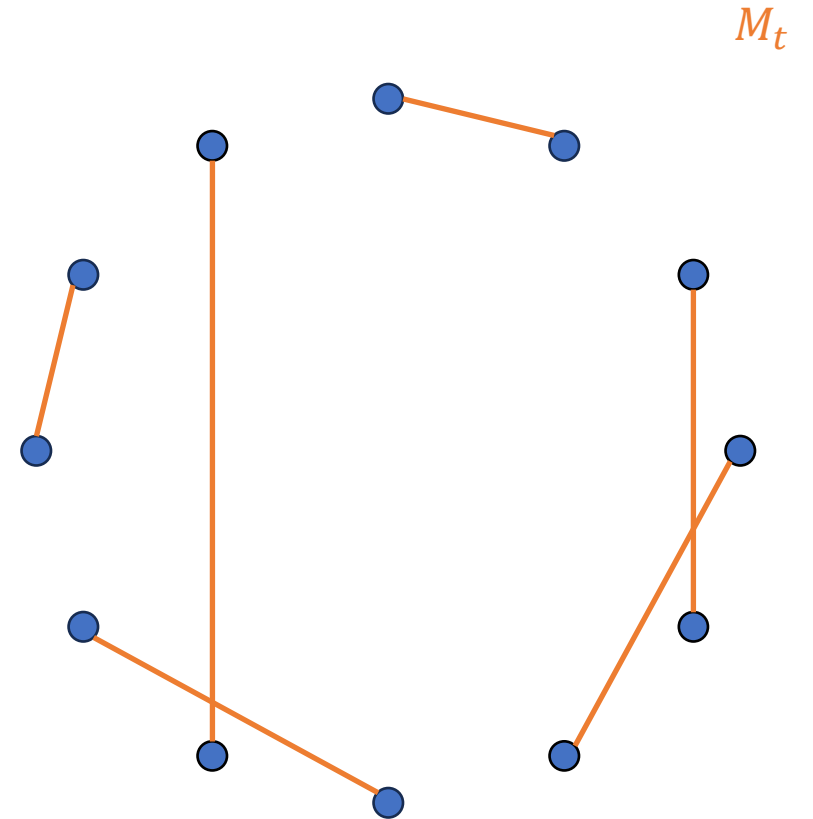
Let's consider Fourier coefficients of a_t and b_t .

$$\hat{a}_t(S) = \begin{cases} \frac{|A_t|}{2^n} (-1)^{w_t \cdot s}, & \text{if } S = M_t^{Tr} s \text{ for some } s \in \{0, 1\}^{\alpha n} \\ 0 & \text{otherwise} \end{cases}$$

Basic facts about the setting

Let's consider Fourier coefficients of a_t and b_t .

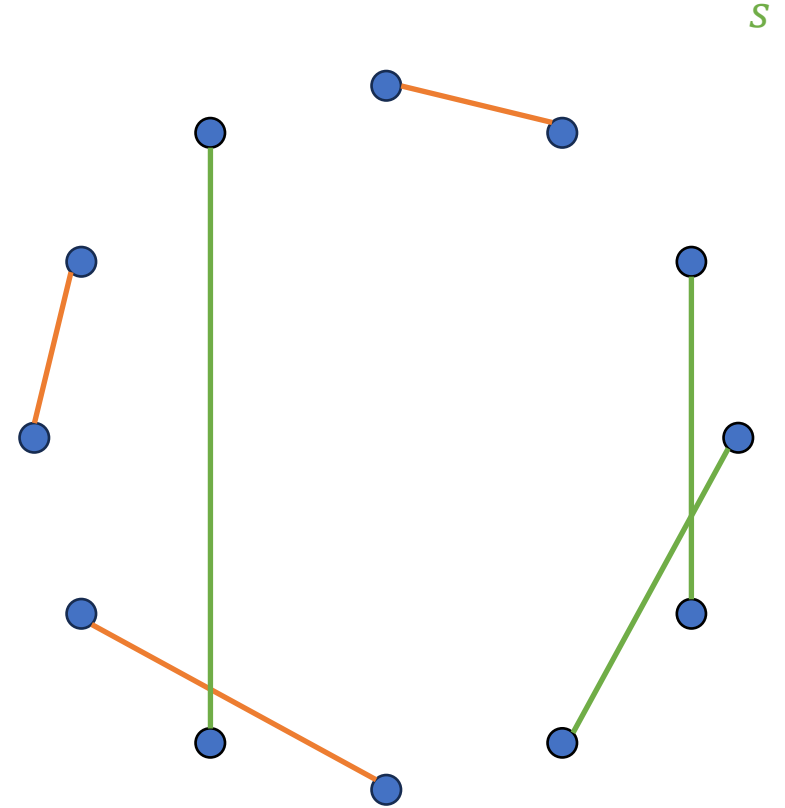
$$\hat{a}_t(S) = \begin{cases} \frac{|A_t|}{2^n} (-1)^{w_t \cdot S}, & \text{if } S = M_t^{Tr} s \text{ for some } s \in \{0, 1\}^{\alpha n} \\ 0 & \text{otherwise} \end{cases}$$



Basic facts about the setting

Let's consider Fourier coefficients of a_t and b_t .

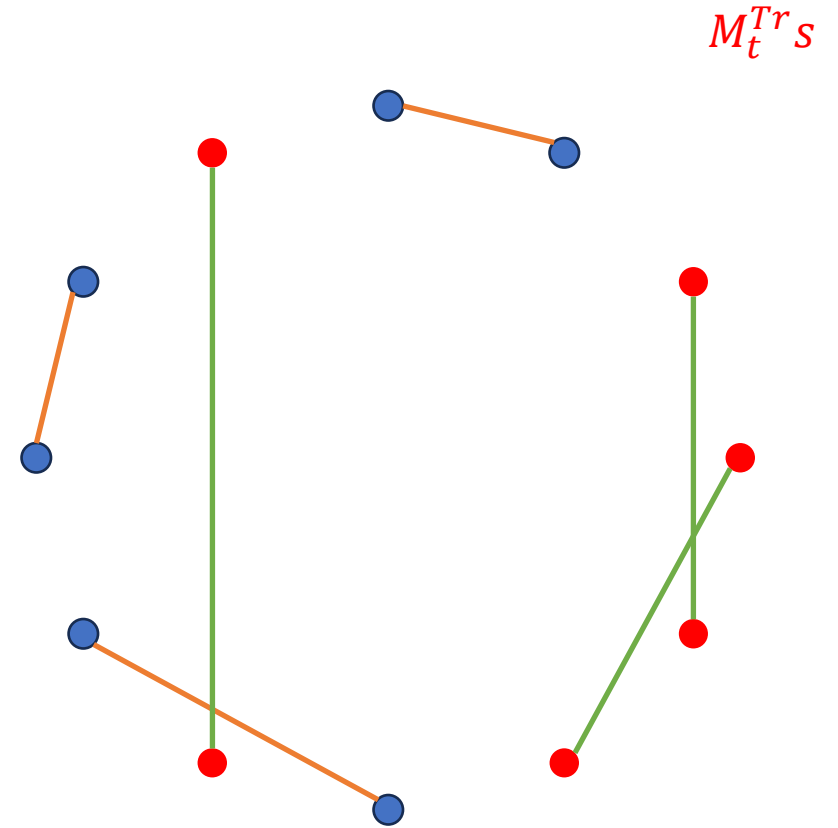
$$\hat{a}_t(S) = \begin{cases} \frac{|A_t|}{2^n} (-1)^{w_t \cdot s}, & \text{if } S = M_t^T r \text{ for some } s \in \{0, 1\}^{\alpha n} \\ 0 & \text{otherwise} \end{cases}$$



Basic facts about the setting

Let's consider Fourier coefficients of a_t and b_t .

$$\hat{a}_t(S) = \begin{cases} \frac{|A_t|}{2^n} (-1)^{w_t \cdot s}, & \text{if } S = M_t^{Tr} s \text{ for some } s \in \{0, 1\}^{\alpha n} \\ 0 & \text{otherwise} \end{cases}$$



Basic facts about the setting

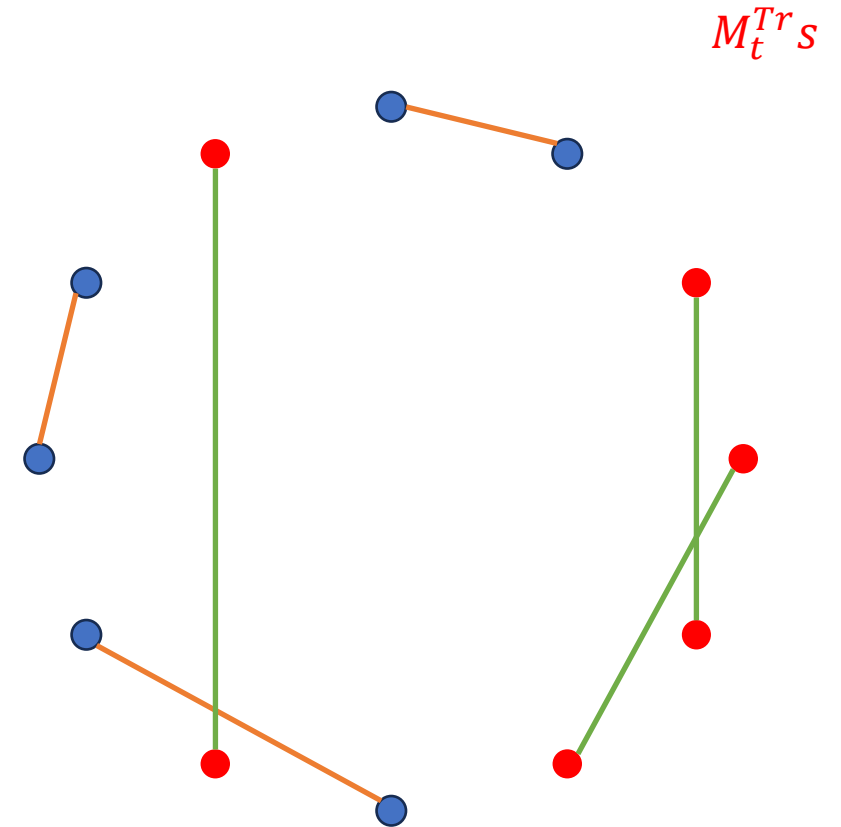
Let's consider Fourier coefficients of a_t and b_t .

$$\hat{a}_t(S) = \begin{cases} \frac{|A_t|}{2^n} (-1)^{w_t \cdot S}, & \text{if } S = M_t^{Tr} s \text{ for some } s \in \{0, 1\}^{\alpha n} \\ 0 & \text{otherwise} \end{cases}$$

In general, if $W \subseteq \{0, 1\}^{\alpha n}$ and $A = \{x \in \{0, 1\}^n \mid Mx \in W\}$ then

$$\hat{a}(S) = \begin{cases} \hat{1}_W(s), & \text{if } S = M^{Tr} s \text{ for some } s \in \{0, 1\}^{\alpha n} \\ 0 & \text{otherwise} \end{cases}$$

- Fourier coefficients of a_t of odd weight are zero
- Fourier coefficients of a_t of weight $> 2\alpha n$ are zero
- The sum of Fourier coefficients of weight $2l$ has only $\binom{n}{l}$ non-zero terms
- Fourier spectrum of a_t is sparse



Basic facts about the setting

$$\hat{a}_t(S) = \begin{cases} \frac{|A_t|}{2^n} (-1)^{w_t \cdot S}, & \text{if } S = M_t^{Tr} s \text{ for some } s \in \{0, 1\}^{\alpha n} \\ 0 & \text{otherwise} \end{cases}$$

By convolution theorem,

$$\hat{b}_t(S) = (\hat{a}_t * \hat{b}_{t-1})(S) = \sum_{U \in \{0,1\}^n} \hat{a}_t(U) \hat{b}_{t-1}(S \oplus U) = \sum_{\substack{U \in \{0,1\}^n \\ \exists l: |U|=2l}} \hat{a}_t(U) \hat{b}_{t-1}(S \oplus U)$$

- All of the odd-weight coefficients of $\hat{b}_t(S)$ are zero!
-And probably Fourier spectrum is sparse as well...

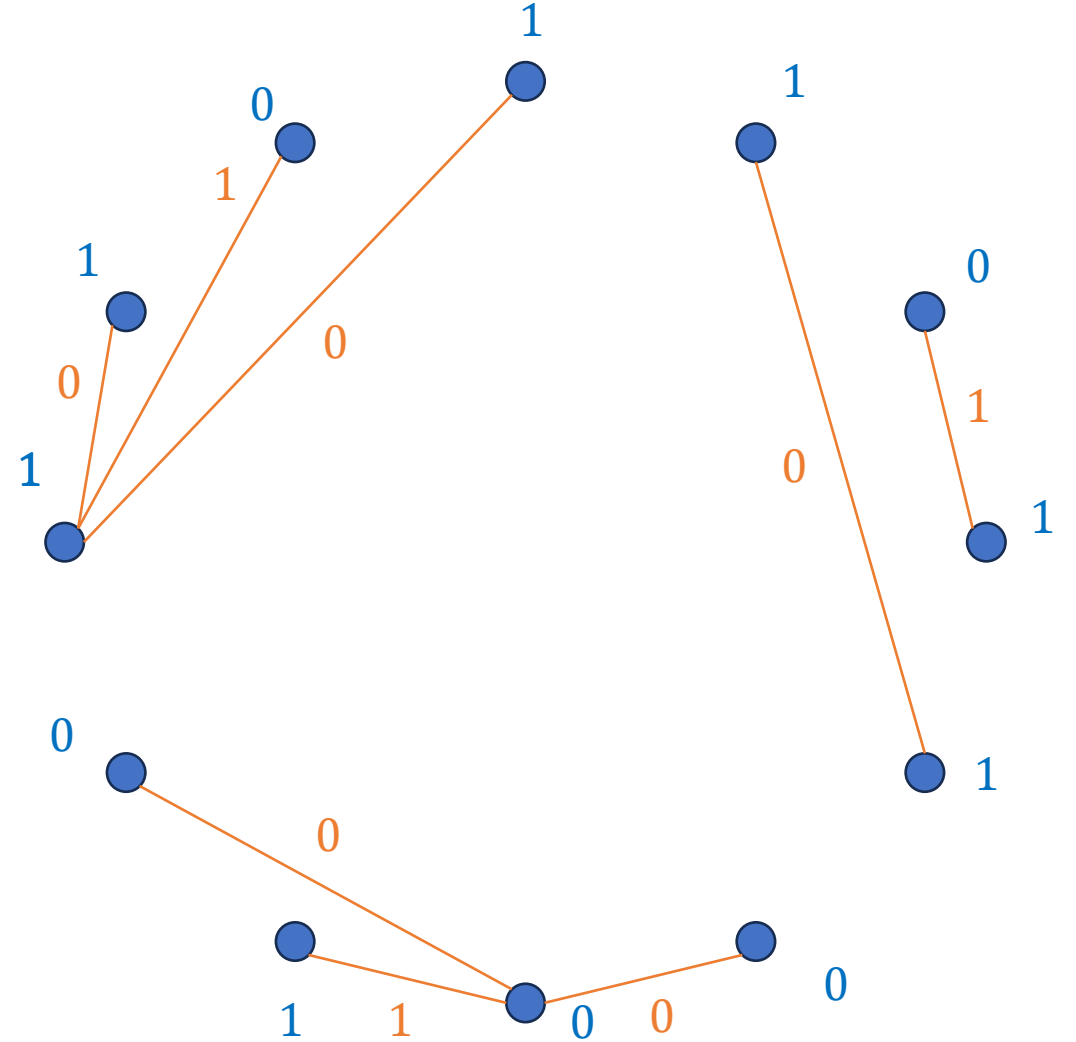
Fourier analysis of component growing protocol

$\hat{b}_t(S) = 0$ if $|S \oplus C|$ is odd for some component C .

Fourier analysis of component growing protocol

$\hat{b}_t(S) = 0$ if $|S \oplus C|$ is odd for some component C .

$$\begin{aligned}\hat{b}_t(S) &= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} b_t(x) (-1)^{S \cdot x} = \frac{1}{2^n} \sum_{x \in B_t} (-1)^{S \cdot x} \\ &= \frac{1}{2^n} (|\{x \in B_t : S \cdot x = 0\}| - |\{x \in B_t : S \cdot x = 1\}|)\end{aligned}$$



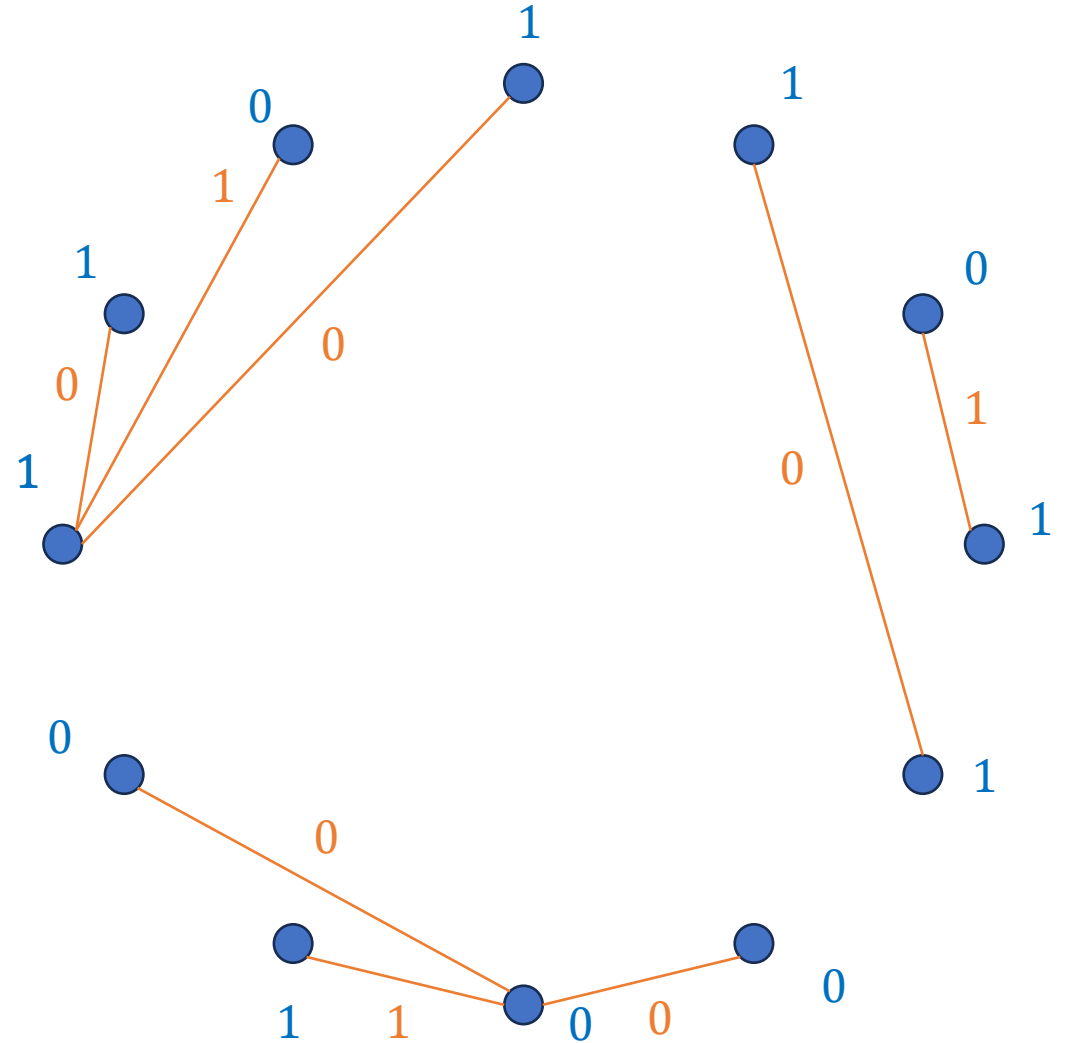
Fourier analysis of component growing protocol

$\hat{b}_t(S) = 0$ if $|S \oplus C|$ is odd for some component C .

$$\begin{aligned}\hat{b}_t(S) &= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} b_t(x) (-1)^{S \cdot x} = \frac{1}{2^n} \sum_{x \in B_t} (-1)^{S \cdot x} \\ &= \frac{1}{2^n} (|\{x \in B_t : S \cdot x = 0\}| - |\{x \in B_t : S \cdot x = 1\}|)\end{aligned}$$

Let S have odd intersection with component $C \in \{0,1\}^n$.

- $S \cdot C = 1$.
- For all $x \in B_t$ it's true that $x + C \in B_t$.



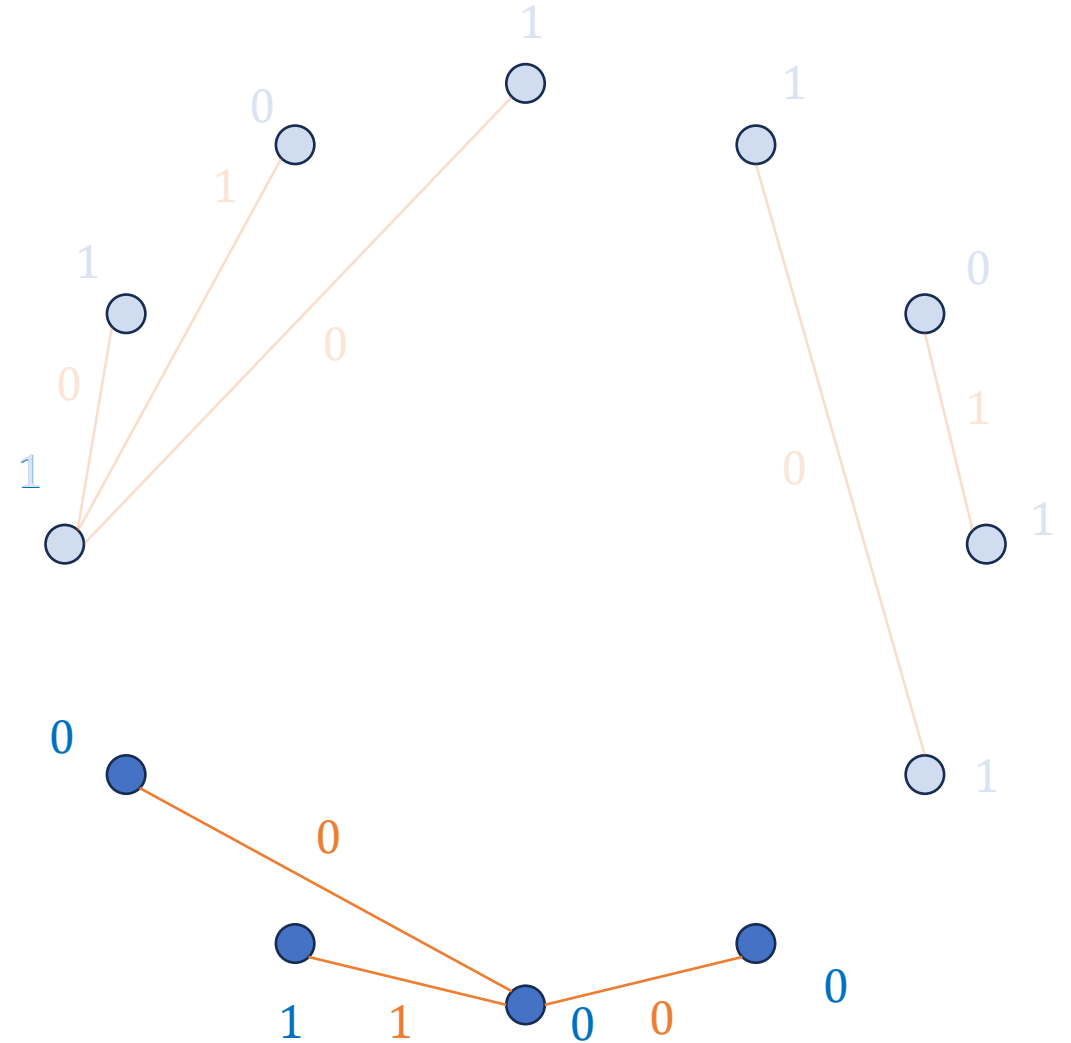
Fourier analysis of component growing protocol

$\hat{b}_t(S) = 0$ if $|S \oplus C|$ is odd for some component C .

$$\hat{b}_t(S) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} b_t(x) (-1)^{S \cdot x} = \frac{1}{2^n} \sum_{x \in B_t} (-1)^{S \cdot x} = \frac{1}{2^n} (|\{x \in B_t : S \cdot x = 0\}| - |\{x \in B_t : S \cdot x = 1\}|)$$

Let S have odd intersection with component $C \in \{0,1\}^n$.

- $S \cdot C = 1$.
- For all $x \in B_t$ it's true that $x + C \in B_t$.



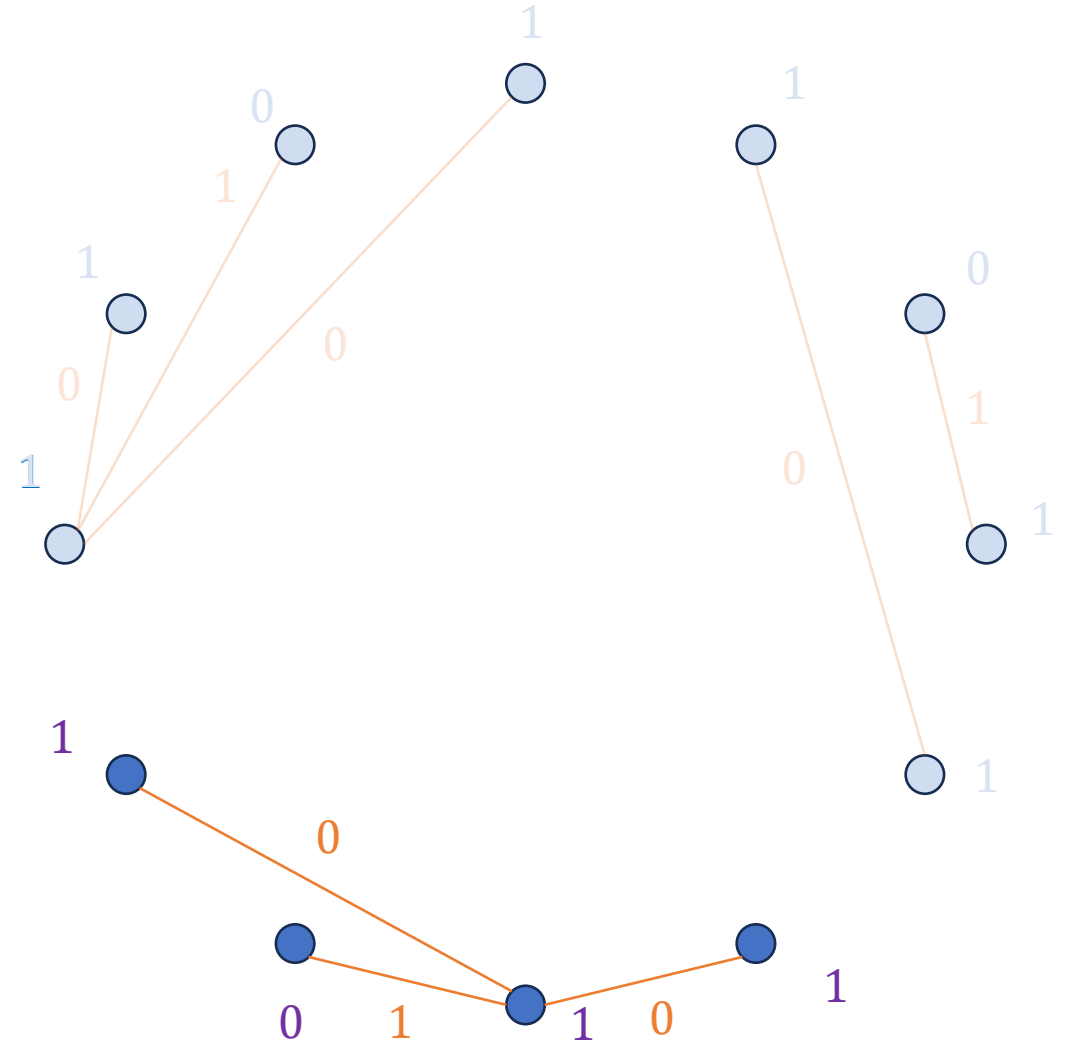
Fourier analysis of component growing protocol

$\hat{b}_t(S) = 0$ if $|S \oplus C|$ is odd for some component C .

$$\hat{b}_t(S) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} b_t(x) (-1)^{S \cdot x} = \frac{1}{2^n} \sum_{x \in B_t} (-1)^{S \cdot x} = \frac{1}{2^n} (|\{x \in B_t : S \cdot x = 0\}| - |\{x \in B_t : S \cdot x = 1\}|)$$

Let S have odd intersection with component $C \in \{0,1\}^n$.

- $S \cdot C = 1$.
- For all $x \in B_t$ it's true that $x + C \in B_t$.



Fourier analysis of component growing protocol

$\hat{b}_t(S) = 0$ if $|S \oplus C|$ is odd for some component C .

$$\begin{aligned}\hat{b}_t(S) &= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} b_t(x) (-1)^{S \cdot x} = \frac{1}{2^n} \sum_{x \in B_t} (-1)^{S \cdot x} \\ &= \frac{1}{2^n} (|\{x \in B_t : S \cdot x = 0\}| - |\{x \in B_t : S \cdot x = 1\}|)\end{aligned}$$

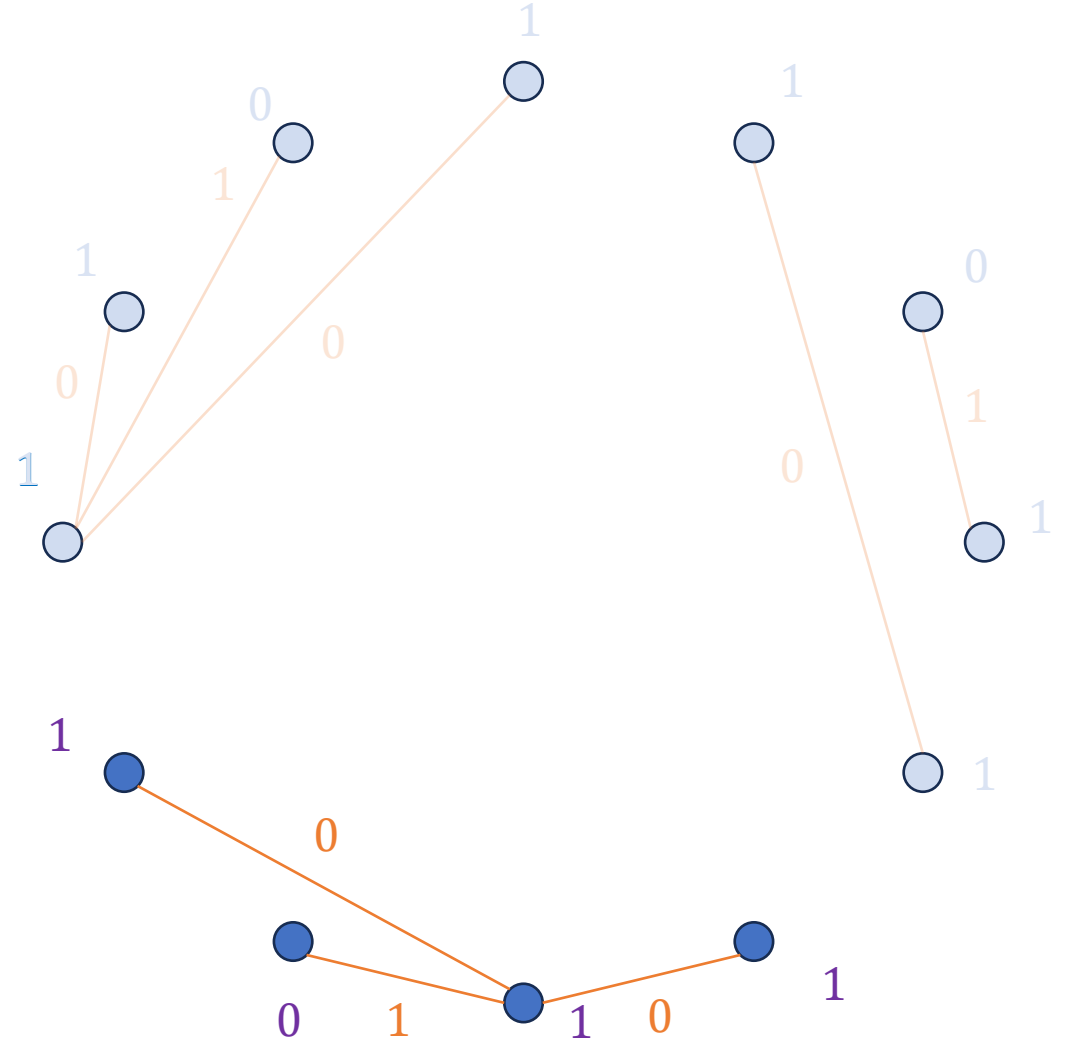
Let S have odd intersection with component $C \in \{0,1\}^n$.

- $S \cdot C = 1$.
- For all $x \in B_t$ it's true that $x + C \in B_t$.

$$S \cdot (x + C) = S \cdot x + 1$$

So

$$\hat{b}_t(S) = \frac{1}{2^n} (|\{x \in B_t : S \cdot x = 0\}| - |\{x \in B_t : S \cdot x = 1\}|) = 0$$



Fourier analysis of component growing protocol

Let's analyze the second layer of Fourier spectrum of b_t

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2}} |\hat{b}_t(S)| = \frac{1}{2} \sum_{\substack{u,v \in [n] \\ u \neq v}} |\hat{b}_t(\{u,v\})| = \frac{1}{2} \sum_{i \in [k]} \sum_{\substack{u,v \in C_i \\ u \neq v}} |\hat{b}_t(\{u,v\})| \approx \frac{|B_t|}{2^n} \sum_{i \in [k]} |C_i^t|^2$$

Fourier analysis of component growing protocol

Let's analyze the second layer of Fourier spectrum of b_t

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2}} |\hat{b}_t(S)| = \frac{1}{2} \sum_{\substack{u,v \in [n] \\ u \neq v}} |\hat{b}_t(\{u,v\})| = \frac{1}{2} \sum_{i \in [k]} \sum_{\substack{u,v \in C_i \\ u \neq v}} |\hat{b}_t(\{u,v\})| \approx \frac{|B_t|}{2^n} \sum_{i \in [k]} |C_i^t|^2$$

From combinatorial analysis, the probability of succeeding is at most

$$\sim \frac{T \sum_{i \in [k]} |C_i^T|^2}{n} = \frac{T}{n} \frac{2^n}{|B_T|} \sum_{\substack{S \in \{0,1\}^n \\ |S|=2}} |\hat{b}_T(S)|$$

Fourier analysis of component growing protocol

Let's analyze the second layer of Fourier spectrum of b_t

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2}} |\hat{b}_t(S)| = \frac{1}{2} \sum_{\substack{u,v \in [n] \\ u \neq v}} |\hat{b}_t(\{u,v\})| = \frac{1}{2} \sum_{i \in [k]} \sum_{\substack{u,v \in C_i \\ u \neq v}} |\hat{b}_t(\{u,v\})| \approx \frac{|B_t|}{2^n} \sum_{i \in [k]} |C_i^t|^2$$

From combinatorial analysis, the probability of succeeding is at most

$$\sim \frac{T \sum_{i \in [k]} |C_i^T|^2}{n} = \frac{T}{n} \frac{2^n}{|B_T|} \sum_{\substack{S \in \{0,1\}^n \\ |S|=2}} |\hat{b}_T(S)|$$

Generalization challenges:

- Higher order coefficients are determined by weight-2 coefficients.
- Combinatorial analysis does not generalize.

Plan

1. Communication model and streaming lower bounds
2. DIHP problem, reduction from DIHP to Max-Cut
3. Simple protocols for DIHP
4. Fourier analysis of the protocol
- 5. Generalization of the analysis**
6. Intro to quantum
7. How is the quantum result achieved?

Fourier analysis

Bounding lemma

Let $W \subseteq \{0, 1\}^m$, $|W| \geq 2^{m-\beta}$. Then for every $l \leq \beta$

$$\sum_{\substack{S \in \{0,1\}^m \\ |S|=l}} |\hat{\mathbb{1}}_W(S)| \leq \frac{|W|}{2^m} \left(\frac{O(\sqrt{\beta n})}{l} \right)^l$$

Follows from hypercontractivity and Cauchy-Schwarz.

Fourier analysis

Bounding lemma

Let $W \subseteq \{0, 1\}^m$, $|W| \geq 2^{m-\beta}$. Then for every $l \leq \beta$

$$\sum_{\substack{S \in \{0,1\}^m \\ |S|=l}} |\hat{\mathbb{1}}_W(S)| \leq \frac{|W|}{2^m} \left(\frac{O(\sqrt{\beta n})}{l} \right)^l$$

Follows from hypercontractivity and Cauchy-Schwarz.

In general, if $W \subseteq \{0, 1\}^{\alpha n}$ and $A = \{x \in \{0, 1\}^n \mid Mx \in W\}$ then

$$\hat{a}(S) = \begin{cases} \hat{\mathbb{1}}_W(s), & \text{if } S = M^{Tr} s \text{ for some } s \in \{0, 1\}^{\alpha n} \\ 0 & \text{otherwise} \end{cases}$$

Bounded sets

$B \subset \{0, 1\}^n$ is (C, β) -**bounded set** if

- For all $l \leq \beta$

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\hat{b}(S)| \leq \frac{|B|}{2^n} \left(\frac{C\sqrt{\beta n}}{l} \right)^l$$

- For all $\beta < l < \frac{n}{C^2}$

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\hat{b}(S)| \leq \frac{|B|}{2^n} \left(\frac{C^2 n}{l} \right)^{\frac{l}{2}}$$

Bounded sets

$B \subset \{0, 1\}^n$ is (C, β) -**bounded set** if

- For all $l \leq \beta$

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\hat{b}(S)| \leq \frac{|B|}{2^n} \left(\frac{C\sqrt{\beta n}}{l} \right)^l$$

- For all $\beta < l < \frac{n}{C^2}$

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\hat{b}(S)| \leq \frac{|B|}{2^n} \left(\frac{C^2 n}{l} \right)^{\frac{l}{2}}$$

How are communication and boundedness related?

For every big $C, \delta < \frac{1}{2}$, small α :

- Let B be (C, β) -bounded for $\beta \in [\ln n, O(n)]$
- $|B| \geq 2^{n-\beta}$.
- Let M be a uniformly random matching on $[n]$ of size αn .

Then with constant probability over M for any $q: \{0, 1\}^{\alpha n} \rightarrow \mathbb{R}$

$$1 - \delta \leq \frac{\mathbb{E}_{x \leftarrow B}[q(Mx)]}{\mathbb{E}_{w \leftarrow \{0,1\}^{\alpha n}}[q(w)]} \leq 1 + \delta$$

Fourier analysis: generalization

For every

- Small α , big C , $\beta < O(\frac{n}{C^3})$, $\delta < 1/2$
- $B \subseteq \{0, 1\}^n$, B is (C, β) -bounded
- M is uniformly random matching of size αn
- $W \subseteq \{0, 1\}^{\alpha n}$ such that $|W| \geq 2^{\alpha n - \beta}$
- $A = \{x \in \{0, 1\}^n \mid Mx \in W\}$

With constant probability over the choice of the matching $D = B \cap A$ is $((\frac{10^9}{\delta}) C, \beta)$ -bounded.

Proof ideas:

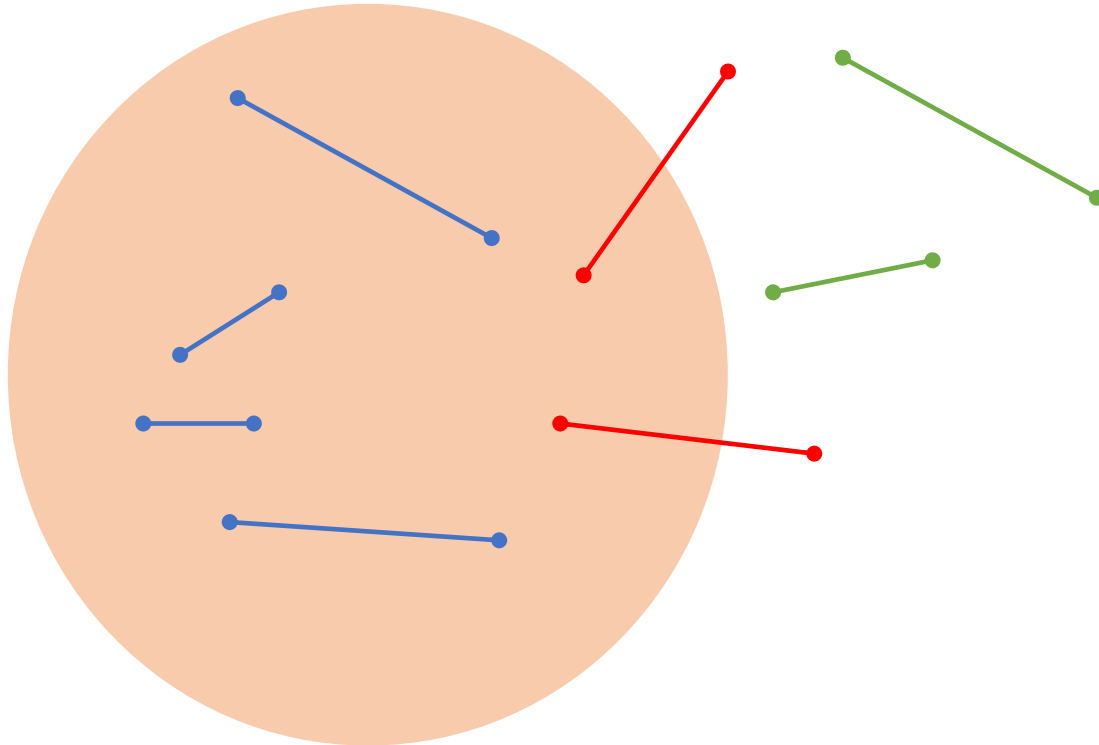
Let d be the indicator function of D .

1. Convolution theorem: $\hat{d} = \hat{a} * \hat{b}$
2.
$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} \hat{d}(S) = \sum_{S \in \{0,1\}^n} \sum_{\substack{s \in \{0,1\}^{\alpha n} \\ |M^{Tr} s \oplus S|=2l}} \hat{a}(M^{Tr} s) \hat{b}(S \oplus M^{Tr} s)$$
3. Mass transfer: How much do low/high weight coefficients of $\hat{b}$ influence low/high weight coefficients of $\hat{d}$?

Generalization: combinatorics

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l_2}} |\hat{a}(S)| \leq \sum_{\substack{S \in \{0,1\}^n \\ |S|=2l_2}} \sum_{s \in \{0,1\}^{an}} |\hat{b}(S \oplus M^{Tr}s) \hat{a}(M^{Tr}s)| \leq \sum_{l_1 \in [n/2]} \left(\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l_1}} |\hat{b}(S)| \sum_{\substack{s \in \{0,1\}^{an} \\ |M^{Tr}s \oplus S|=2l_2}} |\hat{a}(M^{Tr}s)| \right)$$

Let's split this a bit more. Fix S , $|S| = 2l_1$. Remember, $s \in \{0, 1\}^{an}$ indicates a subset of a matching.



a = number of edges of M and s fully contained in S .

b = number of edges of M and s on the boundary of S .

c = number of edges of M and s fully outside of S .

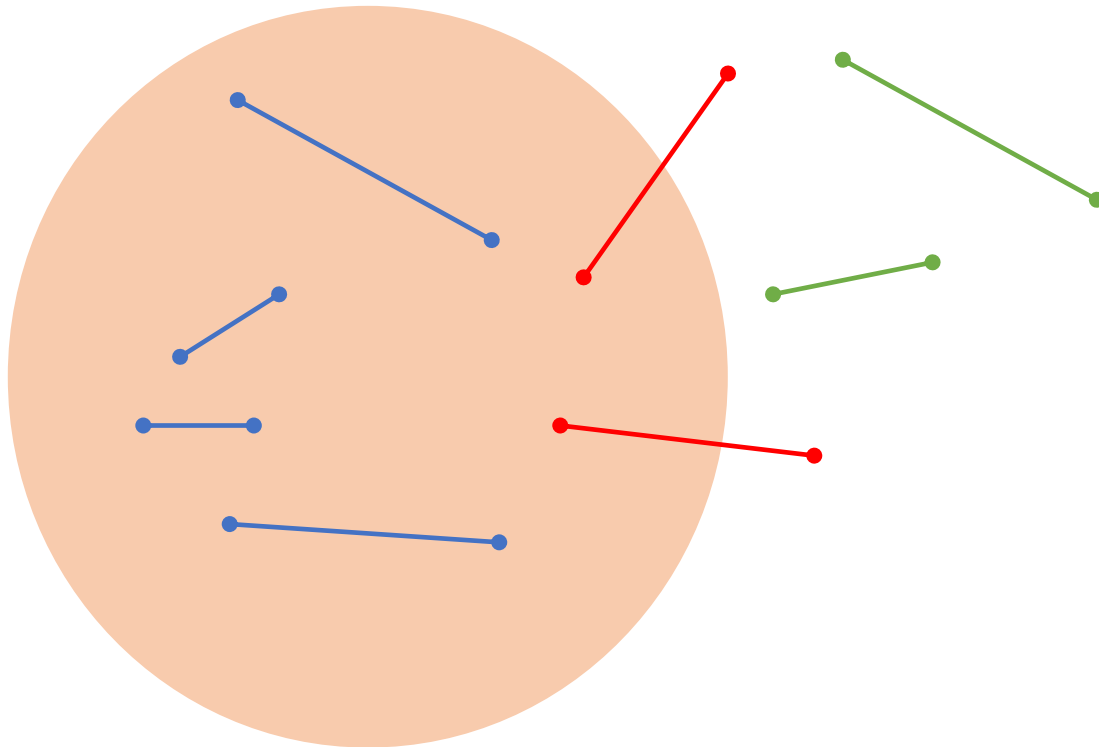
And since $|M^{Tr}s \oplus S| = 2l_2$ and $|S| = 2l_1$,

$$l_1 + c - a = l_2$$

Generalization: combinatorics

S is fixed, $|S| = 2l_1$, S has structure (a, b, c) , $l_1 + c - a = l_2$.

$$\sum_{\substack{s \in \{0,1\}^{\alpha n} \\ |M^{Tr}s \oplus S| = 2l_2}} |\hat{a}(M^{Tr}s)| = \sum_{\substack{u \in \{0,1\}^{\alpha n} \\ |u| = a}} \sum_{\substack{v \in \{0,1\}^{\alpha n} \\ |v| = b}} In_S(u) \partial_S(v) \sum_{\substack{w \in \{0,1\}^{\alpha n} \\ |w| = c}} |\hat{a}(M^{Tr}(u \oplus v \oplus w))|$$



a = number of edges of M and s fully contained in S .

b = number of edges of M and s on the boundary of S .

c = number of edges of M and s fully outside of S .

And since $|M^{Tr}s \oplus S| = 2l_2$ and $|S| = 2l_1$,

$$l_1 + c - a = l_2$$

Generalization: combinatorics

S is fixed, $|S| = 2l_1$, S has structure (a, b, c) , $l_1 + c - a = l_2$.

$$\sum_{\substack{s \in \{0,1\}^{\alpha n} \\ |M^{Tr} s \oplus S| = 2l_2}} |\hat{a}(M^{Tr} s)| = \sum_{\substack{u \in \{0,1\}^{\alpha n} \\ |u| = a}} \sum_{\substack{v \in \{0,1\}^{\alpha n} \\ |v| = b}} In_S(u) \partial_S(v) \sum_{\substack{w \in \{0,1\}^{\alpha n} \\ |w| = c}} |\hat{a}(M^{Tr}(u \oplus v \oplus w))|$$

Overview:

1. Bound $\sum_{\substack{w \in \{0,1\}^{\alpha n} \\ |w| = c}} |\hat{a}(M^{Tr}(u \oplus v \oplus w))|$ for any fixed u, v, M since $\hat{a}$ is sparse.
2. Bound $\sum_{\substack{u \in \{0,1\}^{\alpha n} \\ |u| = a}} \sum_{\substack{v \in \{0,1\}^{\alpha n} \\ |v| = b}} In_S(u) \partial_S(v)$ for matchings sampled u.a.r. and fixed S .
4. Done!

Generalization: combinatorics

S is fixed, $|S| = 2l_1$, S has structure (a, b, c) , $l_1 + c - a = l_2$.

$$\sum_{\substack{s \in \{0,1\}^{\alpha n} \\ |M^{Tr} s \oplus S| = 2l_2}} |\hat{a}(M^{Tr} s)| = \sum_{\substack{u \in \{0,1\}^{\alpha n} \\ |u| = a}} \sum_{\substack{v \in \{0,1\}^{\alpha n} \\ |v| = b}} In_S(u) \partial_S(v) \sum_{\substack{w \in \{0,1\}^{\alpha n} \\ |w| = c}} |\hat{a}(M^{Tr}(u \oplus v \oplus w))|$$

Remember, we want the bound for

$$\sum_{\substack{S \in \{0,1\}^n \\ |S| = 2l_2}} |\hat{d}(S)| \leq \sum_{l_1 \in [n/2]} \left(\sum_{\substack{S \in \{0,1\}^n \\ |S| = 2l_1}} |\hat{b}(S)| \sum_{\substack{s \in \{0,1\}^{\alpha n} \\ |M^{Tr} s \oplus S| = 2l_2}} |\hat{a}(M^{Tr} s)| \right)$$

Overview:

1. Bound $\sum_{\substack{w \in \{0,1\}^{\alpha n} \\ |w| = c}} |\hat{a}(M^{Tr}(u \oplus v \oplus w))|$ for any fixed u, v, M since $\hat{a}$ is sparse.
2. Bound $\sum_{\substack{u \in \{0,1\}^{\alpha n} \\ |u| = a}} \sum_{\substack{v \in \{0,1\}^{\alpha n} \\ |v| = b}} In_S(u) \partial_S(v)$ for matchings sampled u.a.r. and fixed S .
4. Done!

Generalization: combinatorics

S is fixed, $|S| = 2l_1$, S has structure (a, b, c) , $l_1 + c - a = l_2$.

$$\sum_{\substack{s \in \{0,1\}^{\alpha n} \\ |M^{Tr} s \oplus S| = 2l_2}} |\hat{a}(M^{Tr} s)| = \sum_{\substack{u \in \{0,1\}^{\alpha n} \\ |u| = a}} \sum_{\substack{v \in \{0,1\}^{\alpha n} \\ |v| = b}} In_S(u) \partial_S(v) \sum_{\substack{w \in \{0,1\}^{\alpha n} \\ |w| = c}} |\hat{a}(M^{Tr}(u \oplus v \oplus w))|$$

Remember, we want the bound for

$$\sum_{\substack{S \in \{0,1\}^n \\ |S| = 2l_2}} |\hat{d}(S)| \leq \sum_{l_1 \in [n/2]} \left(\sum_{\substack{S \in \{0,1\}^n \\ |S| = 2l_1}} |\hat{b}(S)| \sum_{\substack{s \in \{0,1\}^{\alpha n} \\ |M^{Tr} s \oplus S| = 2l_2}} |\hat{a}(M^{Tr} s)| \right)$$

Overview:

1. Bound $\sum_{\substack{w \in \{0,1\}^{\alpha n} \\ |w| = c}} |\hat{a}(M^{Tr}(u \oplus v \oplus w))|$ for any fixed u, v, M since $\hat{a}$ is sparse.
2. Bound $\sum_{\substack{u \in \{0,1\}^{\alpha n} \\ |u| = a}} \sum_{\substack{v \in \{0,1\}^{\alpha n} \\ |v| = b}} In_S(u) \partial_S(v)$ for matchings sampled u.a.r. and fixed S .
3. Bound $\sum_{\substack{S \in \{0,1\}^n \\ |S| = 2l_1}} |\hat{b}(S)|$ from the boundedness of B .
4. Done!

Generalization result

Previous lemma + induction = B_t is bounded for all t .



Communication bound

For every $\varepsilon \in (0, 1)$ every protocol for $\text{DIHP}(n, \alpha, = 10^{11}, O(\frac{1}{\alpha\varepsilon^2}))$ that succeeds with probability $2/3$ has communication complexity $\geq n / \left(\frac{1}{\varepsilon}\right)^{O(1/\varepsilon^2)}$.



Streaming bound

For every $\varepsilon \in (0, \frac{99}{100})$ every randomized single-pass streaming algorithm that yields $(2 - \varepsilon)$ -approximation to Max-Cut must use $\frac{n}{\left(\frac{1}{\varepsilon}\right)^{\left(\frac{C'}{\varepsilon^2}\right)}} = \Omega(n)$ space.

Plan

1. Communication model and streaming lower bounds
2. DIHP problem, reduction from DIHP to Max-Cut
3. Simple protocol for DIHP
4. Fourier analysis of the protocol
5. Generalization of the analysis
- 6. Intro to quantum**
7. How is the quantum result achieved?

Quantum computing

Classical state = $a \in \{0, 1\}^\beta$

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho_{a,a} = 1,$$

$\rho_{i,j} = 0$ otherwise.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

State = 00

Quantum computing

Classical state = a .

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho_{a,a} = 1,$$
$$\rho_{i,j} = 0 \text{ otherwise.}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

State = 00

State is a distribution over classical states $\{a_1, a_2, \dots, a_{2^\beta}\}$:
state = a_i with probability p_i .

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho_{a_i, a_i} = p_i,$$
$$\rho_{i,j} = 0 \text{ otherwise.}$$

$$\begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{bmatrix}$$

State = $\begin{cases} 00 \\ 11 \end{cases}$ with equal pr

Quantum computing

Classical state = a .

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho_{a,a} = 1,$$

$$\rho_{i,j} = 0 \text{ otherwise.}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

State = 00

Pure quantum state = $|\psi\rangle$.

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho = |\psi\rangle\langle\psi|$$

$$\begin{bmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix}$$

$$\text{State} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

State is a distribution over classical states $\{a_1, a_2, \dots, a_{2^\beta}\}$:
state = a_i with probability p_i .

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho_{a_i, a_i} = p_i,$$

$$\rho_{i,j} = 0 \text{ otherwise.}$$

$$\begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{bmatrix}$$

State = $\begin{cases} 00 \\ 11 \end{cases}$ with equal pr

Quantum computing

Density matrix $\mathbb{C}^{2^\beta \times 2^\beta}$ describes a state on β qubits.

Classical state = a .

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho_{a,a} = 1,$$

$$\rho_{i,j} = 0 \text{ otherwise.}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

State = 00

Pure quantum state = $|\psi\rangle$.

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho = |\psi\rangle\langle\psi|$$

$$\begin{bmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix}$$

$$\text{State} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

State is a distribution over classical states $\{a_1, a_2, \dots, a_{2^\beta}\}$:
state = a_i with probability p_i .

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho_{a_i, a_i} = p_i,$$

$$\rho_{i,j} = 0 \text{ otherwise.}$$

$$\begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{bmatrix}$$

State = $\begin{cases} 00 \\ 11 \end{cases}$ with equal pr

Mixed quantum state: state = $|\phi_i\rangle$ with probability p_i .

Define $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$:

$$\rho = \sum_{i \in [2^\beta]} p_i |\psi_i\rangle\langle\psi_i|$$

$$\begin{bmatrix} 1/4 & 0 & 0 & 1/4 \\ 0 & 1/4 & -1/4 & 0 \\ 0 & -1/4 & 1/4 & 0 \\ 1/4 & 0 & 0 & 1/4 \end{bmatrix}$$

$$\text{State} = \begin{cases} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \end{cases} \text{ with equal pr}$$

Density matrix: properties

Density matrix $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$ describes a state on β qubits.

1. $\text{Trace}(\rho) = 1$.
2. If ρ describes a distribution over classical states then $\rho = \text{diag}(p_1, p_2, \dots, p_{2^\beta})$.

Density matrix: properties

Density matrix $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$ describes a state on β qubits.

1. $\text{Trace}(\rho) = 1$.
2. If ρ describes a distribution over classical states then $\rho = \text{diag}(p_1, p_2, \dots, p_{2^\beta})$.

Trace norm of a matrix $\|A\|_1 = \text{Trace}(|A|)$.

Density matrix: properties

Density matrix $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$ describes a state on β qubits.

1. $\text{Trace}(\rho) = 1$.
2. If ρ describes a distribution over classical states then $\rho = \text{diag}(p_1, p_2, \dots, p_{2^\beta})$.

Trace norm of a matrix $\|A\|_1 = \text{Trace}(|A|)$.

Fact.

The distinguishability of two distributions ρ_1, ρ_2 over quantum states is given by the trace norm of their difference. The probability of distinguishing is

$$\frac{1}{2} + \frac{1}{2} \|\rho_1 - \rho_2\|_1$$

If the states are distributions over classical states then $\|\rho_1 - \rho_2\|_1$ is the total variation distance between the distributions.

Density matrix: properties

Density matrix $\rho \in \mathbb{C}^{2^\beta \times 2^\beta}$ describes a state on β qubits.

1. $\text{Trace}(\rho) = 1$.
2. If ρ describes a distribution over classical states then $\rho = \text{diag}(p_1, p_2, \dots, p_{2^\beta})$.

Trace norm of a matrix $\|A\|_1 = \text{Trace}(|A|)$.

Fact.

The distinguishability of two distributions ρ_1, ρ_2 over quantum states is given by the trace norm of their difference. The probability of distinguishing is

$$\frac{1}{2} + \frac{1}{2} \|\rho_1 - \rho_2\|_1$$

If the states are distributions over classical states then $\|\rho_1 - \rho_2\|_1$ is the total variation distance between the distributions.

Quantum channel: a linear operator $\mathcal{A}: \mathbb{C}^{2^\beta \times 2^\beta} \rightarrow \mathbb{C}^{2^\beta \times 2^\beta}$ that converts one density matrix to another.

Quantum streaming (classical input and output)

- Start with $|\psi\rangle = |00 \dots 0\rangle$
 - Edges arrive one-by-one in arbitrary order
 - If edge (u, v) arrived, apply $\mathcal{A}_{(u,v)}$ to the current state
- Final state $|\psi\rangle = |\phi\rangle|00 \dots 0\rangle$ where $|\phi\rangle$ is set to the output value

[Kallaugher, Parekh, 2022]

Any $(2 - \varepsilon)$ -approximation quantum algorithm requires $\Omega(n)$ qubits for any ε .

In DIHP:

- Start state $|\psi\rangle = |00 \dots 0\rangle$
- Player t applies a quantum channel $\mathcal{B}_{w_t}^t$ to previous state and sends the result further
- Final state $|\psi\rangle = |10 \dots 0\rangle$ in YES case and $|\psi\rangle = |00 \dots 0\rangle$ in NO case

Comparing classical and quantum

$$\begin{aligned} B_t &= \{x \in \{0, 1\}^n \mid x \text{ is consistent with posted messages}\} \\ A_t &= \{x \in \{0, 1\}^n \mid x \text{ is consistent with message of player } t\} \\ B_t &= A_1 \cap A_2 \cap \dots \cap A_t \\ b_t(x) &= a_t(x) \cdot b_{t-1}(x) = a_1(x) \cdot a_2(x) \cdot \dots \cdot a_t(x) \end{aligned}$$

Goal: bound

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\widehat{b}_t(S)|$$

$$\begin{aligned} f_t(x) &= \text{density matrix of player } t \text{ on input } x \\ \mathcal{A}_x^t &= \mathcal{B}_{M_t x}^t \\ f_t(x) &= \mathcal{A}_x^t f_{t-1}(x) = \mathcal{A}_x^t \mathcal{A}_x^{t-1} \dots \mathcal{A}_x^1 |00 \dots 0\rangle \end{aligned}$$

Goal: bound

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} \|\hat{f}_t(S)\|_1$$

Fourier analysis revisited

Let $f: \{0,1\}^n \rightarrow \mathbb{R}$. Then Fourier transform $\hat{f}: \{0,1\}^n \rightarrow \mathbb{R}$ is defined

$$\hat{f}(S) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x) \cdot (-1)^{x \cdot S}$$

Convolution theorem

For $f, g: \{0,1\}^n \rightarrow \mathbb{R}$

$$(\widehat{f \cdot g})(S) = (\hat{f} * \hat{g})(S) = \sum_{U \in \{0,1\}^n} \hat{f}(U) \cdot \hat{g}(S \oplus U)$$

Fourier analysis revisited

Let $f: \{0,1\}^n \rightarrow \mathbb{C}^{m \times m}$. Then Fourier transform $\hat{f}: \{0,1\}^n \rightarrow \mathbb{C}^{m \times m}$ is defined

$$\hat{f}(S) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x) \cdot (-1)^{x \cdot S}$$

Convolution theorem

For $f, g: \{0,1\}^n \rightarrow \mathbb{C}^{m \times m}$

$$(\widehat{f \cdot g})(S) = (\hat{f} * \hat{g})(S) = \sum_{U \in \{0,1\}^n} \hat{f}(U) \cdot \hat{g}(S \oplus U)$$

Fourier analysis revisited

Let $f: \{0,1\}^n \rightarrow \mathbb{C}^{m \times m}$. Then Fourier transform $\hat{f}: \{0,1\}^n \rightarrow \mathbb{C}^{m \times m}$ is defined

$$\hat{f}(S) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x) \cdot (-1)^{x \cdot S}$$

Convolution theorem

For $f, g: \{0,1\}^n \rightarrow \mathbb{C}^{m \times m}$

$$(\widehat{f \cdot g})(S) = (\hat{f} * \hat{g})(S) = \sum_{U \in \{0,1\}^n} \hat{f}(U) \cdot \hat{g}(S \oplus U)$$

For a family of linear operators $(\mathcal{A}_x)_{x \in \{0,1\}^n}: \mathbb{C}^{m \times m} \rightarrow \mathbb{C}^{m \times m}$ denote

$$\widehat{\mathcal{A}}_S = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \mathcal{A}_x \cdot (-1)^{x \cdot S}$$

For $f: \{0,1\}^n \rightarrow \mathbb{C}^{m \times m}$ and family of linear operators $(\mathcal{A}_x)_{x \in \{0,1\}^n}: \mathbb{C}^{m \times m} \rightarrow \mathbb{C}^{m \times m}$, if $g(x) = \mathcal{A}_x f(x)$ then

$$\hat{g}(S) = \sum_{T \in \{0,1\}^n} \widehat{\mathcal{A}}_T \hat{f}(S \oplus T)$$

Boundedness revisited

For any $g: \{0, 1\}^n \rightarrow \mathbb{C}^{2^\beta \times 2^\beta}$ such that $\|g(x)\|_1 \leq 1$ for all x

- For all $l \leq \beta$

$$\sum_{\substack{S \subseteq [n] \\ |S|=l}} \|\hat{g}(S)\|_1 \leq \left(\frac{O(\sqrt{\beta n})}{l} \right)^l$$

- For all $\beta < l$

$$\sum_{\substack{S \subseteq [n] \\ |S|=l}} \|\hat{g}(S)\|_1 \leq \left(\frac{O(n)}{l} \right)^{\frac{l}{2}}$$

Boundedness revisited

For any $g: \{0, 1\}^n \rightarrow \mathbb{C}^{2^\beta \times 2^\beta}$ such that $\|g(x)\|_1 \leq 1$ for all x

- For all $l \leq \beta$

$$\sum_{\substack{S \subseteq [n] \\ |S|=l}} \|\hat{g}(S)\|_1 \leq \left(\frac{O(\sqrt{\beta n})}{l} \right)^l$$

- For all $\beta < l$

$$\sum_{\substack{S \subseteq [n] \\ |S|=l}} \|\hat{g}(S)\|_1 \leq \left(\frac{O(n)}{l} \right)^{\frac{l}{2}}$$

$B \subset \{0, 1\}^n$ is (C, β) -**bounded set** if

- For all $l \leq \beta$

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\hat{b}(S)| \leq \frac{|B|}{2^n} \left(\frac{C\sqrt{\beta n}}{l} \right)^l$$

- For all $\beta < l < \frac{n}{C^2}$

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\hat{b}(S)| \leq \frac{|B|}{2^n} \left(\frac{C^2 n}{l} \right)^{\frac{l}{2}}$$

Boundedness revisited

For any $g: \{0, 1\}^n \rightarrow \mathbb{C}^{2^\beta \times 2^\beta}$ such that $\|g(x)\|_1 \leq 1$ for all x

- For all $l \leq \beta$

$$\sum_{\substack{S \subseteq [n] \\ |S|=l}} \|\hat{g}(S)\|_1 \leq \left(\frac{O(\sqrt{\beta n})}{l} \right)^l$$

- For all $\beta < l$

$$\sum_{\substack{S \subseteq [n] \\ |S|=l}} \|\hat{g}(S)\|_1 \leq \left(\frac{O(n)}{l} \right)^{\frac{l}{2}}$$

$B \subset \{0, 1\}^n$ is (C, β) -**bounded set** if

- For all $l \leq \beta$

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\hat{b}(S)| \leq \frac{|B|}{2^n} \left(\frac{C\sqrt{\beta n}}{l} \right)^l$$

- For all $\beta < l < \frac{n}{C^2}$

$$\sum_{\substack{S \in \{0,1\}^n \\ |S|=2l}} |\hat{b}(S)| \leq \frac{|B|}{2^n} \left(\frac{C^2 n}{l} \right)^{\frac{l}{2}}$$

Proof overview:

1. Proof by induction
2. Bound mass transfer
3. Bound each step due to sparsity of the graph

Related papers that didn't fit into this talk

- *Exponential separation for one-way quantum communication complexity, with applications to cryptography.* [Gavinsky, Kempe, Kerenidis, Raz, de Wolf'08]
 - Gives an upper bound for two-party version of DIHP for quantum communication
 - Gives a lower bound for two-party version of DIHP for classical communication
 - Uses Fourier analysis for the classical lower bound (l_2 bound)
 - Was used in [Kapralov, Khanna, Sudan'15] to prove $\Omega(\sqrt{n})$ space bound for $(2 - \varepsilon)$ -approximation of Max-Cut
- *The Quantum and Classical Streaming Complexity of Quantum and Classical Max-Cut.* [Kallaugher, Parekh'22]
 - Gives an $\Omega(n)$ bound for $(2 - \varepsilon)$ -approximation of Max-Cut in quantum streaming setting
 - Gives an $\Omega(n)$ bound for $(2 - \varepsilon)$ -approximation of Quantum Max-Cut in quantum streaming setting
 - Gives an $O(\log n)$ bound for $(2 + \varepsilon)$ -approximation of Quantum Max-Cut in quantum streaming setting (non-trivial)
- *Linear Space Streaming Lower Bounds for Approximating CSPs.* [Chou, Golovnev, Sudan, Velingker, Velusamy'22]
 - Gives lower bounds for Max-CSP approximation for a certain family of CSP's
 - Considers a problem similar to DIHP, but over hypergraphs and $\mathbb{Z}_p$
 - Extends the analysis from this talk to Max-CSP's

Summary

- Approximating Max-Cut is as hard as it can be in streaming setting.
- Even for quantum memory!
- Bounding l_1 -norm of Fourier coefficients directly could be much more powerful than l_2 -norm if Fourier spectrum is sparse.
- Lower bounds through Fourier analysis have the potential to be generalized for quantum computation/communication

Summary

- Approximating Max-Cut is as hard as it can be in streaming setting.
- Even for quantum memory!
- Bounding l_1 -norm of Fourier coefficients directly could be much more powerful than l_2 -norm if Fourier spectrum is sparse.
- Lower bounds through Fourier analysis have the potential to be generalized for quantum computation/communication

The end.

Thank you!