Quantum Query complexity lower bounds

Nemo Fournier   Jérémy Petithomme   Ugo Giocanti

December 6, 2019

Outline

1. Nemo
   - Quantum Lower Bounds by polynomials

2. Jérémy
   - Quantum Lower Bounds by Quantum Arguments

3. Ugo
   - Some “easy” to decide properties
   - A general lower bound for functions invariant under transitive group action

Some context

Quantum Lower Bounds by Polynomials (Beals, Cleve, Mosca, Wolf, 1998)

Deutsch–Jozsa algorithm (1992): 2^n queries *vs* 1 query

Simon algorithm (1994): $\Omega\left(2^{\frac{n}{2}}\right)$ queries *vs* $\mathcal{O}(n)$

Grover algorithm (1996): n queries *vs* $\sqrt{n}$ queries

Black-box framework

X

$$x_0, x_1, x_2, x_3, \ldots, x_{N-2},\ x_{N-1}$$

$$\big\downarrow \text{ property } f$$

$$f(X) \in \{0, 1\}$$

Black-box framework

$$X = \boxed{x_0, x_1, x_2, x_3, \ldots, x_{N-2},\ x_{N-1}}$$

$$\Big\downarrow \quad \text{property } f$$

$$f(X) \in \{0, 1\}$$

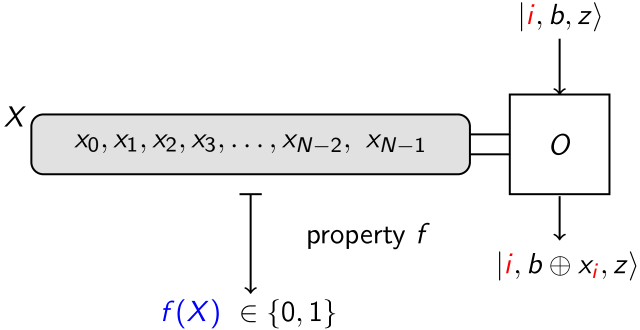
$$f(X) = x_0 \vee x_1 \vee x_2 \vee \cdots \vee x_{N-1}$$

$$f(X) = x_0 \wedge x_1 \wedge x_2 \wedge \cdots \wedge x_{N-1}$$

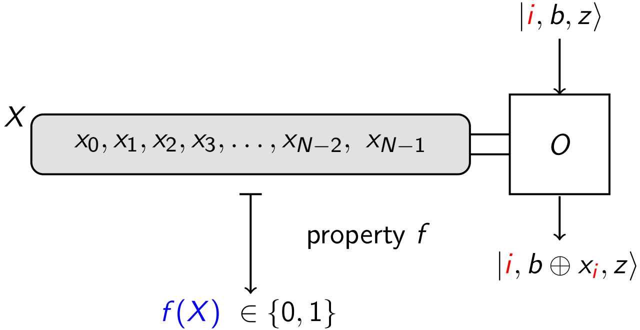
$$f(X) = (-1)^{|X|}$$

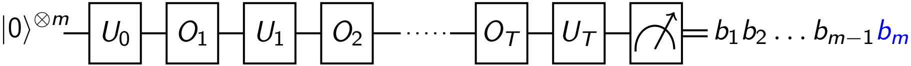
$$f(X) = \text{MAJORITY}(X)$$

Black-box framework

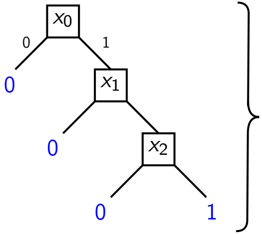


Black-box framework





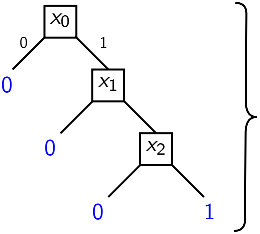
Notions of Query Complexity



$D(f)$

Classical Query Complexity

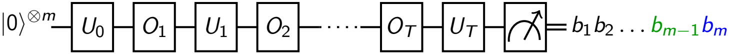
Notions of Query Complexity



$D(f)$

Classical Query Complexity

Quantum Query Complexity



$Q_E(f)$: smallest T in the exact setting.

$Q_2(f)$: smallest T in the approximate setting $(\mathbf{P}\{b_m \neq f(X)\} \leq 1/3)$

$Q_0(f)$: smallest T in the 0-error setting $(b_{m-1} = 1 \implies b_m = f(X))$

Representation by Polynomials

$$f : \{0,1\}^N \to \{0,1\} \text{ and } P \in \mathbf{R}[x_0, x_1, \dots, x_N - 1]$$

P **represents** f if $\forall X \in \{0,1\}^N, P(X) = f(X)$

e.g. $P(X) = 1 - (1 - x_0)\dots(1 - x_{N-1})$ represents OR

P **approximates** f if $\forall X \in \{0,1\}^N, |P(X) - f(X)| \leq 1/3$

e.g. $P(X) = \frac{1}{3}x_0 + \frac{1}{3}x_1$ approximtes AND

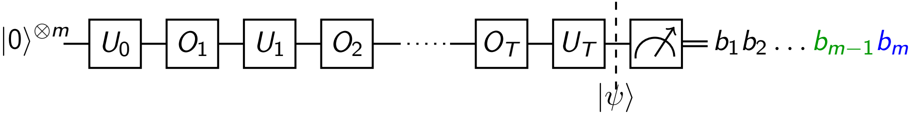
$$\deg(f) = \min_{P \text{ represents } f} \deg P \quad \text{and} \quad \widetilde{\deg}(f) = \min_{P \text{ approximates } f} \deg P$$

Tools from the Polynomial World

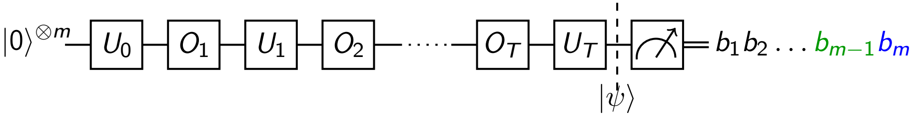
Theorem (Nisan, Szegedy)

If f depends on N variables then $\deg(f) \geq \log N - \mathcal{O}(\log\log N)$

A first Lower Bound, in the exact setting

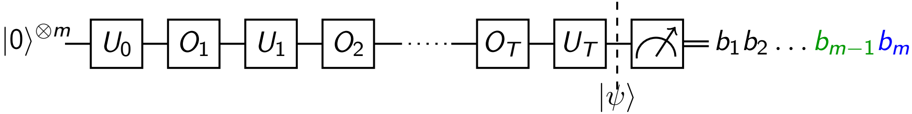


A first Lower Bound, in the exact setting



$$|\psi\rangle = \sum_{k \in \{0,1\}^m} p_k(X) \, |k\rangle$$

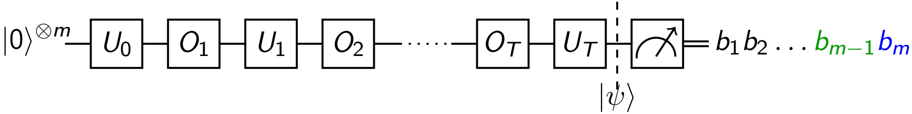
A first Lower Bound, in the exact setting



$$|i, b, z\rangle \mapsto |i, b \oplus x_i, z\rangle$$

$$|\psi\rangle = \sum_{k \in \{0,1\}^m} p_k(X) |k\rangle$$

A first Lower Bound, in the exact setting

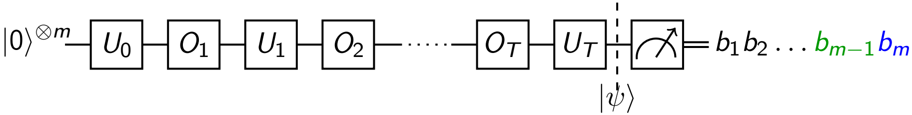


$$|i, b, z\rangle \mapsto |i, b \oplus x_i, z\rangle$$

$$|\psi\rangle = \sum_{k \in \{0,1\}^m} p_k(X) |k\rangle$$

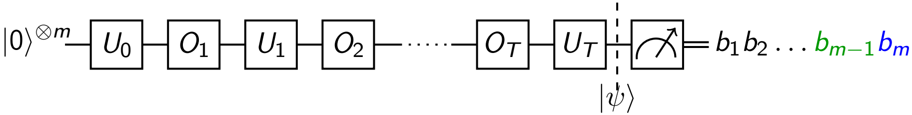
$$\begin{array}{ccc} \alpha |i, 0, z\rangle & \multirow{2}{*}{$\mapsto$} & ((1 - x_i)\alpha + x_i \beta) |i, 0, z\rangle \\ \beta |i, 1, z\rangle & & (x_i \alpha + (1 - x_i)\beta) |i, 1, z\rangle \end{array}$$

A first Lower Bound, in the exact setting



$$|\psi\rangle = \sum_{k \in \{0,1\}^m} p_k(X) |k\rangle \qquad \text{with } \deg p_k \leq T$$

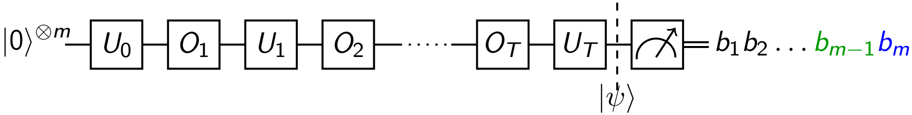
A first Lower Bound, in the exact setting



$$|\psi\rangle = \sum_{k \in \{0,1\}^m} p_k(X)\,|k\rangle \qquad \text{with } \deg p_k \leq T$$

Consequence: for $T = Q_E(f)$, $P(X) = \sum_{k \in B} |p_k(X)|^2$ represents f, and $\deg(P) \leq 2T$, hence $Q_E(f) \geq \deg(f)/2$

A first Lower Bound, in the exact setting



$$|\psi\rangle = \sum_{k \in \{0,1\}^m} p_k(X) \, |k\rangle \qquad \text{with } \deg p_k \leq T$$

Consequence: for $T = Q_E(f)$, $P(X) = \sum_{k \in B} |p_k(X)|^2$ represents f, and $\deg(P) \leq 2T$, hence $Q_E(f) \geq \deg(f)/2$

$$Q_E(f) \geq \frac{\log(N)}{2} - \mathcal{O}(\log \log N)$$

The quantum advantage is at most polynomial

$$Q_E(f) \geq \sqrt{bs(f)/8},\ Q_2(f) \geq \sqrt{bs(f)/16}$$

The quantum advantage is at most polynomial

$Q_E(f) \geq \sqrt{bs(f)/8}$, $Q_2(f) \geq \sqrt{bs(f)/16}$
$D(f) \leq bs(f)^3$

The quantum advantage is at most polynomial

$Q_E(f) \geq \sqrt{bs(f)/8}$, $Q_2(f) \geq \sqrt{bs(f)/16}$
$D(f) \leq bs(f)^3$

$$D(f) \leq 4096 Q_2(f)^6$$

Outline

1. Nemo
   - Quantum Lower Bounds by polynomials
2. Jérémy
   - Quantum Lower Bounds by Quantum Arguments
3. Ugo
   - Some “easy” to decide properties
   - A general lower bound for functions invariant under transitive group action

Motivation

Quantum Algorithm $\rightarrow$ Quantum Adversary

Motivation

Quantum Algorithm $\rightarrow$ Quantum Adversary

Oracle part + Algorithm part

Motivation

Quantum Algorithm $\rightarrow$ Quantum Adversary

Oracle part + Algorithm part $\rightarrow$ entangled

Motivation

Quantum Algorithm $\rightarrow$ Quantum Adversary

Oracle part + Algorithm part $\rightarrow$ entangled

– Tools

Motivation

Quantum Algorithm $\rightarrow$ Quantum Adversary

Oracle part + Algorithm part $\rightarrow$ entangled

- Tools
- New lower bounds

Motivation

Quantum Algorithm $\rightarrow$ Quantum Adversary

Oracle part $+$ Algorithm part $\rightarrow$ entangled

- Tools
- New lower bounds
- General lower bound theorem (Unification of proofs)

Model

We consider:

- A boolean function: $f : \{0,1\}^N \to \{0,1\}$
- An oracle O

Model

We consider:

- A boolean function: $f : \{0,1\}^N \to \{0,1\}$
- An oracle O

Network:

$$U_0 \to O \to U_1 \to O \to ... \to U_{T-1} \to O \to U_T$$

O_x: oracle transformation corresponding to input x

Model

Initial state: $|0\rangle$
Measure: rightmost bit of the final state

Definition (*Error of a quantum network*)

We say that a quantum network computes f with bounded error if, for every $x = (x_1, ...x_N)$, the probability that the rightmost bit of $U_T O_x U_{T-1} ... O_x U_0 |0\rangle$ equals $f(x_1, ..., x_N)$ is at least $1 - \epsilon$ for some $\epsilon > \frac{1}{2}$.

Idea

Let

- $S \subseteq \{0,1\}^N$
- $\mathcal{H}_A$ the workspace of the algorithm A
- $\mathcal{H}_I$ is an "input space"

Idea

Let

$S \subseteq \{0,1\}^N$

$\mathcal{H}_A$ the workspace of the algorithm A

$\mathcal{H}_I$ is an "input space"

We consider the bipartite system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_I$

$$U_T O U_{T-1} \ldots O U_0 \quad \rightarrow \quad U'_T O' U'_{T-1} \ldots O' U'_0$$

where

$U'_i = U_i \otimes I$

O' is simply O_x on $\mathcal{H}_A \otimes |x\rangle$

Idea

Beginning: algorithm in state $|0\rangle$. Initial state of the system:

$$|\psi_{start}\rangle = |0\rangle \otimes \sum_{x \in S} \alpha_x |x\rangle$$

Idea

Beginning: algorithm in state $|0\rangle$. Initial state of the system:

$$|\psi_{start}\rangle = |0\rangle \otimes \sum_{x \in S} \alpha_x |x\rangle$$

Final state

$$|\psi_{end}\rangle = \sum_{x \in S} \alpha_x |\psi_x\rangle \otimes |x\rangle$$

where $|\psi_x\rangle$ is the final state of $U_T O_x U_{T-1} \dots O_x U_0 |0\rangle$.

Idea

Beginning: algorithm in state $|0\rangle$. Initial state of the system:

$$|\psi_{start}\rangle = |0\rangle \otimes \sum_{x \in S} \alpha_x |x\rangle$$

Final state

$$|\psi_{end}\rangle = \sum_{x \in S} \alpha_x |\psi_x\rangle \otimes |x\rangle$$

where $|\psi_x\rangle$ is the final state of $U_T O_x U_{T-1} \ldots O_x U_0 |0\rangle$.

If $\alpha_x = \frac{1}{\sqrt{m}}$ for all x and $\epsilon = 0$,

$$|\psi_{end}\rangle = \frac{1}{\sqrt{m}} \sum_{x \in S} |x\rangle |\varphi_x\rangle \otimes |x\rangle$$

$\Rightarrow$ full entanglement.

Idea

Bound the entanglement:
We trace out $\mathcal{H}_A$ from $|\psi_{start}\rangle$ and $|\psi_{end}\rangle$

$\Rightarrow$ mixed states over $\mathcal{H}_I$

ρ_{start} and ρ_{end} density matrices.

Starting state $\sum_{x \in S} \alpha_x |x\rangle \Leftrightarrow (\rho_{start})_{xy} = \alpha_x^* \alpha_y$.

Lemma

Let A be an algorithm that computes f with probability at least $1 - \epsilon$. Let x, y be such that $f(x) \neq f(y)$. Then,

$$|(\rho_{end})_{xy}| \leq 2\sqrt{\epsilon(1-\epsilon)}|\alpha_x||\alpha_y|$$

General lower bound theorem

Theorem

Let $f(x_1, ..., x_N)$ be a function of n $\{0, 1\}$-valued variables and X, Y be two sets of inputs such that $f(x) \neq f(y)$ if $x \in X$ and $y \in Y$. Let $R \subset X \times Y$ be such that:

1. *For every $x \in X$ there exist at least m different $y \in Y$ such that $(x, y) \in R$.*
2. *For every $y \in Y$ there exist at least m' different $x \in X$ such that $(x, y) \in R$.*
3. *For every $x \in X$ and $i \in \{1, ..., n\}$ there are at most l different $y \in Y$ such that $(x, y) \in R$ and $x_i \neq y_i$.*
4. *For every $y \in Y$ and $i \in \{1, ..., n\}$ there are at most l' different $x \in X$ such that $(x, y) \in R$ and $x_i \neq y_i$.*

Then any algorithm computing f uses $\Omega\left(\sqrt{\frac{mm'}{ll'}}\right)$ queries.

Block sensivity

General lower bound theorem: generalization of the block sensitivity bound.

Theorem

Let f be any Boolean function (or property). Then, any quantum algorithm computing f uses $\Omega(\sqrt{bs(f)})$ queries.

Particular case of the general theorem. Let :

x be the input on which f achieves $bs(f)$

$X = \{x\}$, $Y = \{x^{(S_1)}, ..., x^{(S_{bs(f)})}\}$

$R = \{(x, x^{(S_1)}), (x, x^{(S_2)}), ..., (x, x^{(S_{bs(f)})})\}$.

We have $m = bs(f)$, $m' = 1$, $l = 1$ and $l' = 1$.
Bound :

$$\Omega\left(\sqrt{\frac{mm'}{ll'}}\right) = \Omega\left(\sqrt{bs(f)}\right)$$

AND and OR's

Let $x_1, \ldots, x_N$ be N boolean variables, we consider a function AND and ORs:

$$f(x_1, \ldots, x_N) = (x_1 OR x_2 \ldots OR x_{\sqrt{N}}) AND \ldots AND (x_{N-\sqrt{N}+1} OR \ldots OR x_N)$$

Theorem

Any quantum algorithm computing AND and ORs uses $\Omega(\sqrt{N})$ queries.

Proof.

Application of the general lower bound theorem. □

Better than BS: $\Theta(\sqrt{bs(f)}) = \Theta(\sqrt{N})$.

More general result

Theorem

Let $f(x_1, \ldots, x_N)$ be a function of n $\{0,1\}$-valued variables and X, Y be two sets of inputs such that $f(x) \neq f(y)$ if $x \in X$ and $y \in Y$. Let $R \subset X \times Y$ be such that:

1. *For every $x \in X$ there exist at least m different $y \in Y$ such that $(x, y) \in R$.*
2. *For every $y \in Y$ there exist at least m' different $x \in X$ such that $(x, y) \in R$.*

– *Let $l_{x,i}$ be the number of $y \in Y$ such that $(x, y) \in R$ and $x_i \neq y_i$*

– *Let $l_{y,i}$ be the number of $x \in X$ such that $(x, y) \in R$ and $x_i \neq y_i$*

– *Let l_{max} be the maximum of $l_{x,i} l_{y,i}$ over all $(x, y) \in R$ and $i \in \{1, \ldots, N\}$ such that $x_i \neq y_i$.*

Then any algorithm computing f uses $\Omega\left(\sqrt{\frac{mm'}{l_{max}}}\right)$

Outline

1. Nemo
   - Quantum Lower Bounds by polynomials
2. Jérémy
   - Quantum Lower Bounds by Quantum Arguments
3. Ugo
   - Some “easy” to decide properties
   - A general lower bound for functions invariant under transitive group action

(directed)

Invariance, circularity

Invariance, circularity

Definiton (Invariance)

Let $f : \{0,1\}^N \to \{0,1\}$ be a property, and Γ a subgroup of $\mathfrak{S}_N$. We say that f is invariant under the action of Γ iff :

$$\forall\ (x_1, ..., x_N) \in \{0,1\}^N,\ \forall\ \sigma \in \Gamma,\ f(x_{\sigma(1)}, ..., x_{\sigma(N)}) = f(x_1, ..., x_N)$$

Circular functions

Circular functions

Definiton (circularity)

A circular function $f : \{0,1\}^N \rightarrow \{0,1\}$ *is a property invariant under the cyclic action of* $\Gamma := <(1\ 2\ \ldots\ N)>$, *i.e :*

$$\forall (x_1, \ldots, x_n) \in \{0,1\}^N,\ \forall l \in \{1, \ldots, N\},\ f(x_{1+l \ mod(N)}, \ldots, x_{N+l \ mod(N)}) = f(x_1, \ldots, x_N)$$

Circular functions

Definiton (circularity)

A circular function $f : \{0,1\}^N \rightarrow \{0,1\}$ *is a property invariant under the cyclic action of* $\Gamma :=< (1\ 2\ ...\ N) >$, *i.e :*

$$\forall (x_1, ..., x_n) \in \{0,1\}^N,\ \forall l \in \{1, ..., N\},\ f(x_{1+l \ mod(N)}, \dots, x_{N+l \ mod(N)}) = f(x_1, ..., x_N)$$

Theorem (Sun, Xiaoming, Yao, 2004)

There exists a circular non-constant function $f : \{0,1\}^N \rightarrow \{0,1\}$, *such that forall* $\epsilon > 0$*:*

$$Q_2(f) = \mathcal{O}(N^{\frac{1}{4}+\epsilon})$$

Graph Properties

We identify $\{1, ..., N\}$ with set of edges when $N = \binom{n}{2}$ (resp. with set of arcs when $N = n(n-1)$), and $\{0,1\}^N$ with set of graphs (resp. directed graph).

Graph Properties

We identify $\{1, ..., N\}$ with set of edges when $N = \binom{n}{2}$ (resp. with set of arcs when $N = n(n-1)$), and $\{0,1\}^N$ with set of graphs (resp. directed graph).

Definiton (Graph properties)

A (directed) graph property $f : \{0,1\}^N \to \{0,1\}$ *when* $N = \binom{n}{2}$ *(resp.* $N = n(n-1)$*) is a property stable under graph isomorphism.*

Graph Properties

We identify $\{1, \ldots, N\}$ with set of edges when $N = \binom{n}{2}$ (resp. with set of arcs when $N = n(n-1)$), and $\{0,1\}^N$ with set of graphs (resp. directed graph).

Definiton (Graph properties)

A (directed) graph property $f : \{0,1\}^N \to \{0,1\}$ when $N = \binom{n}{2}$ (resp. $N = n(n-1)$) is a property stable under graph isomorphism.

Claim

A property $f : \{0,1\}^N \to \{0,1\}$ is a graph property iff it is invariant by the group action induced by relabelling of vertices.

Graph properties in the classical deterministic model

Graph properties in the classical deterministic model

Theorem (Rivest, Vuillemin, 1976)

If $f : \{0,1\}^N \to \{0,1\}$ *is a non-constant monotone graph property or a directed graph property, we have:*

$$D(f) = \Omega(N) = \Omega(n^2)$$

Graph properties in the classical deterministic model

Theorem (Rivest, Vuillemin, 1976)

If $f : \{0,1\}^N \to \{0,1\}$ is a non-constant monotone graph property or a directed graph property, we have:

$$D(f) = \Omega(N) = \Omega(n^2)$$

Theorem (Karp's/evasiveness conjecture, 1973)

If $f : \{0,1\}^N \to \{0,1\}$ is a non-constant monotone graph property, then:

$$D(f) = N = \binom{n}{2}$$

.

Scorpion Graph

Scorpion Graph

Definiton (Scorpion Graph)

A graph G is a Scorpion iff there exist three distinct special vertices $B, T, S \in V$ (Body, Tail and Sting), such that:

- *S has degree 1 and its only neighbour is T,*
- *T has degree 2 and its two neighbors are S and B,*
- *B has degree $n - 2$ (with $n = |V(G)|$).*

Scorpion Graph

Definiton (Scorpion Graph)

A graph G is a Scorpion iff there exist three distinct special vertices $B, T, S \in V$ (Body, Tail and Sting), such that:

- *S has degree 1 and its only neighbour is T,*
- *T has degree 2 and its two neighbors are S and B,*
- *B has degree $n - 2$ (with $n = |V(G)|$).*

Theorem (Sun, Xiaoming, Yao, 2004)

Forall $\epsilon > 0$, we have:

$$Q_2(f_{scorpion}) = \mathcal{O}(N^{\frac{1}{4}+\epsilon})$$

Sink

Sink

Definiton (Sink)

A directed graph G is a sink if there exists a vertex v with out-degree 0 *and in-degree n.*

Sink

Definiton (Sink)

A directed graph G is a sink if there exists a vertex v with out-degree 0 and in-degree n.

Theorem (Sun, Xiaoming, Yao, 2004)

Forall $\epsilon > 0$, we have:

$$Q_2(f_{sink}) = \mathcal{O}(N^{\frac{1}{4}+\epsilon})$$

Outline

1. Nemo
   - Quantum Lower Bounds by polynomials
2. Jérémy
   - Quantum Lower Bounds by Quantum Arguments
3. Ugo
   - Some "easy" to decide properties
   - A general lower bound for functions invariant under transitive group action

Definition (Transitivity)

A subgroup Γ of $\mathfrak{S}_N$ is said to have a transitive action on $\{1, ..., N\}$ if forall $i, j \in \{1, ...N\}$, there exists $\sigma \in \Gamma$ such that: $\sigma(i) = j$. In other words, the action of Γ on $\{1, .., N\}$ has only one orbit.

Definition (Transitivity)

A subgroup Γ of $\mathfrak{S}_N$ is said to have a transitive action on $\{1, ..., N\}$ if forall $i, j \in \{1, ...N\}$, there exists $\sigma \in \Gamma$ such that: $\sigma(i) = j$. In other words, the action of Γ on $\{1, .., N\}$ has only one orbit.

Example

Everything we saw until now: circular properties, graph properties, directed graph properties.

A general lower bound

A general lower bound

Theorem (Sun, Xiaoming, Yao, 2004)

If there exists some subgroup Γ *of* $\mathfrak{S}_N$ *acting transitively on* $\{1, ..., N\}$*such that the property* $f : \{0,1\}^N \to \{0,1\}$ *is invariant under the action of* Γ*, then :*

$$Q_2(f) = \Omega(N^{\frac{1}{4}})$$

Thank you