Razborov's lower bound on quantum communication complexity of set disjointness

Andris Ambainis
University of Latvia

Communication complexity

Alice $\underset{\longrightarrow}{\overset{\longrightarrow}{\longleftarrow}}$ Bob

x $\qquad\qquad\qquad$ y

$f(x,y)$?

Communication complexity = the number of (qu)bits that Alice and Bob need to communicate to compute $f(x,y)$.

Examples

1. Alice has $x \in \{0,1\}^n$, Bob has $y \in \{0,1\}^n$ and they have to determine if $x = y$

2. Compute $IP(x,y) = (\sum_i x_i \cdot y_i) \bmod 2$

3. $DISJ(x,y) = \bigvee_i (x_i \cdot y_i)$

   (x represents $X \subseteq \{1, \dots n\}$,
   y represents $Y \subseteq \{1, \dots n\}$,
   $DISJ(x,y) = 1$ iff $X \cap Y \neq 0$)

Variants

- Sampling: Alice and Bob start with no input and have to produce x, y so that (x,y) is distributed according to Π.

- Q-sampling: No input, have to produce
$$\sum_{x,y} \alpha_{xy} |x\rangle |y\rangle$$
with x held by Alice, y by Bob.

Complexity of set disjointness

Probabilistic:

$\Omega(n)$ bits needed [KS90, Razb92]

Quantum:

$O(\sqrt{n}\,\log n)$ qubits enough
[BCW97, HW02]

$\Omega(\sqrt{n})$ lower bound [Razb 02]

Computation vs. communication

$$\boxed{\text{Computing } f(x_1, \ldots x_n) \text{ in query model}} \qquad O(m)$$

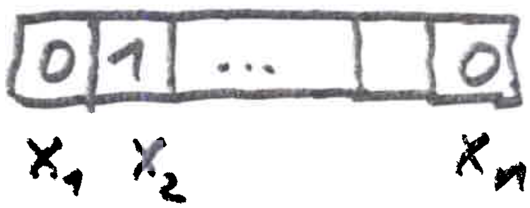
$$\Downarrow$$

$$\boxed{\text{Computing } f(x_1 \cdot y_1, x_2 \cdot y_2, \cdots, x_n \cdot y_n) \text{ in communication model}} \qquad O(m \cdot \log n)$$

- Communication lower bounds can be much more difficult.

Quantum protocol

- Grover's search:



  Can find i such that $x_i = 1$ in $O(\sqrt{n})$ quantum steps.

- Set disjointness:

  Define $x_i = 1$ if $i \in X \cap Y$.

- $O(\sqrt{n})$ steps, $O(\log n)$ qubit comm. in each of them.

Outline of Razborov's proof

- Restrict to $|X| = |Y| = \ell \approx \text{const} \cdot n$
- Communication matrix

$$(M_f)_{X,Y} = f(X,Y)$$

- Step 1:

protocol with c qubit communication

$$\Downarrow$$

P - low-rank approximation of M

$P(X,Y)$ - probability that protocol answers $f(X,Y) = 1$.

Outline

- Step 2:

  let p_i be average of $P(X, Y)$,
  $|X \cap Y| = i$.

  consider $\vec{p} = (p_0, p_1, \cdots \; p_\ell)$
  $$p_0 \geq \epsilon, \quad p_1 \leq 1-\epsilon, \quad \ldots, \quad p_\ell \leq 1-\epsilon$$

- Step 3:

  express $\vec{p} = \sum_j a_j \vec{\lambda}_j$,

  $\vec{\lambda}_j$ - eigenvalue vectors,

  $\Sigma |a_j| \leq 2^c$

- Step 4:

  show $\vec{\lambda}_j$ - polynomial of degree j,

  $\vec{\lambda}_j$ - small if $j \geq \text{const} \cdot c$

Outline

$$\vec{p} = (p_0, p_1, \cdots \quad p_\ell)$$
$$\begin{array}{cccc} & \geq & \leq & & \leq \\ & \epsilon & 1-\epsilon & & 1-\epsilon \end{array}$$

- Step 5:
  - take $\vec{p}' = \sum_{j=0}^{\text{const}\cdot c} a_j \cdot \vec{\lambda}_j$
  - $\vec{p}'$ = good approximation of $\vec{p}$.
  - $\vec{p}' = (p_0', \cdots \quad p_\ell')$,

    $p_i' = g(i)$, g - poly of degree $O(c)$
  - Any such g must have degree $\Omega(\sqrt{n})$

Low rank approximation

Lemma [Kremer, Yao] State after communicating $\leq c$ qubits is

$$|\psi\rangle = \sum_{i \in \{0,1\}^c} |A_i(X)\rangle \cdot |B_i(Y)\rangle$$

- Note $|A_i(X)\rangle \otimes |B_i(Y)\rangle$ is a state that can be created without communication.
- $\| A_i(X) \| \leq 1, \ \| B_i(Y) \| \leq 1.$

Low rank approximation

- The probability of protocol claiming $f(X,Y)=1$ is

$$\| \psi_1 \|^2 = \langle \psi_1 | \psi_1 \rangle =$$

$$= \sum_i \langle A_i(X)| \langle B_i(Y)| \cdot \sum_j |A_j(X)\rangle |B_j(Y)\rangle =$$

$$= \sum_{i,j} \langle A_i(X)|A_j(X)\rangle \cdot \langle B_i(Y)|B_j(Y)\rangle$$

- Matrix $P = \sum P_{ij}$,

$$(P_{ij})_{x,y} = \langle A_i(X)|A_j(X)\rangle \cdot \langle B_i(Y)|B_j(Y)\rangle -$$

rank 1.

- Rank of $P \le 2^{2c}$

Low rank approximation

- M - matrix of correct answers

  $$M_{X,Y} = f(X,Y)$$

- P - matrix of protocol's output probabilities

- If protocol correct,

  $$|M_{X,Y} - P_{X,Y}| \leq \epsilon, \quad \|M - P\|_\infty \leq \epsilon.$$

- $\text{Rank } P \leq 2^{2c}$

Quantities

- Define $p_i = \frac{1}{N_i} \sum_{\substack{X,Y: \\ |X \cap Y| = i}} P_{X,Y}$,

  N_i - number of $(X, Y) : |X \cap Y| = i$.

- Then:

  $p_0 \leq \epsilon$, $p_i \geq 1 - \epsilon$ for $i \geq 1$.

- We can write

  $p_i = \langle P, \mu_i \rangle$,

  $$(\mu_i)_{X,Y} = \begin{cases} \frac{1}{N_i} & \text{if } |X \cap Y| = i \\ 0 & \text{if } |X \cap Y| \neq i \end{cases}$$

Eigenspaces

	E_0	E_1	$\cdots$	E_ℓ
M_0	λ_{00}	λ_{01}	$\cdots$	$\lambda_{0\ell}$
M_1	λ_{10}	λ_{11}	$\cdots$	$\lambda_{1\ell}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
M_t	λ_{t0}	λ_{t1}	$\cdots$	$\lambda_{t\ell}$

- Matrices $M_0, \cdots M_t$ have the same eigenvectors
- Eigenvectors can be partitioned into eigenspaces $E_0, E_1, \cdots E_\ell$, $\ell = |X|$.

Eigenspaces

- $E_0, E_1, \dots E_\ell$ are common to any matrix $M_{X,Y} = g(|X \cap Y|)$

- $\dim E_0 = 1$,
  $\dim E_i = \binom{n}{i} - \binom{n}{i-1}$

- $E_0 = \{(a, a, \dots a)\}$

- F_i = linear combinations of
  $$(v_{j_1, \dots j_i})_X = \begin{cases} 1 & \text{if } \{j_1, \dots j_i\} \subseteq X \\ 0 & \text{otherwise} \end{cases}$$

- $E_i = F_i \cap (E_0 \oplus E_1 \oplus \cdots E_{i-1})^\perp$.

Using eigenspaces

	$p_0 = \langle P, \mu_0 \rangle$	$p_1 = \langle P, \mu_1 \rangle$	....	$\vec{p}$
E_0	λ_{00}	λ_{10}	....	$\vec{\lambda_0}$
E_1	λ_{01}	λ_{11}	....	$\vec{\lambda_1}$
....	....	....		
E_i	λ_{0i}	λ_{1i}	....	$\vec{\lambda_i}$

- We pick a_i so that

$$\vec{p} = \sum_i a_i \vec{\lambda_i}$$

- Note $\sum_i |a_i| \leq 2^{2c} \cdot N$

Properties of eigenvalues

<u>Claim</u> Let λ_{st} be the eigenvalue of M_s corresponding to eigenspace E_t. Then,

1. $\lambda_{st} = F_t(s)$, F_t - poly of deg. t
   (Hahn polynomial)

2. $|\lambda_{st}| \leq \frac{1}{N \cdot c^t}$

<u>Proof</u>: By writing E_t explicitly.

- We can omit $\vec{\lambda}_i$ for $i \geq \text{const} \cdot c$

- Remaining vector

$$\sum_{i=0}^{\text{const} \cdot c} a_i \vec{\lambda}_i = (g(0), g(1), \ldots \; g(t))$$

g - poly of degree $O(c)$.

Approximation

- We now have

$$\sum_{i=0}^{\text{const}\cdot\varepsilon} a_i \vec{\lambda_i} = (g(0), g(1), \dots g(t))$$

- $g(0) \leq \epsilon + \delta$

- $g(i) \geq 1 - \epsilon - \delta, \; i \in \{1, \dots t\}$.

- Polynomial g approximates

$$f(i) = \begin{cases} 0 & i = 0 \\ 1 & i \in \{1, \dots t\} \end{cases}$$

- This requires degree $\Omega(\sqrt{t}) = \Omega(\sqrt{n})$.

Approximation

- The last step is the same as in „quantum lower bounds by polynomials" [BBC+98].
- They used $g(i)$ to describe search with i marked items.
- Razborov uses $g(i)$ to describe the case when $|X \cap Y| = i$.
- Communication complexity similar to query complexity?

Conclusion

- Razborov has shown $\Omega(\sqrt{n})$ lower bound on quantum communication complexity of set disjointness, resolving 5-year old open problem.
- Bound is also true if Alice and Bob can share an entanglement.
- Bound extends to other symmetric functions. If $f(X,Y)=0$ for $|X \cap Y| = k$, $f(X,Y)=1$ for $k+1$, $\Omega(\sqrt{kn})$ lower bound.

Sampling

- Sampling:

  generate $X, Y, f(X, Y)$

  with (X, Y) uniformly distributed

  over $|X| = |Y| = \sqrt{n}$

- Q-sampling:

  generate

$$\sum |X\rangle |Y\rangle |f(X, Y)\rangle$$

Results

- Computing $DISJ(X, Y)$ takes $O(\sqrt[4]{n} \log$ qubits if $|X| = |Y| = \sqrt{n}$ [BCW 97].

- Razborov's proof gives us $\Omega(\sqrt[4]{n})$.

- Sampling / qsampling can be done with $O(\log n)$ qubits.

- Classically both tasks (sampling and computing) take $\Theta(\sqrt{n})$ bits.

- What is happening?

Sampling

- Algorithm for sampling disjoint subsets uses first $O(1)$ eigenspaces to solve problem.
- Razborov shows that even first $o(\sqrt{n})$ eigenspaces cannot solve computing problem.

Sampling

- Sampling uses ℓ_1 distance for error

$$\sum_{x,y} |p_{x,y} - p'_{x,y}|$$

(q-sampling ℓ_2 distance)

- Computing uses ℓ_∞ distance

$$\max_{x,y} |p_{x,y} - p'_{x,y}|.$$

Future work

- Query complexity has lots of results without counterparts in communication complexity. For example,

$$Q(f) \geq \sqrt[6]{D(f)}$$

for any total f.

- Is this true for communication complexity