Quantum Algorithms for Learning Symmetric Juntas via Adversary Bound

Alexander Belov
MIT

June 11, 2014
The 29th CCC, Vancouver

Introduction

Problem Formulation

Fixed: Symmetric Boolean function $h\colon \{0,1\}^k \to \{0,1\}$.

Given: Oracle access to $f_A\colon \{0,1\}^n \to \{0,1\}$ with $n \gg k$ defined by

$$f_A(x) = h(x_A)$$

for some k-subset A.

Task: Learn the function, i.e., find A.

Fixed: Symmetric Boolean function $h\colon \{0,1\}^k \to \{0,1\}$.

Given: Oracle access to $f_A\colon \{0,1\}^n \to \{0,1\}$ with $n \gg k$ defined by

$$f_A(x) = h(x_A)$$

for some k-subset A.

Task: Learn the function, i.e., find A.

- We identify $x \in \{0,1\}^n$ with the subset $S \subseteq [n]$.
- Different from usual junta learning:
  - function h is fixed,
  - no PAC learning.

Problem Formulation

Fixed: Symmetric Boolean function $h\colon \{0,1\}^k \to \{0,1\}$.

Given: Oracle access to $f_A\colon \{0,1\}^n \to \{0,1\}$ with $n \gg k$ defined by

$$f_A(x) = h(x_A)$$

for some k-subset A.

Task: Learn the function, i.e., find A.

- There are $\binom{n}{k}$ possible outcomes.
  Requires
  $\log\binom{n}{k} = \Omega\left(k \log \frac{n}{k}\right)$ randomised queries.

Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

NB: Before Shor's and Grover's algorithms!

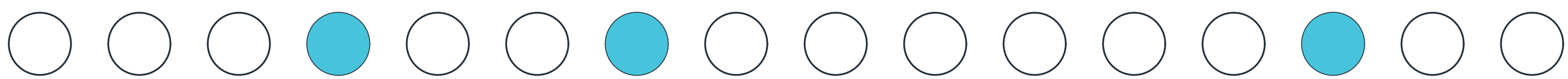
Examples

Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

(Combinatorial) Group Testing problem, Dorfman (1943)

The case of $h =$ OR.

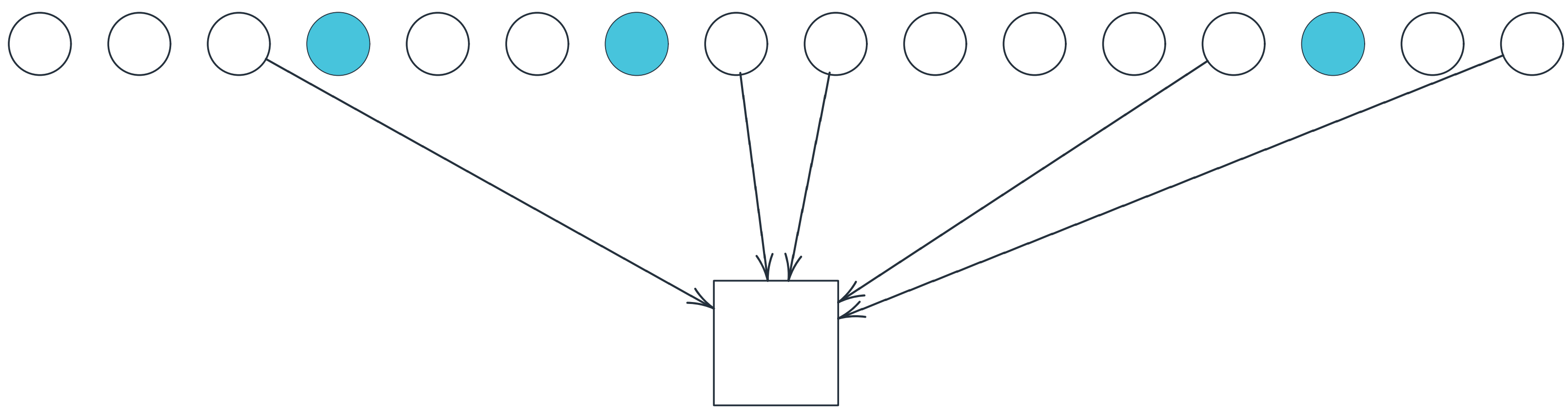


Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

(Combinatorial) Group Testing problem, Dorfman (1943)

The case of $h =$ OR.

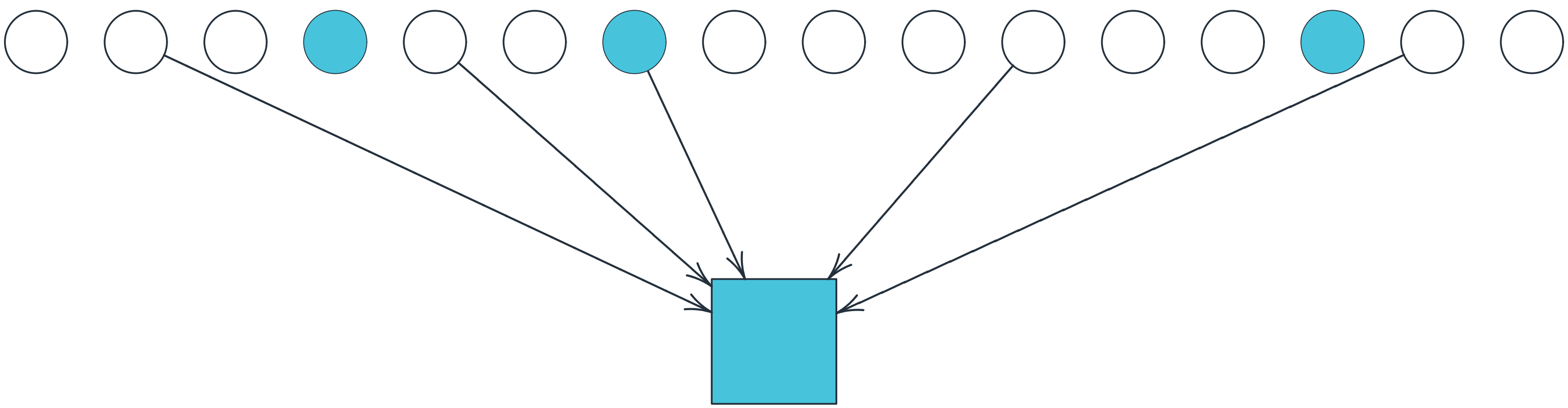


Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

(Combinatorial) Group Testing problem, Dorfman (1943)

The case of $h =$ OR.



Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

(Combinatorial) Group Testing problem, Dorfman (1943)

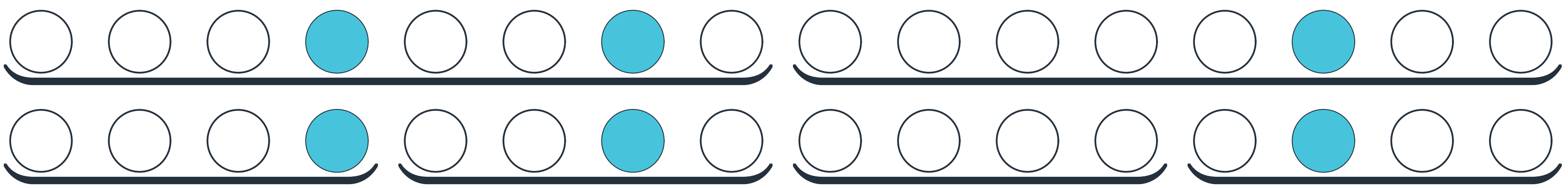
The case of $h =$ OR.

Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

(Combinatorial) Group Testing problem, Dorfman (1943)

The case of $h =$ OR.

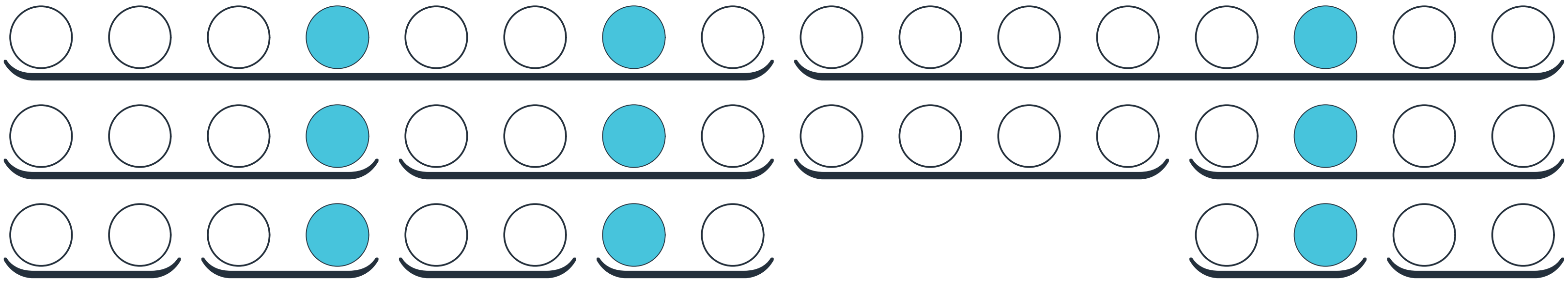


Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

(Combinatorial) Group Testing problem, Dorfman (1943)

The case of $h =$ OR.

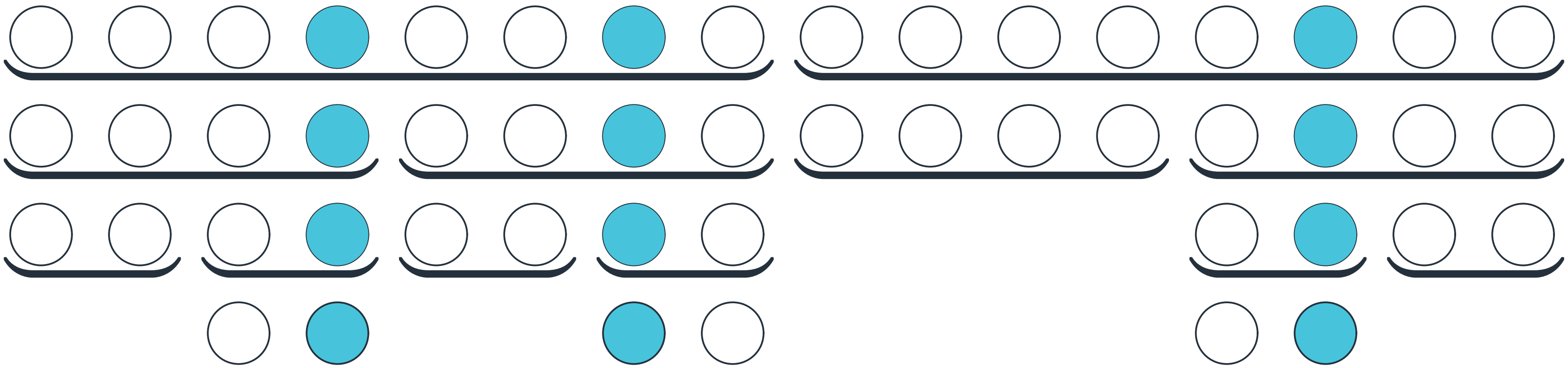


Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

(Combinatorial) Group Testing problem, Dorfman (1943)

The case of $h =$ OR.

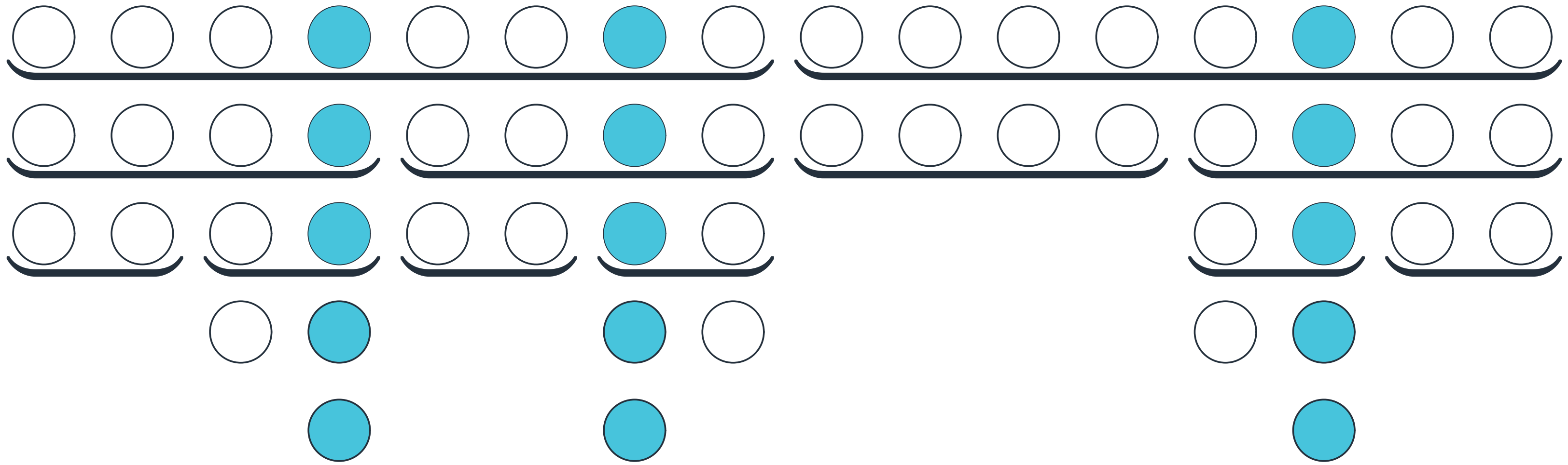


Bernstein-Vazirani problem (1993)

Solve the case of $h =$ XOR in 1 quantum query exactly.

(Combinatorial) Group Testing problem, Dorfman (1943)

The case of $h =$ OR.

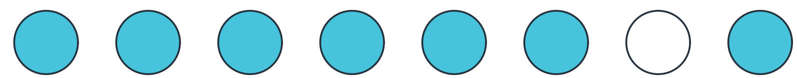


Gives $O(k \log n)$ algorithm. Can be reduced to $O\left(k \log \frac{n}{k}\right)$.

More on Group Testing

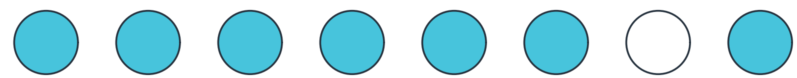
Quantum Lower Bound due to Ambainis and Montanaro (2013)

Consider the case $n = k + 1$.



Quantum Lower Bound due to Ambainis and Montanaro (2013)

Consider the case $n = k + 1$.



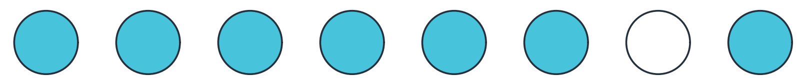
- If we query $S = \emptyset$, the answer is always 0.
- If we query S with $|S| > 1$, the answer is always 1.

Equivalent to the search for the unmarked element.
Requires $\Omega(\sqrt{k})$ quantum queries.

More on Group Testing

Quantum Lower Bound due to Ambainis and Montanaro (2013)

Consider the case $n = k + 1$.



- If we query $S = \emptyset$, the answer is always 0.
- If we query S with $|S| > 1$, the answer is always 1.

Equivalent to the search for the unmarked element.
Requires $\Omega(\sqrt{k})$ quantum queries.

Previous Quantum Upper Bound: $O(k)$.

Our Results

- We prove a tight $O(\sqrt{k})$ upper bound for group testing.
- We give an alternative formulation for a general h.
- We construct a $O(k^{1/4})$ quantum query algorithm when
  - $h =$ EXACTLY-HALF (tight);
  - $h =$ MAJORITY.

Group Testing

Adversary Bound: Ambainis (2000); Høyer *et al.* (2006); Reichardt *et al.* (2010)

Tight characterisation of quantum query complexity.
$\mathcal{C}$: the family of all k-subsets of $[n]$.

$$
\begin{array}{lll}
\text{minimise} & \displaystyle\max_{A\in\mathcal{C}} \sum_{S\subseteq[n]} X_S[\![A,A]\!] & \\
\text{subject to} & \displaystyle\sum_{S\colon f_A(S)\neq f_B(S)} X_S[\![A,B]\!] = 1 & \text{for all } A\neq B \text{ in } \mathcal{C}; \\
 & X_S \text{ is a p.s.d. } \mathcal{C}\times\mathcal{C} \text{ matrix} & \text{for all } S\subseteq[n],
\end{array}
$$

$$X_S = \left(\boxed{\Pr[S]} \right)$$

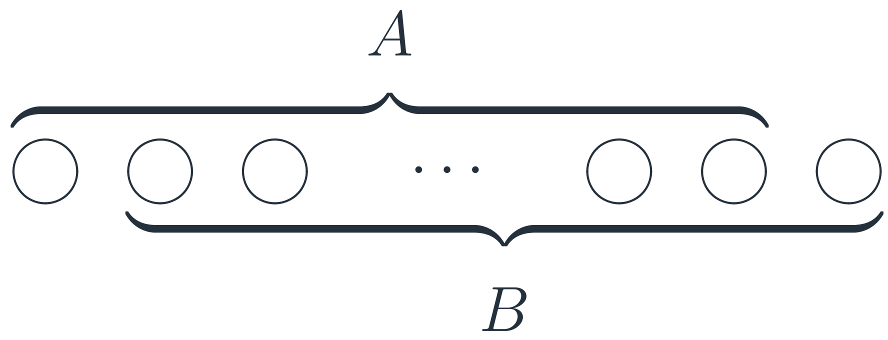
$$\Pr[S] = p^{|S|}(1-p)^{n-|S|} \qquad \text{for some } 0 < p < 1$$

- Which subsets A do we include?

We have constraint

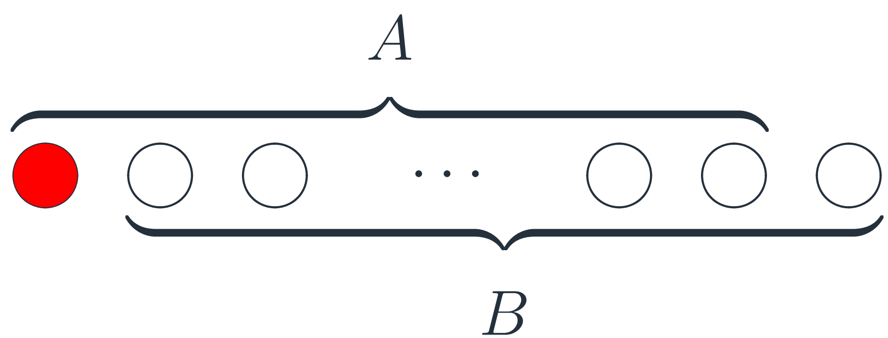
$$\sum_{S:\, f_A(S) \neq f_B(S)} X_S[\![A, B]\!] = 1.$$

"Hardest" when A and B differ in 1 element:



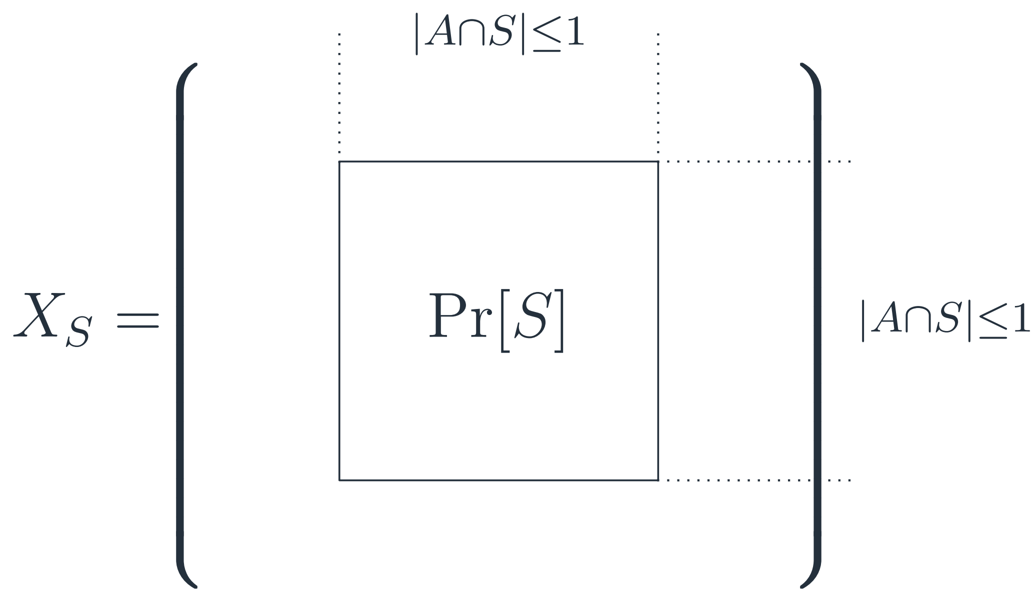
Hard Case: Constraint

$$\sum_{S:\, f_A(S)\neq f_B(S)} X_S[\![A,B]\!]$$ is the probability of $f_A(S) \neq f_B(S)$:

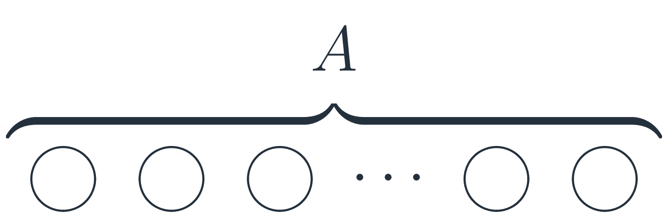


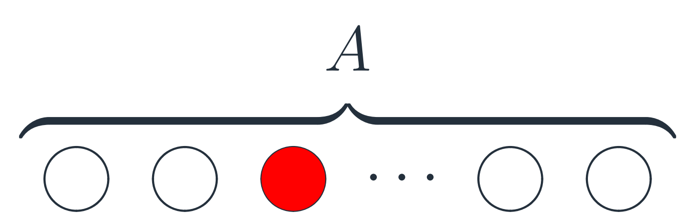
- It equals $2p(1-p)^k$.
- In X_S we include A satisfying $|A \cap S| \leq 1$.

Hard Case: Objective Value



$$
\begin{aligned}
\sum_{S \subseteq [n]} X_S[\![A, A]\!] &= \sum_{S:|S \cap A|=0} X_S[\![A, A]\!] + \sum_{S:|S \cap A|=1} X_S[\![A, A]\!] \\
&= \Pr_S[S \cap A = \emptyset] + \Pr_S[|S \cap A| = 1] \\
&= (1-p)^k + kp(1-p)^{k-1}.
\end{aligned}
$$





Hard Case: Analysis

$$X_S = \begin{array}{cc} |A\cap S|\leq 1 & \\ \left(\begin{array}{ccc} & & \\ & \boxed{\Pr[S]} & \\ & & \end{array}\right) & |A\cap S|\leq 1 \end{array}$$

Objective: $$\begin{array}{c} (1-p)^k \\ kp(1-p)^{k-1} \end{array}$$

Constraint: $$2p(1-p)^k$$

Hard Case: Analysis

$$X_S = \alpha \begin{array}{cc} \begin{array}{ccc} \qquad & |A \cap S| \le 1 & \qquad \end{array} & \\ \begin{pmatrix} \qquad & \qquad & \qquad \\ & \boxed{\Pr[S]} & \\ & & \end{pmatrix} & |A \cap S| \le 1 \end{array}$$

Objective: $\cancel{(1-p)^k}$ $\quad 1-p$

$\cancel{kp(1-p)^{k-1}}$ $\quad kp$

Constraint: $\cancel{2p(1-p)^k}$ $\quad 2p(1-p)$

Hard Case: Analysis

$$X_S = \alpha \begin{array}{cc} \begin{array}{cc} A\cap S=\emptyset & |A\cap S|=1 \end{array} & \\ \left(\begin{array}{cc} \beta\,\Pr[S] & \Pr[S] \\ \Pr[S] & \frac{\Pr[S]}{\beta} \end{array}\right) & \begin{array}{l} A\cap S=\emptyset \\ |A\cap S|=1 \end{array} \end{array}$$

Objective: $\cancel{(1-p)^k}$ $\cancel{kp(1-p)^{k-1}}$ $1-p$ kp $\sqrt{kp(1-p)}$

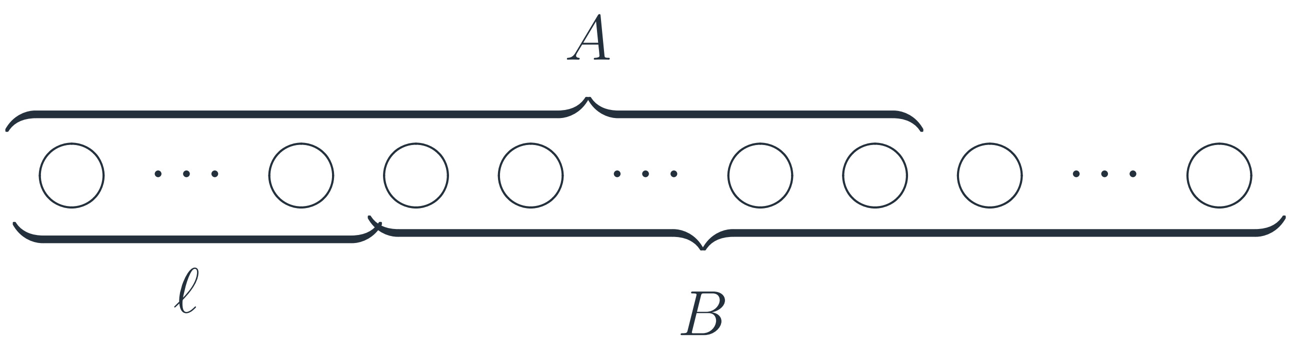
Constraint: $\cancel{2p(1-p)^k}$ $2p(1-p)$

By plugging $p = 1/2$ and rescaling, we get complexity $O(\sqrt{k})$.

General Case

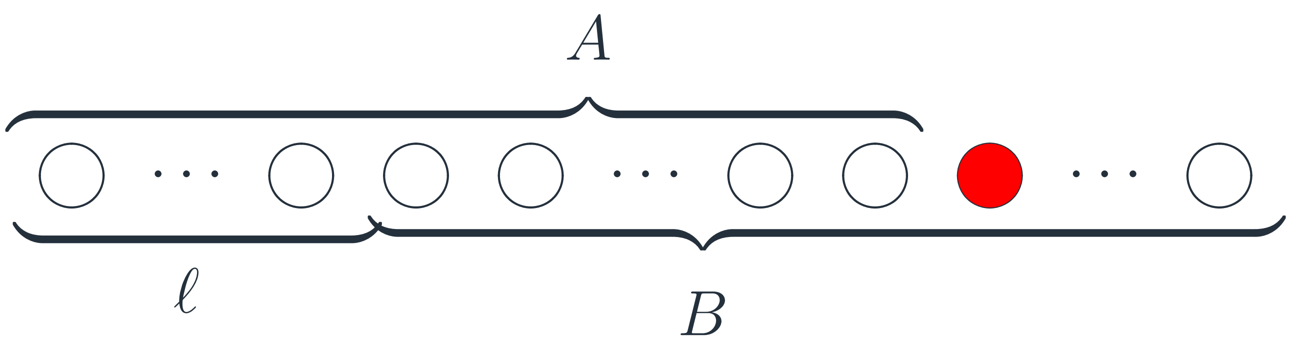
BUT!

What if A and B differ in $\ell > 1$ elements?



BUT!

What if A and B differ in $\ell > 1$ elements?



The probability is $2\ell p(1-p)^{k+\ell-1}$.

General Case: Analysis

$$X_S = \begin{array}{cc} \begin{array}{c} |A \cap S| \leq 1 \\ \left(\begin{array}{ccc} & & \\ & \boxed{\Pr[S]} & \\ & & \end{array} \right) \end{array} & |A \cap S| \leq 1 \end{array}$$

Objective: $$(1-p)^k$$ $$kp(1-p)^{k-1}$$

Constraint: $2\ell p(1-p)^{k+\ell-1}$

General Case: Analysis

$$X_S = \alpha \begin{array}{cc} \begin{array}{cc} A\cap S=\emptyset & |A\cap S|=1 \end{array} & \\ \left(\boxed{\begin{array}{c:c} \beta \Pr[S] & \Pr[S] \\ \hdashline \Pr[S] & \frac{\Pr[S]}{\beta} \end{array}} \right) & \begin{array}{c} A\cap S=\emptyset \\ |A\cap S|=1 \end{array} \end{array}$$

Objective: $\cancel{(1-p)^k}$ $\quad 1/(2p)$ $\longrightarrow \sqrt{\frac{k}{4p(1-p)}}$

$\cancel{kp(1-p)^{k-1}}$ $\quad k/(2(1-p))$ $\longrightarrow \sqrt{\frac{k}{4p(1-p)}}$

Constraint: $\cancel{2\ell p(1-p)^{k+\ell-1}}$ $\quad \ell(1-p)^{\ell-1}$

Objective: $\cancel{(1-p)^k}$ $\quad 1/(2p)$ $\rightarrow \sqrt{\frac{k}{4p(1-p)}}$

$\cancel{kp(1-p)^{k-1}}$ $\quad k/(2(1-p))$ $\rightarrow \sqrt{\frac{k}{4p(1-p)}}$

Constraint: $\cancel{2\ell p(1-p)^{k+\ell-1}}$ $\quad \ell(1-p)^{\ell-1}$

Now we integrate by p from 0 to 1:

$$X_S = \int_0^1 X_S(p)\mathrm{d}p$$

$$\frac{\sqrt{k}}{2}\int_0^1 \frac{\mathrm{d}p}{\sqrt{p(1-p)}} = \frac{\pi\sqrt{k}}{2}$$

$$\int_0^1 \ell(1-p)^{\ell-1}\mathrm{d}p = 1.$$

Other Functions

Previous analysis works because we considered two values of $|A \cap S|$ only.

Alternative scheme:

- Adversary lower bound
- Equivalent formulation via representation theory
- Semidefinite duality
- Solution of the dual problem

maximise $\max\{d_0, d_1, \ldots, d_{k-1}, d_k = 0\}$

subject to

for all integers $0 < m \leq k,\ 0 \leq t \leq k - m,$ and real $0 < p < 1$:

Orthonormal basis of $\mathbb{R}^{m+1}$ defined by normalised Krawtchouk polynomials:

$$\varkappa_\ell = \text{normalised} \left(\sqrt{\binom{m}{x} p^x (1-p)^{m-x}} \sum_{i=0}^{\ell} (-1)^i p^{\ell-i} (1-p)^i \binom{x}{i} \binom{m-x}{\ell-i} \right)_x$$

Equivalent Formulation

maximise $\max\{d_0, d_1, \ldots, d_{k-1}, d_k = 0\}$

subject to

for all integers $0 < m \leq k,\ 0 \leq t \leq k - m$, and real $0 < p < 1$:

$$\left(\sum_{i=0}^{m} d_{k-i} \varkappa_{m-i} \varkappa^*_{m-i} \right)$$

Equivalent Formulation

maximise $\max\{d_0, d_1, \ldots, d_{k-1}, d_k = 0\}$

subject to

for all integers $0 < m \leq k,\ 0 \leq t \leq k - m,$ and real $0 < p < 1$:

$h^{-1}(0){-}t$

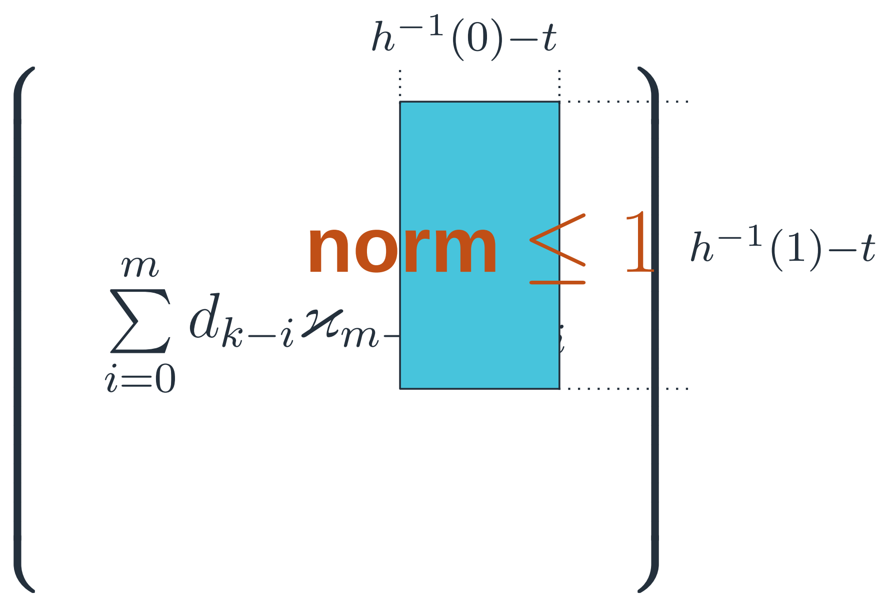
$$\left(\sum_{i=0}^{m} d_{k-i} \varkappa_{m-} \cdots \right)$$

$h^{-1}(1){-}t$

maximise $\max\{d_0, d_1, \ldots, d_{k-1}, d_k = 0\}$

subject to

for all integers $0 < m \leq k$, $0 \leq t \leq k - m$, and real $0 < p < 1$:



- From basic properties of $\varkappa_\ell$, we get a $O(k^{1/4})$ upper bound for
  - MAJORITY and EXACTLY-HALF.
- The result for EXACTLY-HALF is tight.

- Adversary bound rules!
- Optimal algorithms for OR and EXACT-HALF.
- Super-quadratic separation between randomised and quantum query complexities.

- MAJORITY ?
  - Is it more like XOR, or like OR ?
  - We know that:
    - Bernstein-Vazirani style approach fails,
    - simple lower bounds fails.

- Other functions: t-THRESHOLD, EXACTLY-t ?

- Further applications of these results and techniques ?

Thank you!