Quantum PRP/PRF Switching Lemma via Adversary Method

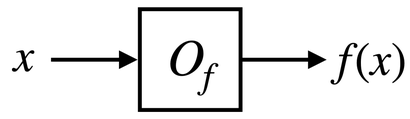
Towards Tight Bounds for 3-Collision

Ansis Rosmanis

Graduate School of Mathematics, Nagoya University

k-Collision problem

Given an oracle access to $f\colon \{1,\dots,n\} \to \{1,\dots,n\}$,



decide if there are k distinct $x_1, x_2, \dots, x_k$ such that $f(x_1) = f(x_2) = \ldots = f(x_k)$.

Query complexity

$$k = 2 : \Theta(n^{2/3}),$$
$$k = 3 : \Omega(n^{2/3}),\ \mathrm{O}(n^{5/7}),$$
$$k = 4 : \Omega(n^{11/16}),\ \mathrm{O}(n^{11/15}).$$

Importance

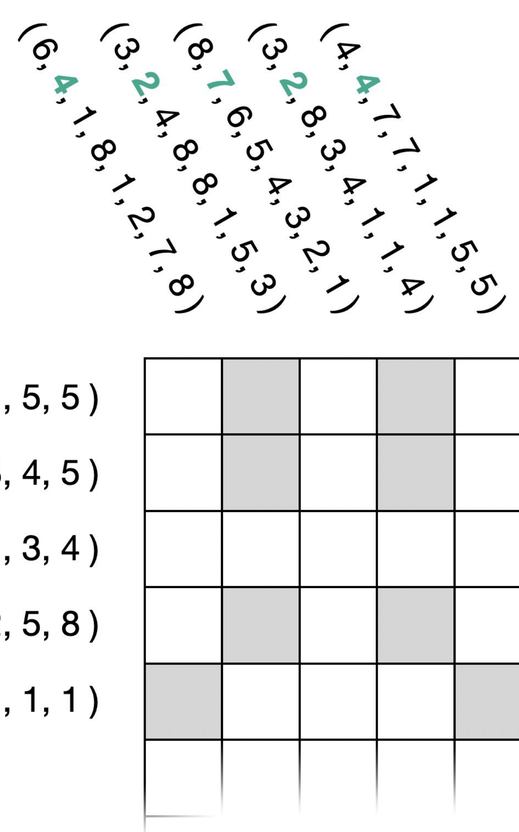
- New algorithmic techniques,
- New lower bound techniques,
- Cryptographic applications.

Quantum adversary method

For a decision problem P, one has to decide if $f \in \mathit{Yes}_\mathsf{P}$ or $f \in \mathit{No}_\mathsf{P}$.

$$f = (f(1), f(2), \dots, f(n))$$

Γ – any non-zero $\mathit{Yes}_\mathsf{P} \times \mathit{No}_\mathsf{P}$ matrix.



For every input $x \in \{1,\dots,n\}$,

$$\Gamma^{(x)}_{f,g} := \begin{cases} \Gamma_{f,g} & \text{if} \quad f(x) \neq g(x), \\ 0 & \text{if} \quad f(x) = g(x). \end{cases}$$

Adversary bound

Bounded-error quantum query complexity

$$Q_\epsilon(\mathsf{P}) = \Omega\Big(\|\Gamma\| \big/ \max_x \|\Gamma^{(x)}\| \Big) .$$

Challenges

1. Choosing a good Γ,
2. Evaluating the norms.

Hardest instances for 3-Collision

$\mathit{No}_{3\mathsf{C}}$: $\mathrm{im}_{\mathrm{mult}} f$ contains $n/2$ pairs;

$\mathit{Yes}_{3\mathsf{C}}$: $\mathrm{im}_{\mathrm{mult}} f$ contains $n/2 - 2$ pairs and a quadruple.

The structure makes constructing lower bounds for the $k = 3$ case more difficult than for the $k = 2$ case.

Assignment vectors

Assignment : partial function $\alpha\colon \{1,\dots,n\} \to \{1,\dots,n\}$.

Compatibility : f agrees with α if $\alpha(x) = f(x)$ for all $x \in \mathrm{dom}\,\alpha$.

For every Yes-certificate α:

$$|w_\alpha\rangle \overset{unit}{:=} \sum_{\substack{f \in \mathit{Yes} \\ \alpha \subset f}} |f\rangle \qquad \text{and} \qquad |v_\alpha\rangle \overset{unit}{:=} \sum_{\substack{f \in \mathit{No} \\ \alpha \subset f}} |f\rangle.$$

We interpret the state of the adversary being in $|w_\alpha\rangle$ or $|v_\alpha\rangle$ as the algorithm having learnt that f agrees with α.

This is reminiscent of dual learning graphs.

Candidate adversary matrix

Inspired by lower bounds for dual adaptive learning graphs, I propose constructing the adversary matrix Γ as a linear combination of

$$L_{i,o} := \Bigg(\sum_{\substack{\alpha \\ |\mathrm{dom}\,\alpha| = i \\ |\mathrm{im}\,\alpha| = o}} |w_\alpha\rangle\langle v_\alpha| \Bigg) \Pi_{i,o}$$

where $\Pi_{i,o}$ is a certain projector related to the symmetries of the problem:

$$\Gamma := \sum\nolimits_{i,o} (n^{5/7} - i - n^{1/7}(i - o)) L_{i,o}.$$