

QII Exercise sheet 8

Quantum Fingerprinting

We consider a different scenario here where Alice and Bob have respectively a string $x \in \{0, 1\}^n$ and $y \in \{0, 1\}^n$. They each send a message to a referee R that has to determine whether $x = y$ or not. Alice and Bob *do not have shared randomness*.

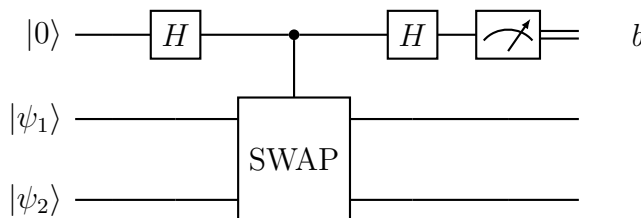
Alice, Bob and the referee cooperate and they win iff. R outputs “0” if $x = y$ and “1” if $x \neq y$.

Assume the referee has a procedure that given any 2 states $|\psi_1\rangle, |\psi_2\rangle$ outputs “0” wp $\frac{1}{2} + \frac{|\langle\psi_1|\psi_2\rangle|^2}{2}$.

Exercise 1. Using states of the form $|\psi_x\rangle = \frac{1}{\sqrt{n}} \sum_i |i\rangle |x_i\rangle$, give a procedure where Alice and Bob send states of size $\lceil \log_2(n) \rceil + 1$ and where the referee always succeeds when $x = y$ and succeeds wp. $\frac{1}{2} - \frac{\delta^2}{2}$ where $\delta = \frac{1}{n} |\{i : x_i = y_i\}|$.

Exercise 2. We assume there exists a function $E : \{0, 1\}^n \rightarrow \{0, 1\}^m$ with $m = 2n$ st. $\forall x, y \neq x \in \{0, 1\}^n, |\{i \in [m] : E(x)_i = E(y)_i\}| \leq \frac{28m}{30}$ (Such a function can be constructed using an error-correcting code). Show how to use this function in order to win the game with constant probability non zero when $x \neq y$, by sending $O(\log(n))$ qubits to the referee.

Exercise 3. For 2 states $|\psi_1\rangle, |\psi_2\rangle$, we consider the circuit



where the second gate is a control-SWAP defined as

$$C - \text{SWAP} |0\rangle |x\rangle |y\rangle = |0\rangle |x\rangle |y\rangle ; C - \text{SWAP} |1\rangle |x\rangle |y\rangle = |1\rangle |y\rangle |x\rangle .$$

for any $x, y \in \{0, 1\}$. Show that this circuit performs the procedure of the referee that outputs 0 wp. $\frac{1}{2} + \frac{|\langle\psi_1|\psi_2\rangle|^2}{2}$.

Hidden Matching Problem

Alice has a random string $x = (x_1, \dots, x_n)$ unknown to Bob with n even. Bob has a matching M which is a list of $\frac{n}{2}$ disjoint pairs (i, j) for $i, j \neq i \in \{1, \dots, n\}$. For example for $n = 6$, the list $((1, 4), (2, 3), (5, 6))$ is a possible matching. For $n = 10$, the lists $((1, 7), (2, 9), (3, 4), (5, 10), (6, 8))$ and $((1, 4), (2, 10), (3, 5), (6, 9), (7, 8))$ are two possible matchings.

Alice and Bob cooperate and we are in the one-way communication model where Alice is allowed to send a single message to Bob. Bob outputs a triplet (i, j, b) . They win iff. $(i, j) \in M$ and $x_i \oplus x_j = b$.

Exercise 4. We consider the following quantum protocol for this problem

- Alice creates the state $|\psi_x\rangle = \frac{1}{\sqrt{n}} \sum_{l=1}^n (-1)^{x_l} |l\rangle$ and sends it to Bob.
- Bob has a matching $M = ((i_1, j_1), \dots, (i_{n/2}, j_{n/2}))$. Let $\Pi = \{\Pi_i\}_{i \in \{1, \dots, n/2\}}$ be a projective measurement with $\Pi_k = |i_k\rangle\langle i_k| + |j_k\rangle\langle j_k|$. Bob measures using this measurement. He uses the resulting outcome to output a triplet (i, j, b) in a way you will show in one of the questions.

1. What is the size of $|\psi_x\rangle$?
2. Show that Π is a valid quantum measurement.
3. For each $k \in \{1, \dots, n/2\}$, what is the probability that Bob outputs “ k ”?
4. Assume Bob gets outcome k , what is the remaining state $|\psi_x^k\rangle$ after the measurement?
5. Show how Bob can output (i, j, b) from his outcome “ k ” and the state $|\psi_x^k\rangle$.

Exercise 5. Show a randomized strategy where Alice sends a message of size $\tilde{O}(\sqrt{n})$ that succeeds w.p. at least $\frac{2}{3}$. Think of the birthday’s paradox.

This is actually optimal for classical one-way communication so it shows an exponential separation between classical and quantum one-way communication complexity. See [GKK⁺06] for more details.

References

- [GKK⁺06] Dmytro Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. *arXiv*, <https://arxiv.org/abs/quant-ph/0611209>, 2006.