

Answers to Quantum Information exercise 7, 8 and 9.

Exercise 7: Quantum key distribution

- a) If Alice and Bob share N entangled qubits in the state $|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle$, then their measurements are completely correlated, so they obtain the identical string of N random bits. No information is contained in this string, as required by the impossibility to transmit information faster than the speed of light.
- b) Bob only measures the qubits he receives after Alice has told him which went through the Hadamard gate, and for those he only measures after having passed them again through a Hadamard gate, thereby undoing the operation (H^2 is the identity).
- c) Eve does not know which qubits went through the Hadamard gate when she intercepts the qubits, since that information only comes available once Bob has received them. Eve might measure the qubits and then pass them on to Bob, but then Bob will find measurement outcomes that differ from those prepared by Alice. They can find out the qubits were intercepted by comparing part of their random key, if there is a disagreement they will know that the key has been compromised and have to try again.
- d) The inner products are conserved, so $\langle\phi_\nu|\phi_\mu\rangle = \langle\phi_\nu|\phi_\mu\rangle\langle\Phi_\nu|\Phi_\mu\rangle$. Take the nonzero inner products for $\nu, \mu = 1, 3$ or $1, 4$ or $2, 3$ or $2, 4$ to find $\langle\Phi_\nu|\Phi_\mu\rangle = 1$ for these combinations of ν, μ , hence $\Phi_1 = \Phi_3 = \Phi_4$ and $\Phi_2 = \Phi_3 = \Phi_4$. The conclusion is that all four Φ_ν 's are identical.

Exercise 8: Quantum algorithms

- a) at most $2^{N-1} + 1$ evaluations are needed, if the first 2^{N-1} evaluations all give the same output it could still be either class C or class B, but then the next evaluation will distinguish the two classes (class C if it is still the same, class B if it is different).
- b) after the Hadamard gate, each qubit $|0\rangle \mapsto 2^{-1/2}(|0\rangle + |1\rangle)$, so the output of the N qubits is a string of N binary digits, which encode the integer $x \in \{0, 1, 2, \dots, 2^N - 1\}$ in binary notation.
- c) The operation $|x\rangle \mapsto |f(x)\rangle$ is not reversible, you cannot deduce the input from the output, hence it cannot be a unitary operation, which is reversible by definition.
- d) The operation is linear and conserves the norm, hence unitary.
- e) If the function $f(x)$ is constant, the state entering and exiting the black box is the

same up to a phase factor, so the Hadamard gate acts twice on the same state, and since H^2 is the identity we recover the initial state with all qubits equal to $|0\rangle$.

f) The Hadamard gate H acting on each of the N qubits encoded in the binary string $x = x_1 x_2 \dots x_N$ produces the output

$$|x\rangle \mapsto 2^{-N/2} \sum_{y=0}^{2^N-1} (-1)^{x \odot y} |y\rangle,$$

with $x \odot y = \sum_i x_i y_i$ (bitwise multiplication). So the zero output, with all $y_i = 0$, appears with weight $2^{-N} \sum_x (-1)^{f(x)}$ which equals zero if $f(x)$ equals 0 and 1 equally often.

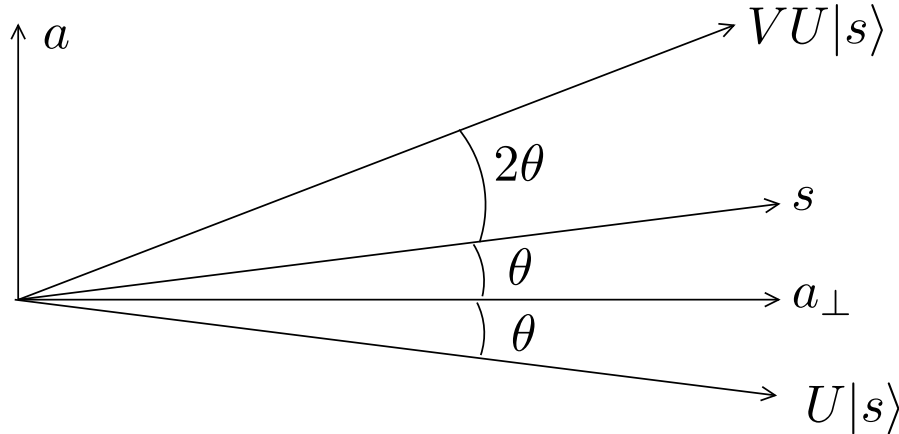
g) Adding the same binary twice does not change the parity.

h) If you measure $f(x_0)$ in the ancilla register, the first register must be in the superposition $|x_0\rangle + |x_0 \oplus a\rangle$.

i) A Hadamard acting on each of the N qubits in the first register maps

$$|x_0\rangle + |x_0 \oplus a\rangle \mapsto \sum_{x_1} [(-1)^{x_0 \odot x_1} + (-1)^{(x_0 \oplus a) \odot x_1}] |x_1\rangle.$$

The term in square brackets vanishes if $a \odot x_1 = 1$, so only terms in the sum with $a \odot x_1 = 0$ remain.



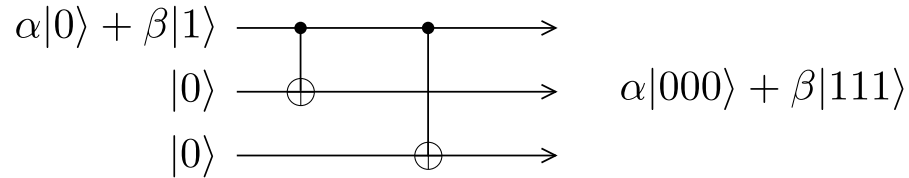
j) The vector $|a_\perp\rangle$ makes an angle $\theta = \arcsin \mathcal{N}^{-1/2} \approx \mathcal{N}^{-1/2}$ with the vector $|s\rangle$; The unitary U reflects a state in the line $|a_\perp\rangle$, while V reflects it in the line $|s\rangle$; the combined effect is that a state is rotated over an angle $2\theta = 2\mathcal{N}^{-1/2}$.

k) the two vectors $|s\rangle$ and $|a\rangle$ are nearly orthogonal for $\mathcal{N} \gg 1$, so the final state $|a\rangle$ is reached from $|s\rangle$ after T iterations when $T\theta \approx \pi/2$, hence $T \approx \frac{1}{4}\pi\sqrt{\mathcal{N}}$.

Exercise 9: Quantum error correction

a) If one bit differs from the other two, that bit has been flipped.

b) two CNOT gates:



c) the encoded state is an eigenstate of S_1 and of S_2 , and it remains an eigenstate if one of the qubits has flipped, so it is not affected by a measurement of S_1 and S_2 ; if the measurement outcome is 1, 1 then no error has happened, if the outcome is $-1, -1$ then the second qubit has flipped, if the outcome is $-1, 1$ the first qubit has flipped, and if the outcome is 1, -1 the third qubit has flipped.

d) Application of the Hadamard gate to the qubits is a change of basis; in the new basis $\sigma_x \mapsto H\sigma_x H^\dagger = \sigma_z$ and $\sigma_z \mapsto \sigma_x$, so we should measure $S_1 = \sigma_x \otimes \sigma_x \otimes 1$ and $S_2 = 1 \otimes \sigma_x \otimes \sigma_x$ to correct for σ_z errors on one qubit.