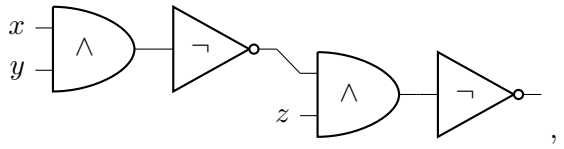
Solutions to Exercise Set 4

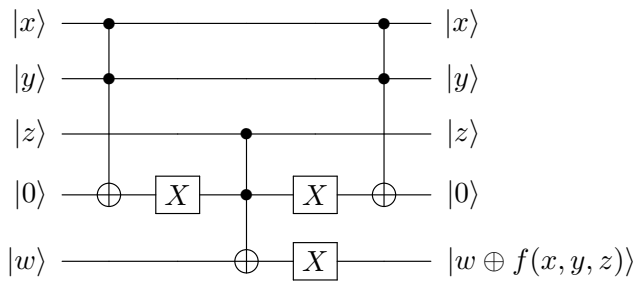
Solution 4.1 First of all, we note that this is not an instantiation of Theorem 4.5, since neither $U_\vee$ nor $U_\neg = \mathit{CNOT}$ are available as quantum gates. On the positive side, $U_\wedge$ is precisely the Toffoli gate, and the Pauli X gate can well be understood as a quantum variant of $\neg$. Finally, $\vee$ can be computed by means of $\wedge$ and $\neg$; indeed, we have that $a \vee b = \neg(\neg a \wedge \neg b)$. Thus, by means of the latter, we see that the circuit



consisting of $\wedge$ and $\neg$ gates only, computes the same function f, i.e.,

$$(x \wedge y) \vee \neg z = \neg\big(\neg(x \wedge y) \wedge z\big)\,.$$

Written like this, it is straightforward to verify that U_f is computed by means of the following quantum circuit, using Toffoli and Pauli X gates, and one "work qubit":



Solution 4.2 We follow the analysis of Simon's algorithm from the lecture notes. In the more general case here, we obtain that after the measurement of the second register (which is done for the purpose of the analysis only), the state of the first register collapses to

$$\frac{1}{2^{d/2}} \sum_{v \in V} |x \oplus v\rangle\,,$$

where d is the dimenstion of V, so that $|V| = 2^d$. Applying $H^{\otimes n}$ maps this into

$$\frac{1}{2^{d/2}} \frac{1}{2^{n/2}} \sum_{v \in V} \sum_{y} (-1)^{(x \oplus v) \cdot y} |y\rangle = \frac{1}{2^{d/2+n/2}} \sum_{y} (-1)^{x \cdot y} \sum_{v \in V} (-1)^{v \cdot y} |y\rangle\,.$$

Thus, the probability to observe y after measuring is

$$p_y = \frac{1}{2^{d+n}} \left| \sum_{v \in V} (-1)^{v \cdot y} \right|^2 = \begin{cases} 2^{d-n} & \text{if } y \in V^\perp \\ 0 & \text{else}\,. \end{cases}$$

The latter follows from the fact that if $y \notin V^\perp$, and thus there exists $v_\circ \in V$ with $v_\circ \cdot y = 1$, then $V \to V$, $v \mapsto v \oplus v_\circ$ induces a bijection between $\{v \in V \mid v \cdot y = 0\}$ and $\{v \in V \mid v \cdot y = 1\}$. The measurement outcome is thus a uniformly random $y \in V^\perp$.

Repeating, say, $n + k$ times thus results in $n + k$ uniformly random and independent vectors in $V^\perp$, and so, by Lemma 3.12, they span all of $V^\perp$ except with probability 2^{-k}. Thus, a basis of V can then be (efficiently) computed.

Solution 4.4 Using the notation from the lecture notes, for $M = 2^n/4$ we obtain that $|\psi\rangle = |\psi_{\theta_\circ}\rangle = \cos(\theta_\circ)\,|\beta\rangle + \sin(\theta_\circ)\,|\gamma\rangle$ with $\theta_\circ \in [0, \frac{\pi}{2}]$ such that $\sin(\theta_\circ) = \sqrt{M/N} = \frac{1}{2}$. It turns out that this means that $\theta_\circ = \frac{\pi}{6}$ (i.e. 30°); indeed, due to $\sin(\theta_\circ) = \frac{1}{2}$, the two vectors $|\psi_{\theta_\circ}\rangle$ and $|\beta\rangle = |\psi_0\rangle$ form *half* of an equilateral triangle, and so $\theta_\circ$ is half the angle in an equilateral triangle, which is $\frac{\pi}{3}$ (i.e. 60°). But then, just after one Grover iteration, we obtain the state $|\psi_{3\theta_\circ}\rangle = |\psi_{\frac{\pi}{2}}\rangle = |\gamma\rangle$. Thus, measuring this state produces an x that satisfies $f(x) = 1$ with certainly (by choice of $|\gamma\rangle$).

Solution 4.5 We can follow very closely the analysis of the original algorithm, except that now we consider the state $|\psi\rangle = A|0\rangle$, but still have that $P' := APA^\dagger = A(2|0\rangle\langle 0| - \mathbb{I})A^\dagger = 2|\psi\rangle\langle\psi| - \mathbb{I}$. Furthermore, we now set

$$|\gamma\rangle = \frac{1}{\sqrt{p}} \sum_{\substack{x \text{ s.t.} \\ f(x)=1}} \alpha_x |x\rangle \qquad \text{and} \qquad |\beta\rangle = \frac{1}{\sqrt{1-p}} \sum_{\substack{x \text{ s.t.} \\ f(x)=0}} \alpha_x |x\rangle\,,$$

and then write

$$|\psi\rangle = \sqrt{1-p}\,|\beta\rangle + \sqrt{p}\,|\gamma\rangle = \cos(\theta_\circ)\,|\beta\rangle + \sin(\theta_\circ)\,|\gamma\rangle =: |\psi_{\theta_\circ}\rangle\,,$$

but where now $\theta_\circ \in [0, \frac{\pi}{2}]$ is such that $\sin(\theta_\circ) = \sqrt{p}$, rather than $\sqrt{M/2^n}$. The rest of the analysis carries over verbatim. In particular, P' still acts as a reflection across the axis spanned by $|\psi\rangle$, and so G still acts as a rotation by angle $2\theta_\circ$ — but now for this larger value of $\theta_\circ$. Thus, the query complexity now becomes $\ell = O(1/\theta_\circ) \leq O(1/\sin(\theta_\circ)) = O\big(1/\sqrt{p}\big)$, and the probability of observing x with $f(x) = 1$ is still at least $1 - \sin(\theta_\circ)^2 = 1 - p$. Thus, given that $p \geq M/2^n$, we have an improvement in the complexity of the algorithm; on the other hand, the success probably is smaller, but the interesting case is of course when p is still very small, and thus this can be neglected.