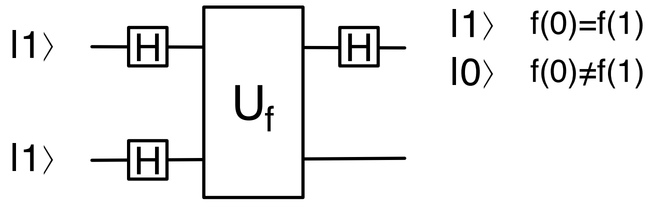
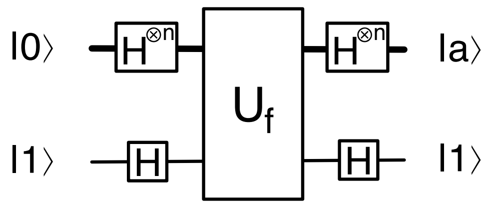
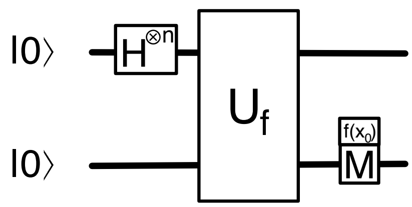
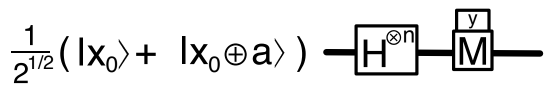


Deutsch (p.44), factor of 2 speedup to determine whether or not 1bit→1bit function $f(x)$ is constant

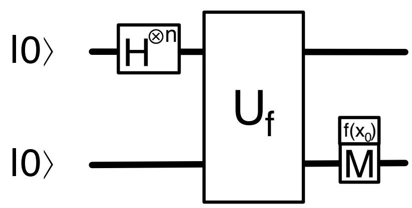


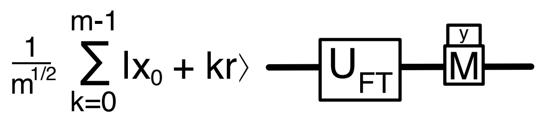
Bernstein–Vazirani (p.52), $f(x) = a \cdot x \equiv \oplus_i a_i x_i$, factor of n speedup to determine a





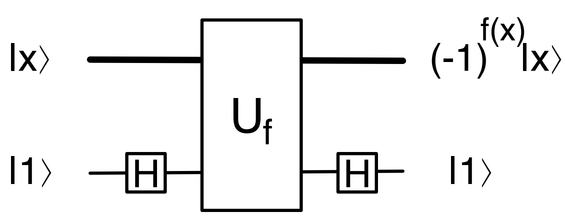
Simon (p.56), $f(x) = f(x \oplus a)$, measured y has $a \cdot y = 0$ (equivalently $\sum_i a_i y_i = 0$ mod2), exponential speedup ($2^{n/2} \to O(n)$) to determine a

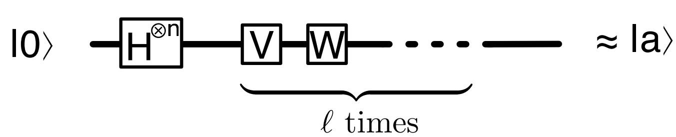




Shor (p.70), $f(x) = f(x + r)$, resulting y is measured with probability $p(y) = \frac{1}{2^n m}\left|\sum_{k=0}^{m-1} \mathrm{e}^{2\pi i k r y/2^n}\right|^2$, gives $|y - 2^n/r| < 1/2$ with $p > .4$, sufficient to determine period r via partial fraction expansion, exponential speedup $(n2^n, \exp(n^{1/3}) \to O(n^3)\ )$. (Note: replaces $\mathbf{H}^{\otimes n}|x\rangle = \frac{1}{2^{n/2}}\sum_{0\le y<2^n} \mathrm{e}^{i\pi x\cdot y}|y\rangle$ with $\mathbf{U}_{\mathrm{FT}}|x\rangle = \frac{1}{2^{n/2}}\sum_{0\le y<2^n} \mathrm{e}^{2\pi i x y/2^n}|y\rangle$.)

Practical application is $f(x) \equiv b^x \,\mathrm{mod} N$, where $b \equiv a^c \,\mathrm{mod} N$ is an encrypted message, from which d', satisfying $cd' \equiv 1 \,\mathrm{mod} r$, can be calculated, and d' recovers unencrypted message $a \equiv b^{d'} \,\mathrm{mod} N$ (in contrast to using d, with $cd = 1 \,\mathrm{mod}(p-1)(q-1)$, where $N = pq$ and r divides $(p-1)(q-1) = |G_{pq}|$).





Grover (p.90), $f(x) = 1$ only for (m) marked value(s) $x = a$, uses "phase kickback" to express $\mathbf{U}_f$ in terms of $\mathbf{V} = \mathbf{1} - 2|a\rangle\langle a|$, and $\mathbf{W} = 2|\phi\rangle\langle\phi| - \mathbf{1} = \mathbf{H}^{\otimes n}\big(2|0\rangle\langle 0| - \mathbf{1}\big)\mathbf{H}^{\otimes n}$ is easily constructed. Applying $\ell \approx \frac{\pi}{4}\frac{2^{n/2}}{\sqrt{m}}$ times gives probability $p(a) \approx 1 - O(m/2^n)$, for square-root speedup $(2^n/m \to \sqrt{2^n/m}\ )$.

P. Ginsparg, Physics 4481-7681; CS 4812 (Fall 2014)