Amplitude Amplification

: Suppose we have
- an algorithm A for a function $g(x)$
- with probability $\Pr[A(x) = g(x)] \geq p \; \forall x$
- a checking procedure $f(x,y) = \begin{cases} 1 & \text{if } y = g(x) \\ 0 & \text{otherwise} \end{cases}$

Classical: repeat $O(1/p)$ times.

Create a state $|\psi\rangle = A|x\rangle|0\ldots0\rangle$

$$|\psi'\rangle = \sqrt{p}\,|x\rangle|g(x)\rangle|\psi^{good}_{ws}\rangle + \sqrt{1-p}\,|x\rangle \sum_{y \neq g(x)} |y\rangle|\psi^{y}_{ws}\rangle$$

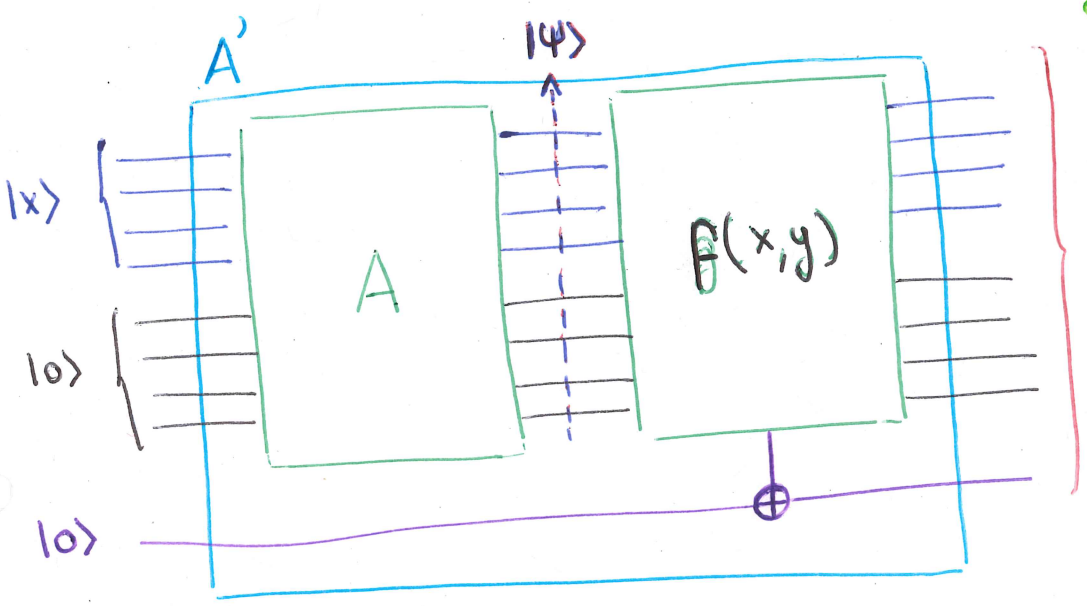
$|\psi\,good\rangle$ (check bit) $\qquad$ $|\psi\,bad\rangle$ (check bit)

$f(x,y)$

$$O_f|x\rangle|y\rangle|0\rangle \longrightarrow \begin{cases} |x\rangle|y\rangle|1\rangle & \text{if } g(x) = y \\ |x\rangle|y\rangle|0\rangle & \text{otherwise} \end{cases}$$

phase kick-back : $U_f|x\rangle|y\rangle \longrightarrow (-1)^{f(x,y)}|x\rangle|y\rangle$

U_f acts as $I - 2|\psi_{good}\rangle\langle\psi_{good}|$ on span $\{|\psi_{good}\rangle, |\psi_{bad}\rangle\}$



$$|\psi'\rangle = \sqrt{p}\,|\psi_{good}\rangle|1\rangle + \sqrt{1-p}\,|\psi_{bad}\rangle|0\rangle$$

$$U_0 = 2|\psi'\rangle\langle\psi'| - I = A'\left[2|x\bar{0}\rangle\langle x\bar{0}| - I\right]A'^{\dagger}$$

Amplitude Amplification $\Rightarrow (U_0 U_f)^T A'|x\rangle|\bar{0}\rangle$

$\approx |\psi\,good\rangle|1\rangle$ for $T = O\left(\frac{1}{\sqrt{p}}\right)$

QUADRATIC SPEED UP (see Grover's algorithm)