CSE596 Lecture Wed 12/4 Fall 2019

Reversible Functions: Given $f_n : \{0,1\}^n \to \{0,1\}^n$ define $F_f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ by

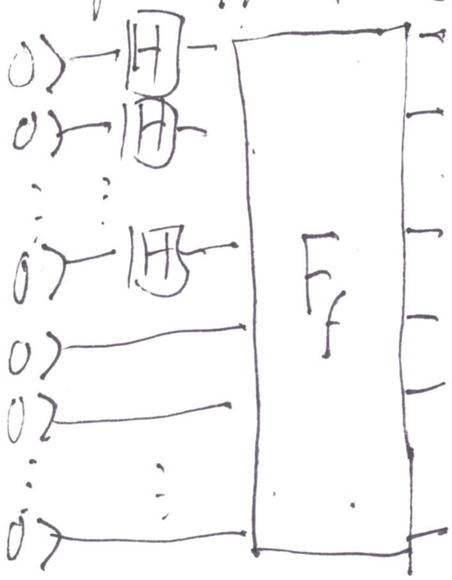
$F_f(x \cdot y) = (x \cdot (y \oplus f(x)))$ ($\oplus$ = bitwise XOR)

$F_f(x, 0^n) = x f(x)$

Even if f is not 1-1, F_f is always 1-1.

Further usage: Define $H^{\otimes n} = \underbrace{H \otimes \cdots \otimes H}_{n \text{ times}} = \frac{1}{\sqrt{2^n}} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & & & & \\ 1 & & & & & \\ \vdots & & & & & \\ 1 & & & & & \end{bmatrix}$

Also put $H' = H^{\otimes n} \otimes I^{\otimes n}$ on $2n$ qubits. Then:



gives $F_f \circ H' \cdot e_{0^{2n}}$ [where $H' e_{0^{2n}} = (1^n\ 0\ \cdots\ 0)$ column]

$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} e_x \otimes e_{f(x)} = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$ — functional superposition

The nub of the assertion that universal QC is feasible is that for $[f_n] \in P$, sufficiently close approximations to $F_f \circ H' |x\, 0^n\rangle$ are feasible to construct. Needed for Shor's Algorithm in particular.

We will explore some cases for $n = 1$ or 2 where we may start with $H^{\otimes 2n}$ also.

Deutsch's Problem: ($n=1$) How many evaluations of a given $f : \{0,1\} \to \{0,1\}$ do we need to tell apart the cases f = always 0, f = always 1 from $f(x) = x$, $f(x) = \neg x$?

Classically, we need to evaluate f on both args to tell. Quantumly, evaluating F_f once on $H^{\otimes 2}|00\rangle$ is enough.

What are the four F_f fns?

$f = 0$: $z = y \oplus 0 = y$

$F_0(x, y) = (x, y)$ $\therefore F_0 = I^{\otimes 2}$

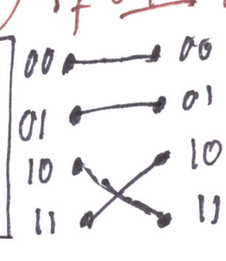
$f = 1$:

$F_0(x, y) = (x, y \oplus 1) = I \otimes X$

$f = id$: CNOT: (34)

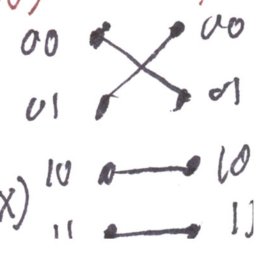
$F_0(x, y) = (x, y \oplus x)$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

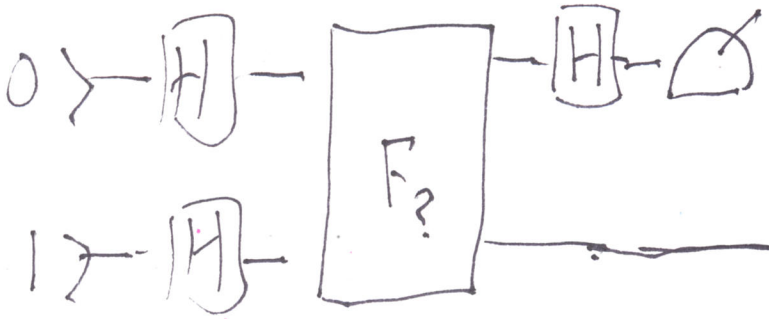


$f = \neg x$

$F_0(x, y) = (x, y \oplus \neg x)$



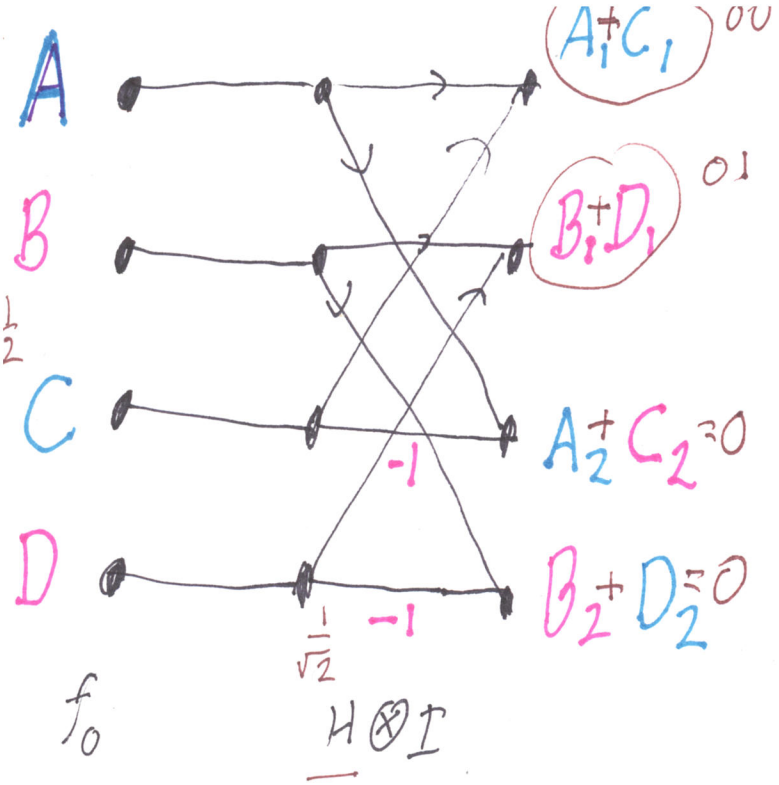
Circuit and Setup for Deutsch's Algorithm



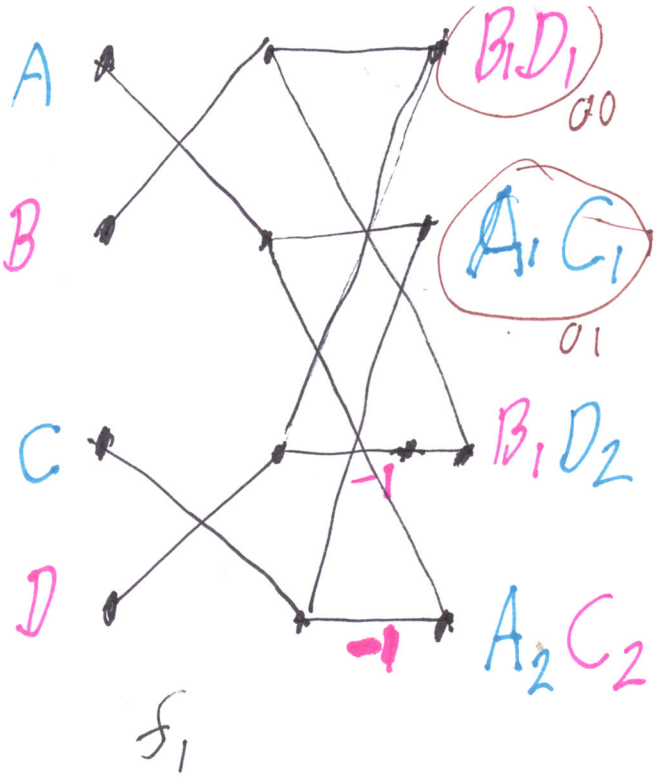
$$\frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}$$

$$H \otimes H = \frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}$$

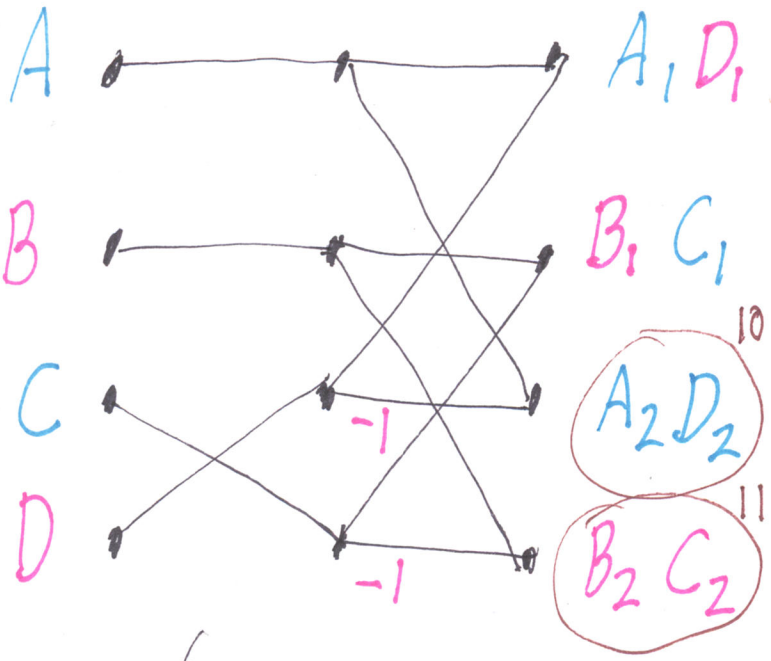
input 01, so we get this column



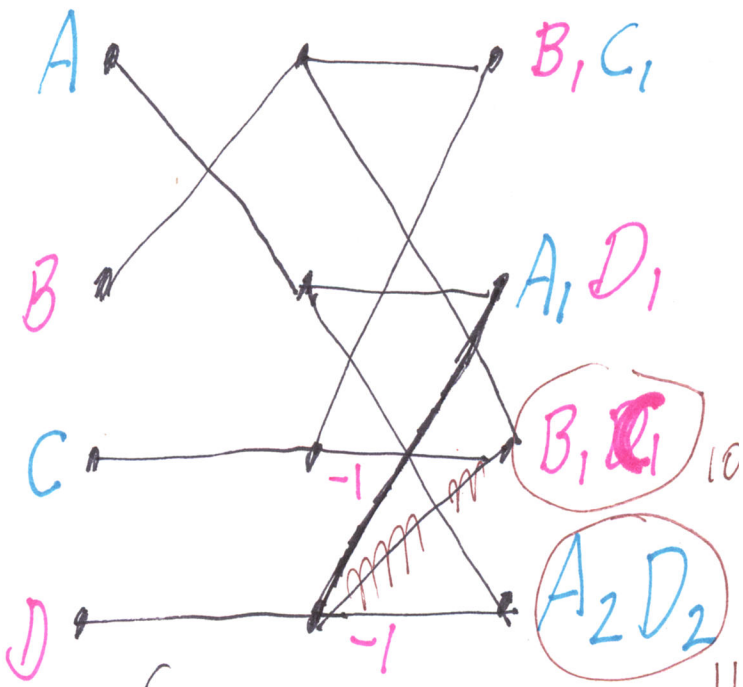
f_0 $\quad H \otimes I$



f_1



f_{id}



$f_{\neg}$

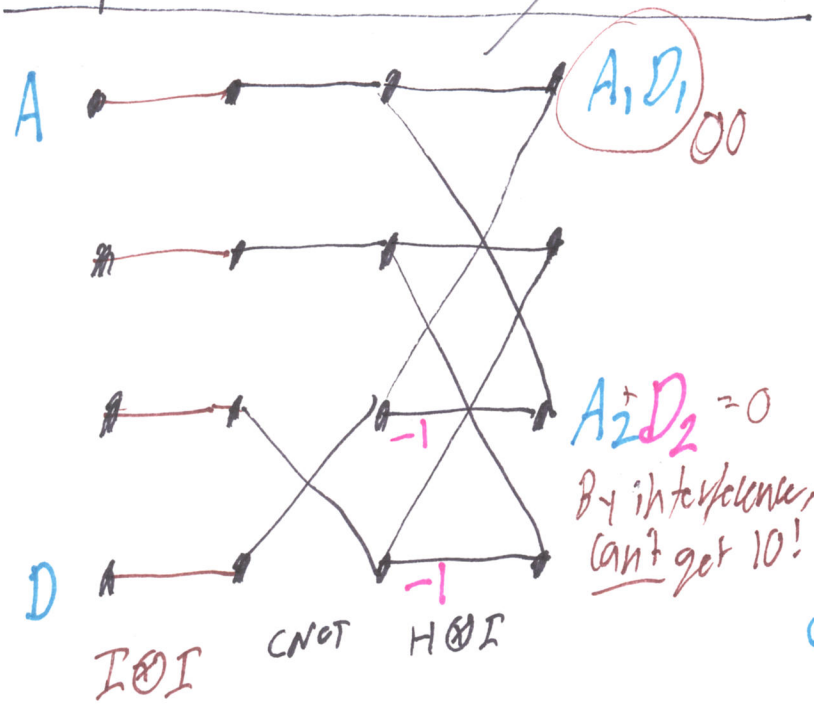
For the constant functions, measurement gives 00 or 01 : $W_1 = 0$

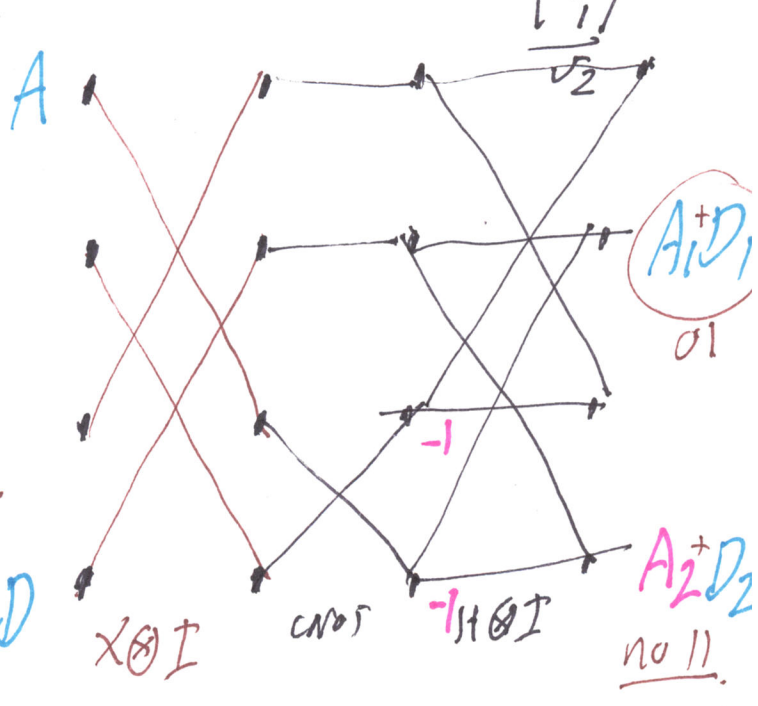
For the balanced functions, measurement gives 10 or 11 : $W_1 = 1$.

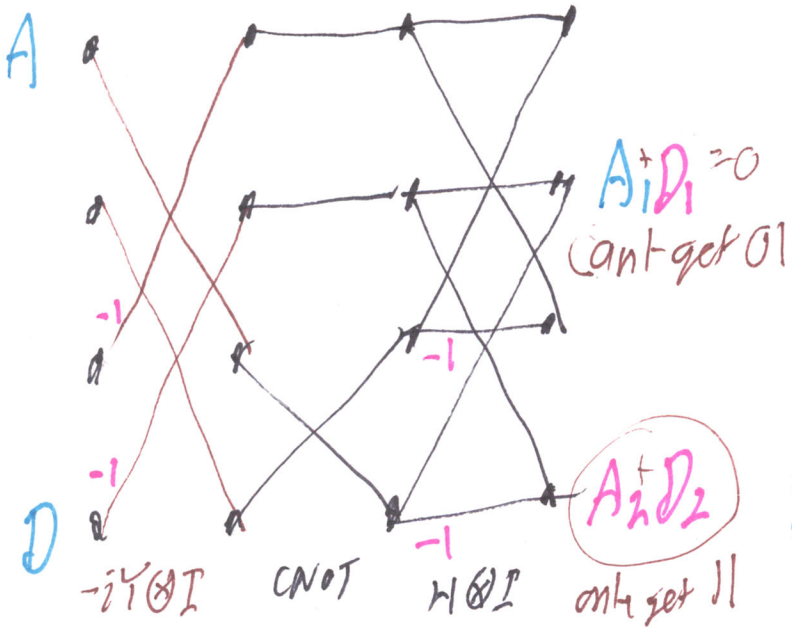
Thus Deutsch's Problem is solvable with one "quantum query" to F.

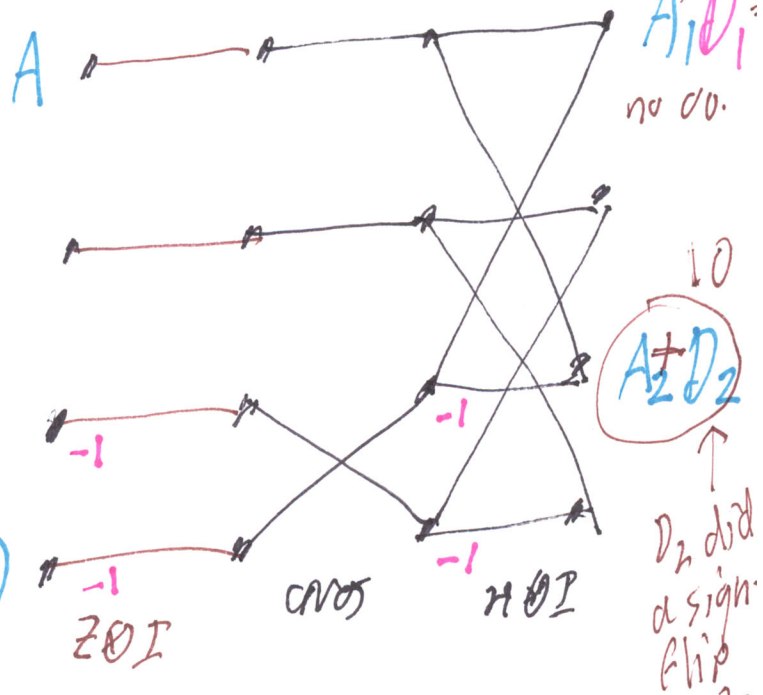
Deutsch-Jozsa Problem: Same math works for input $0^n 1$, $H^{\otimes n+1}$ then F then $H^{\otimes n}$.

Superdense Coding Example: Alice & Bob share $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$









Circuit: