Bernstein - Vazirani's Algorithm (Application of Fourier sampling)

Promise: $f(x) = (a)\, x \pmod 2$ — a: unknown

$a = 0 \rightarrow f(x)$ constant

$a \neq 0 \rightarrow f(x)$ balanced

$= \sum_i a_i x_i \pmod 2$

$$\hat{f}(y) = \frac{1}{2^n} \sum_x (-1)^{xy + ax} = \frac{1}{2^n} \sum_x (-1)^{x(a \oplus y)} = \begin{cases} 1 & \text{if } a = y \iff a \oplus y = 0 \\ 0 & \text{otherwise} \end{cases}$$

bit by bit addition modulo 2

Classicaly: each query to the black box reveals at most one bit about a.

$\rightarrow \Omega(n)$ queries

Here: linear separation $(\Theta(1)$ vs $\Theta(n))$

BUT doesn't separate BQP^{O_f} of BPP^{O_f}

possible to separate using a recursive version

"black box model"