



۸۱۰۱۰۱۵۵۸

پردازش اطلاعات کوانتومی  
نام و نام خانوادگی: مهدی وجهی



ارائه ۸

## ۱ الگوریتم Bernstein – Vazirani

این الگوریتم همانند الگوریتم *Deutsch – Josza* است. روش ها همان است تنها کمی شکل سوال متفاوت است. در این الگوریتم ما تعدادی ورودی داریم و یک مدار نامشخص که بسته به ورودی ها غیر آخر و مقداری که برای هر کدام دارد آنها را ضرب می کند و سپس مقادیر را به پیمانه ۲ جمع می کند اگر مقدار ۱ شد آخرین ورودی را نقیض می کند. روش همان است تمامی ورودی ها را با هادامارد در حالت برهمنهی قرار می دهیم همه  $|+\rangle$  و آخری  $|-\rangle$  است. سپس از مدار عبور می دهیم و از همه غیر آخری هادامارد می گیریم و اندازه می گیریم. آنهایی که مقدار ۱ دارند یعنی ضربی که در آنها ضرب شده ۱ است و بقیه ۰. دلیل این موضوع *Phase Kickback* است. مدار و معادلات آن به شکل زیر است.

$$\begin{array}{c}
 |0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} \boxed{U} \xrightarrow{H^{\otimes n}} \text{Measurement} \\
 |-\rangle \xrightarrow{\oplus} \boxed{U}
 \end{array}
 \quad \text{Before } U : |\psi\rangle = \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} |x\rangle (|0\rangle - |1\rangle)$$

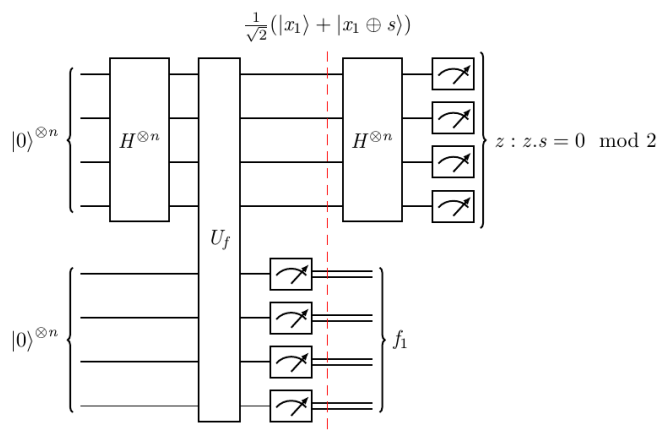
$$\begin{aligned}
 \text{After } U : |\psi\rangle &= \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} f_s |x\rangle (|0\rangle - |1\rangle) & f_s &= s \cdot x \bmod 2 \\
 &= \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} (-1)^{s \cdot x} |x\rangle (|0\rangle - |1\rangle) & H^{\otimes n} |x\rangle &= \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle
 \end{aligned}$$

$$\text{Before meas} : \Rightarrow |\psi\rangle = |s\rangle |-\rangle$$

همچنین پیاده سازی الگوریتم در *qiskit* نیز پیوست شد.

## ۲ الگوریتم Simon

در این الگوریتم مجدد جعبه سیاهی داریم مانند *Deutsch – Josza* اما تابع به شکل  $f : \{0,1\}^n \rightarrow \{0,1\}^n$  است. همچنین درباره این تابع می دانیم که:  $f(x) = f(x \oplus s)$   $s \in \{0,1\}^n$



شکل ۱: مدار الگوریتم سیمون

هدف این الگوریتم پیدا کردن همان  $s$  است در روش کلاسیک ما باید بیش از نصف حالات را امتحان کنیم  $(2^{n-1} + 1)$  با الگوریتم های کلاسیک احتمالاتی این مقدار به  $2^{n/2}$  کاهش پیدا می کند. در این الگوریتم نیز ابتدا تمام ورودی ها را در حالت  $|+\rangle$  قرار می دهیم سپس از اوراکل رد می کنیم. در مرحله بعدی مقادیر خروجی را اندازه می گیریم، این کار باعث می شود که حالت های ورودی که در برهم نهی کامل هستند به  $\frac{1}{\sqrt{2}}(|x_1\rangle + |x_1 \oplus s\rangle)$  فروشکست می کند که زوج حالت مولد خروجی تابع است.

در نهایت چیزی در حدود ۸۵ درصد مباحث را فهم کردم.