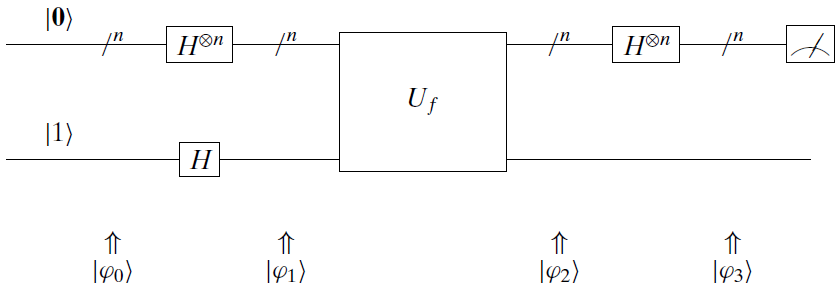
# رایانش کوانتومی
# الگوریتم برنشتاین-وزیرانی

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان




# الگوریتم دویچ–جوتزا

در نتیجه، وابستگی احتمال رمبش به $|\mathbf{0}\rangle$ به $f(\boldsymbol{x})$

در صورت تابع ثابت بودن $f(\boldsymbol{x})$ به ۱، کیوبیت‌های بالائی برابر:

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)|\mathbf{0}\rangle}{2^n} = \frac{-(2^n)|\mathbf{0}\rangle}{2^n} = -1|\mathbf{0}\rangle.$$

در صورت تابع ثابت بودن $f(\boldsymbol{x})$ به **0**، کیوبیت‌های بالائی برابر:

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n} 1|\mathbf{0}\rangle}{2^n} = \frac{2^n|\mathbf{0}\rangle}{2^n} = +1|\mathbf{0}\rangle.$$

# الگوریتم برنشتاین-وزیرانی

تابع مفروض $f: \{0,1\}^n \rightarrow \{0,1\}^n$ با امکان ارزیابی اما به صورت جعبه سیاه

همچنین اطمینان از وجود رشته دودویی $\boldsymbol{s} = s_0 s_1 s_2 \cdots s_{n-1}$ به طوری که برای هر $\boldsymbol{x},\boldsymbol{y} \in \{0,1\}^n$ داریم،

$$f(\boldsymbol{x}) = (\boldsymbol{s}.\boldsymbol{x})\%2 = \langle \boldsymbol{s},\boldsymbol{x} \rangle = s_0 x_0 \oplus s_1 x_1 \oplus s_2 x_2 \oplus \cdots \oplus s_{n-1} x_{n-1}$$

$\boldsymbol{s}$ نامعلوم

راه‌حل کلاسیکی

- با جستجو و پرسش تک بیت در هر زمان
- تمامی رشته‌های با وزن همینگ یک

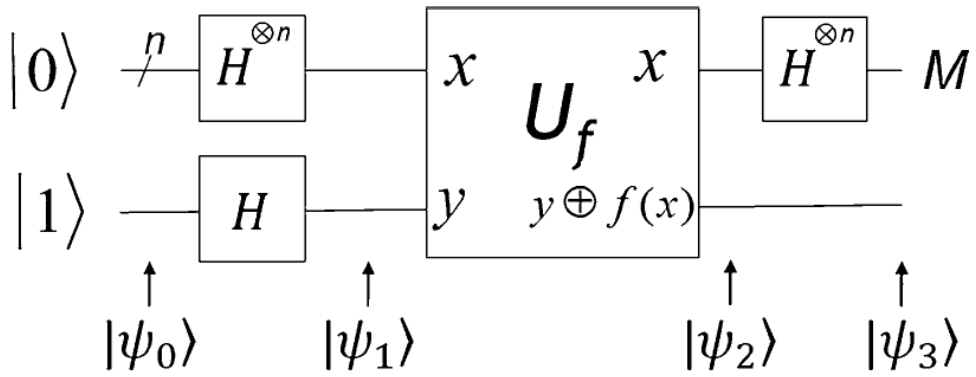
$$f(1000) = s_1$$
$$f(0100) = s_2$$
$$f(0010) = s_3$$
$$f(0001) = s_4$$

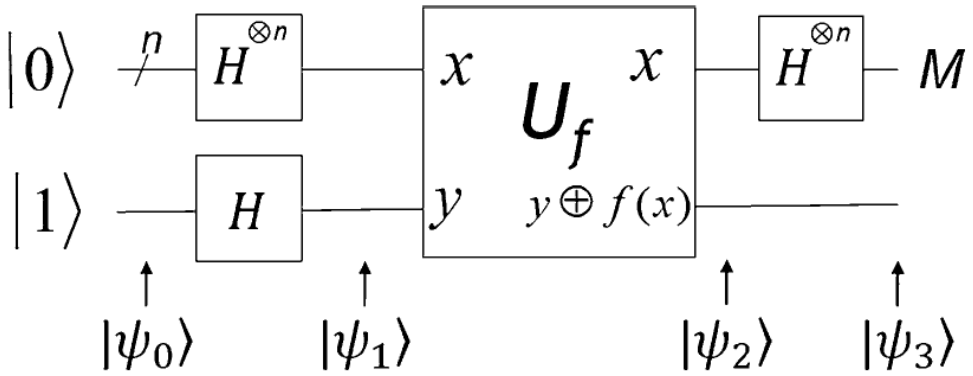
# الگوریتم برنشتاین-وزیرانی

پس جستجوی از مرتبهٔ n

راه‌حل برنشتاین وزیرانی

- کوانتومی
- از مرتبه یک






# الگوریتم برنشتاین-وزیرانی

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

$$|\psi_1\rangle = H^{\otimes n+1}|\psi_0\rangle = \frac{1}{\sqrt{2}^n}\sum_{x=0}^{2^n-1}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

اعمال $U_f$: تبدیل $|x\rangle$ به $(-1)^{f(x)}$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2}^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

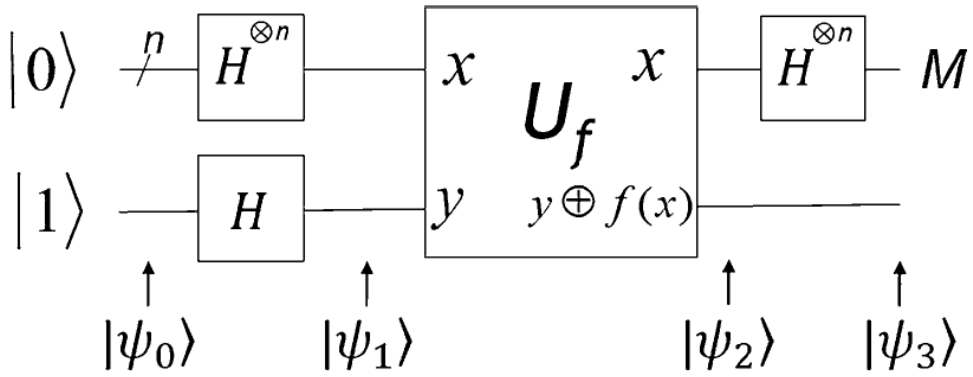
$$= \frac{1}{\sqrt{2}^n}\sum_{x=0}^{2^n-1}(-1)^{s.x}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

اعمال هدامرد

$$|\psi_3\rangle = \left(H^{\otimes n} \otimes I\right)|\psi_2\rangle = \frac{1}{2^n}\sum_{z=0}^{2^n-1}\sum_{x=0}^{2^n-1}(-1)^{s.x \oplus x.z}|z\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{2^n}\sum_{z=0}^{2^n-1}\left(\sum_{x=0}^{2^n-1}(-1)^{(s\oplus z).x}\right)|z\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

# الگوریتم برنشتاین-وزیرانی




$$\frac{1}{۲^n}\sum_{z=0}^{۲^n-۱}\left(\sum_{x=0}^{۲^n-۱}(-۱)^{(s\oplus z).x}\right)|z\rangle\otimes\left(\frac{|0\rangle-|۱\rangle}{\sqrt{۲}}\right)$$

اگر $s \oplus \mathrm{z} = 0$ یا $z = s$ آن‌گاه بزرگی

$$\frac{1}{۲^n}\sum_{x=0}^{۲^n-۱}(-۱)^{(s\oplus z).x}$$

برابر ۱
در نتیجه

$$|\psi_۳\rangle = ۱|s\rangle\otimes\left(\frac{|0\rangle-|۱\rangle}{\sqrt{۲}}\right)$$

مقدار اندازه‌گیری‌شده برابر $s$
اگر $z \neq s$ آن‌گاه بزرگی

$$\frac{1}{۲^n}\sum_{x=0}^{۲^n-۱}(-۱)^{(s\oplus z).x}$$

برابر صفر

# منابع


ارنسن

Chen, C.-Y. (2020). An exact quantum algorithm for testing Boolean functions with one uncomplemented product of two variables. Quantum Information Processing, 19(7). doi:10.1007/s11128-020-02711-8