رایانش کوانتومی
الگوریتم ها

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

الگوریتم‌ها

طراحی الگوریتم‌ها پیش از وجود ماشین‌های اجرای آنها

الگوریتم‌های کلاسیکی مانند الگوریتم تقسیم اقلیدس

وجود الگوریتم‌های کوانتومی پیش از رایانه‌های کوانتومی

کار با کیوبیت‌ها

حل مسائل با اسلوبی کارآمدتر از رفقای کلاسیکی

الگوریتم‌ها

توضیح بر اساس افزایش پیچیدگی

هر یک بر اساس الگوریتم قبلی

تا رسیدن به الگوریتم شور

- برانگیزانندهٔ توجه به رایانش کوانتومی و اجرای عملیات تجزیه در زمان چندجمله‌ای

نبود هیچ روش کلاسیک جهت انجام در چنین زمانی

الگوریتم‌ها

کار تمامی الگوریتم‌های کوانتومی طبق چارچوبی پایه

آغاز کار دستگاه با کیوبیت‌های در حالت کلاسیک معین

تغییر تمامی آنها به برهم‌نهی بسیاری از حالات

عملیات بر روی برهم‌نهی‌ها با استفاده از چندین عملیات یگانی

اندازه‌گیری کیوبیت در پایان

الگوریتم دویچ

مسئله‌ای خاص از الگوریتم دویچ-جوتزا

- الگوریتم دویچ سرعت رایانش را دو برابر می‌کند
- الگوریتم دویچ-جوتزا سرعت رایانش را نمایی بهبود می‌دهد
  - برای n کیوبیت
    - در حالت کلاسیک $۲^{n-۱} + ۱$ رایانش ولی صرفا ۱ رایانش در الگوریتم دویچ-جوتزا
      - حال نسخه تک بیتی نیز دارای سرعتی نمایی!

الگوریتم دویچ

تابعی ناشناس (اراکل)

تابع: $f:\{0,1\}^n \to \{0,1\}$

- ورودی دودوئی n بیتی
- خروجی تک‌بیتی

یا متعادل یا ثابت

- متعادل: تعداد خروجی‌های با مقدار صفر برابر تعداد خروجی‌های با مقدار یک
- ثابت: همه مقادیر خروجی با هم برابر (یا همگی صفر یا همگی یک)

الگوریتم دویچ-جوتزا

- شناسایی ثابت یا متعادل بودن اراکل

الگوریتم دویچ

مثال- n=3

- اراکل ثابت

$$f(x_2 x_1 x_0) = x_2 \cdot x_1 \cdot x_0 \cdot 0$$

$$f(000) = 0 \cdot 0 \cdot 0 \cdot 0 = 0$$
$$f(001) = 0 \cdot 0 \cdot 1 \cdot 0 = 0$$
$$f(010) = 0 \cdot 1 \cdot 0 \cdot 0 = 0$$
$$f(011) = 0 \cdot 1 \cdot 1 \cdot 0 = 0$$
$$f(100) = 1 \cdot 0 \cdot 0 \cdot 0 = 0$$
$$f(101) = 1 \cdot 0 \cdot 1 \cdot 0 = 0$$
$$f(110) = 1 \cdot 1 \cdot 0 \cdot 0 = 0$$
$$f(111) = 1 \cdot 1 \cdot 1 \cdot 0 = 0$$

الگوریتم دویچ

مثال- n=3

- اراکل متعادل

$$f(x_2 x_1 x_0) = x_2 \oplus x_1 \oplus x_0$$

$$f(000) = 0 \oplus 0 \oplus 0 = 0$$

$$f(001) = 0 \oplus 0 \oplus 1 = 1$$

$$f(010) = 0 \oplus 1 \oplus 0 = 1$$

$$f(011) = 0 \oplus 1 \oplus 1 = 0$$

$$f(100) = 1 \oplus 0 \oplus 0 = 1$$

$$f(101) = 1 \oplus 0 \oplus 1 = 0$$

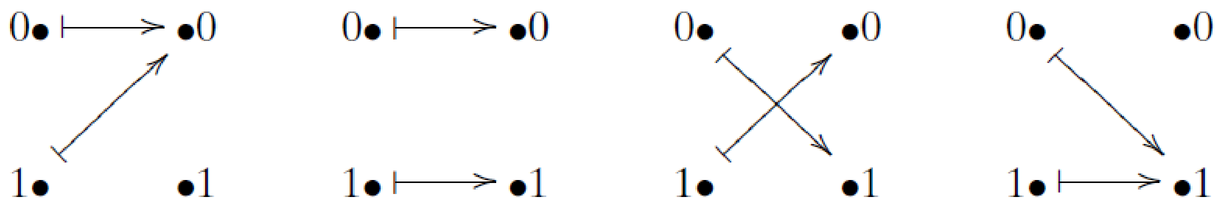
$$f(110) = 1 \oplus 1 \oplus 0 = 0$$

$$f(111) = 1 \oplus 1 \oplus 1 = 1$$

الگوریتم دویچ

ساده‌ترین الگوریتم کوانتومی: الگوریتم دویچ

حل مسئله‌ای ساختگی و کار الگوریتم با توابعی از مجموعهٔ $\{0,1\}$ به مجموعهٔ $\{0,1\}$



الگوریتم دویچ

تابع: $f:\{0,1\} \to \{0,1\}$

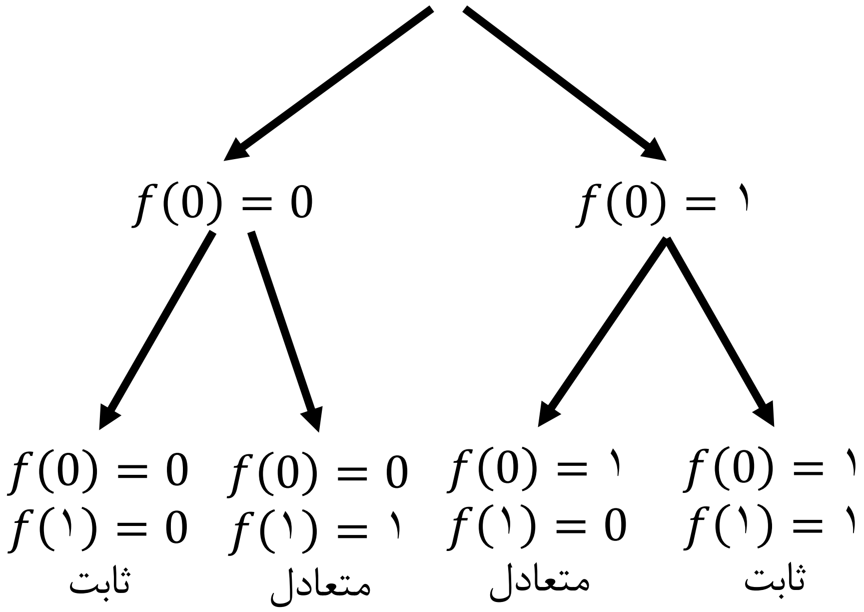
- *متعادل* اگر $f(0) \neq f(1)$
- *ثابت* اگر $f(0) = f(1)$
- پس دو تابع ثابت و دو تابع متعادل

مسئلهٔ الگوریتم دویچ

- با داشتن تابع به عنوان جعبه سیاه و صرفا امکان بررسی خروجی تعیین ثابتی یا تعادل تابع

الگوریتم دویچ

الگوریتم کلاسیک: ارزیابی **f** روی یک ورودی و سپس ارزیابی آن روی ورودی دیگر، و درنهایت مقایسهٔ خروجی‌ها



الگوریتم دویچ

سخن کوتاه، رایانهٔ کلاسیک نیاز به دو بار ارزیابی تابع جهت تعیین نوع

امکان روشی کارآمدتر با رایانه کوانتومی؟

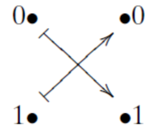
امکان برهم‌نهی «همزمان» دو حالت بنیادی در رایانه کوانتومی

استفاده از آن در الگوریتم پیشنهادی

الگوریتم دویچ

امکان تعبیر تابع به عنوان کنش ماتریسی روی ورودی

- مثال: نگاشت



- متناظر با ماتریس

$$\begin{array}{cc} & \begin{array}{cc} \mathbf{0} & \mathbf{1} \end{array} \\ \begin{array}{c} \mathbf{0} \\ \mathbf{1} \end{array} & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{array}.$$

  - ضرب حالت $|0\rangle$ در سمت راست ماتریس منجر به خروجی حالت $|1\rangle$
  - ضرب حالت $|1\rangle$ در سمت راست ماتریس منجر به خروجی حالت $|0\rangle$
- نام ستون به مثابهٔ ورودی و نام ردیف به مثابهٔ خروجی
- تمرین- ماتریس سه تابع دیگر را روی مجموعه دامنه و هم‌دامنه بدست آورید

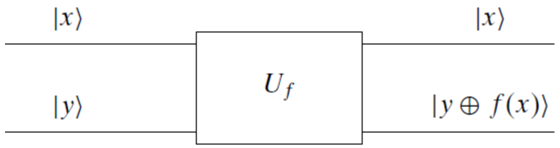
الگوریتم دویچ

عدم کفایت نگاه ماتریسی برای سیستم کوانتومی

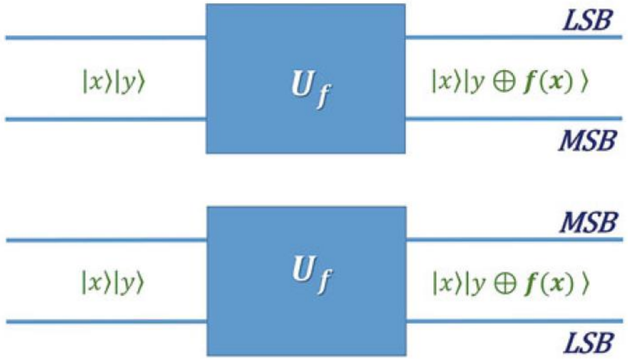
نیاز به افزودنی‌هایی

- یگانی بودن (تبعا برگشت‌پذیری) همهٔ گیت‌ها
- با داشتن خروجی امکان یافتن ورودی
- اگر **f** نام تابع، آن‌گاه جعبه سیاه (اراکل) U_f گیت کوانتومی جهت ارزیابی ورودی

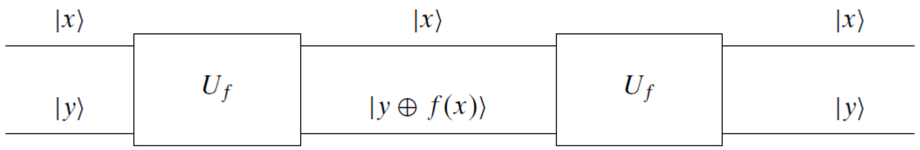
الگوریتم دویچ



- ورودی بالایی $|x\rangle$ مقدار کیوبیتی که دنبال ارزیابی آن هستیم
- ورودی پایینی $|y\rangle$ کنترل‌گر خروجی
- خروجی بالایی همانند و برابر ورودی بالایی $|x\rangle$
- خروجی پایینی برابر کیوبیت $|y \oplus f(x)\rangle$
  - $\oplus$ یاء انحصاری یا جمع دودوئی به پیمانه ۲
- پس تبدیل حالت $|x,y\rangle$ به $|x,y \oplus f(x)\rangle$
  - اگر $y = 0$، آن‌گاه تبدیل حالت $|x,0\rangle$ به $|x,0 \oplus f(x)\rangle = |x,f(x)\rangle$
  - اگر $y = ۱$، آن‌گاه تبدیل حالت $|x,۱\rangle$ به $|x,۱ \oplus f(x)\rangle = |x,\overline{f(x)}\rangle$



الگوریتم دویچ



- برگشت‌پذیری تابع
  - با دو بار قرار دادن مدار پشت سر هم
- به دلیل تبدیل حالت $|x,y\rangle$ به $|x,y \oplus f(x)\rangle$

$$|x, y \oplus f(x) \oplus f(x)\rangle = \left|x, y \oplus \left(f(x) \oplus f(x)\right)\right\rangle = |x, y \oplus 0\rangle = |x, y\rangle$$

- در نتیجه U_f معکوس خود
- در سیستم کوانتومی تناظر ارزیابی f با ضرب حالت در ماتریس یگانی U_f

الگوریتم دویچ

در صورت $f(x) = 0$

$$\boldsymbol{U}_f\,|0\rangle\,|0\rangle = |0\rangle\,|0 \oplus f(0)\rangle = |0\rangle\,|0 \oplus 0\rangle = |0\rangle\,|0\rangle$$

$$\boldsymbol{U}_f\,|0\rangle\,|1\rangle = |0\rangle\,|1 \oplus f(0)\rangle = |0\rangle\,|1 \oplus 0\rangle = |0\rangle\,|1\rangle$$

$$\boldsymbol{U}_f\,|1\rangle\,|0\rangle = |1\rangle\,|0 \oplus f(1)\rangle = |1\rangle\,|0 \oplus 0\rangle = |1\rangle\,|0\rangle$$

$$\boldsymbol{U}_f\,|1\rangle\,|1\rangle = |1\rangle\,|1 \oplus f(1)\rangle = |1\rangle\,|1 \oplus 0\rangle = |1\rangle\,|1\rangle$$

الگوریتم دویچ

در صورت $f(x) = 0$

در صورت $f(x) = 0$

امکان پیاده‌سازی تابع با تابع همانی

امکان پیاده‌سازی تابع با تابع همانی

الگوریتم دویچ

ایجاد برهم‌نهی ورودی‌ها

در جهت ایجاد موازی‌سازی کوانتومی

- جهت ارزیابی بردارهای پایه گوناگون در یک زمان
- نیاز به ایجاد برهم‌نهی $|+\rangle|-\rangle$
- نمایش آن بر اساس پایه استاندارد $|0\rangle/|1\rangle$

$$\begin{aligned} |+\rangle\,|-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{aligned}$$

- دارای اندازه یکسان ولی فازهای متفاوت

الگوریتم دویچ

ارزیابی با استفاده از اوراکل کوانتومی

- اعمال U_f به برهم‌نهی

$$
\begin{aligned}
\boldsymbol{U}_f \,|+\rangle\,|-\rangle &= \boldsymbol{U}_f \left(\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)\right) \\
&= \frac{1}{2}(\boldsymbol{U}_f\,|00\rangle - \boldsymbol{U}_f\,|01\rangle + \boldsymbol{U}_f\,|10\rangle - \boldsymbol{U}_f\,|11\rangle) \\
&= \frac{1}{2}(|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle)
\end{aligned}
$$

الگوریتم دویچ

XOR هر چیزی با 0 برابر با خودش و با 1 برابر قرینهٔ خودش

پس

$$\boldsymbol{U}_f\,|+\rangle\,|-\rangle = \frac{1}{2}\left(|0,\,f(0)\rangle - \left|0,\,\overline{f(0)}\right\rangle + |1,\,f(1)\rangle - \left|1,\,\overline{f(1)}\right\rangle\right)$$

الگوریتم دویچ

فرض بر ثابت بودن تابع، در نتیجه

- $f(0) = f(۱)$، و $\overline{f(0)} = \overline{f(۱)}$
- چون $f(0) = f(۱)$ نوشتن تابع بر اساس $f(0)$
  - دلیل مشابه برای $\overline{f(0)}$

$$
\begin{aligned}
U_f\,|+\rangle\,|-\rangle &= \frac{1}{2}\left(|0, f(0)\rangle - \left|0, \overline{f(0)}\right\rangle + |1, f(1)\rangle - \left|1, \overline{f(1)}\right\rangle\right) \\
&= \frac{1}{2}\left(|0, f(0)\rangle - \left|0, \overline{f(0)}\right\rangle + |1, f(0)\rangle - \left|1, \overline{f(0)}\right\rangle\right) \\
&= \frac{1}{2}\left(|0\rangle\,|f(0)\rangle - |0\rangle\left|\overline{f(0)}\right\rangle + |1\rangle\,|f(0)\rangle - |1\rangle\left|\overline{f(0)}\right\rangle\right) \\
&= \frac{1}{2}\left((|0\rangle + |1\rangle)\,|f(0)\rangle - (|0\rangle + |1\rangle)\left|\overline{f(0)}\right\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|+\rangle\,|f(0)\rangle - |+\rangle\left|\overline{f(0)}\right\rangle\right) \\
&= |+\rangle\,\frac{1}{\sqrt{2}}\left(|f(0)\rangle - \left|\overline{f(0)}\right\rangle\right)
\end{aligned}
$$

الگوریتم دویچ

پس نتیجهٔ تابع ثابت: ضرب $|+\rangle$ در $\frac{۱}{\sqrt{۲}}\left(|f(0)\rangle - |\overline{f(0)}\rangle\right)$

- برهم‌نهی خطی بردارهای پایه
  - در صورت ثابت بودن تابع خروجی کیوبیت $|+\rangle$ خروجی
  - ارزیابی اراکل برای یکبار ولی ارزیابی همزمان هر دو مقدار
  - ثابت نگه‌داشتن مقدار ورودی در صورت ثابت بودن تابع
    - هر دوی ورودی و خروجی برابر $|+\rangle$

الگوریتم دویچ

فرض بر متعادل بودن تابع، در نتیجه

- $f(1) = \overline{f(0)}$ ، و $f(0) = \overline{f(1)}$
- چون $f(0) = \overline{f(1)}$ نوشتن تابع بر اساس $f(0)$
  - دلیل مشابه برای $\overline{f(0)}$

$$\begin{aligned}
U_f \,|+\rangle\,|-\rangle &= \frac{1}{2}\Big(|0,\, f(0)\rangle - \big|0,\, \overline{f(0)}\big\rangle + |1,\, f(1)\rangle - \big|1,\, \overline{f(1)}\big\rangle\Big) \\
&= \frac{1}{2}\Big((|0\rangle - |1\rangle)\,|f(0)\rangle - (|0\rangle - |1\rangle)\,\big|\overline{f(0)}\big\rangle\Big) \\
&= \frac{1}{\sqrt{2}}\Big(|-\rangle\,|f(0)\rangle - |-\rangle\,\big|\overline{f(0)}\big\rangle\Big) \\
&= |-\rangle\,\frac{1}{\sqrt{2}}\Big(|f(0)\rangle - \big|\overline{f(0)}\big\rangle\Big)
\end{aligned}$$

الگوریتم دویچ

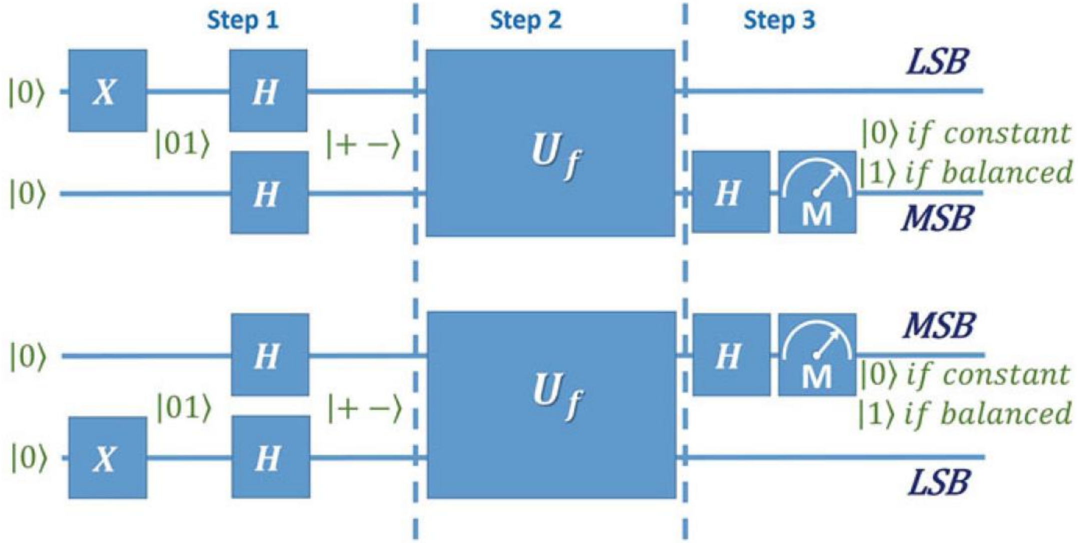
پس نتیجهٔ تابع متعادل: ضرب $|-\rangle$ در $\frac{۱}{\sqrt{۲}}\left(|f(0)\rangle - |\overline{f(0)}\rangle\right)$

- برهم‌نهی خطی بردارهای پایه
  - در صورت ثابت بودن تابع خروجی کیوبیت $|-\rangle$ خروجی
  - ارزیابی اراکل برای یکبار ولی ارزیابی همزمان هر دو مقدار
  - ثابت نگه‌داشتن مقدار ورودی در صورت ثابت بودن تابع
    - هر دوی ورودی و خروجی برابر $|-\rangle$

الگوریتم دویچ

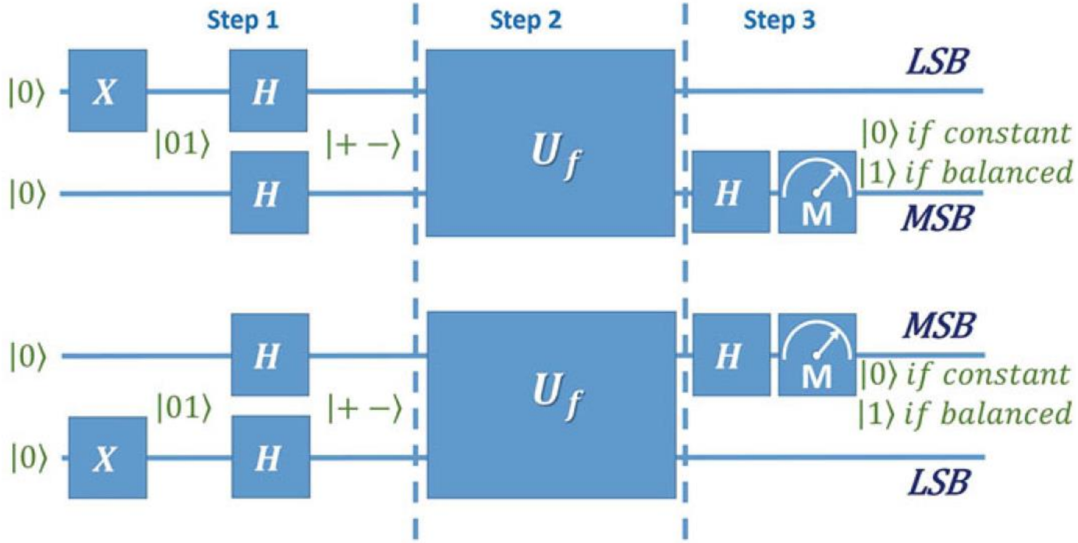
الگوریتم دویچ

- قبول ورودی $|+\rangle|-\rangle$
- خروجی بیشترین مقدار بیت
  - $|+\rangle$ در صورت ثابت بودن تابع f(x)
  - $|-\rangle$ در صورت متعادل بودن تابع f(x)
- پرسش-
  - چگونه ورودی مطلوب را ایجاد کنیم؟
  - با ورودی $|00\rangle$ و استفاده از گیت هدامرد.
    - $H|0\rangle = |+\rangle$
    - $H|۱\rangle = |-\rangle$
  - پس برگرداندن بیت صفر به یک با گیت نقیض X
  - گام یک شکل روبرو



$$(HH)(IX)|0\rangle|0\rangle = (HH)|0\rangle|۱\rangle = |+\rangle|-\rangle$$

الگوریتم دویچ



- چگونه خروجی مطلوب را ایجاد کنیم؟
  - شبیه تدبیر و چارهٔ ورودی
  - تبدیل $|+\rangle|-\rangle$ به بردار صفر و یک با ماتریس هادامرد
    - اثبات کنید؟
  - پس اعمال هادامرد و در صورت صفر بودن
    - متناظر اندازه‌گیری $|+\rangle$ قبل از گیت هادامرد
    - معادل تابع ثابت
  - پس اعمال هادامرد و در صورت یک بودن
    - متناظر اندازه‌گیری $|-\rangle$ قبل از گیت هادامرد
    - معادل تابع متعادل

الگوریتم دویچ

مثال فرض بر ثابت بودن تابع

$$
\begin{aligned}
& \boldsymbol{HI}\left(\frac{1}{2}\left(|0, f(0)\rangle - \left|0, \overline{f(0)}\right\rangle + |1, f(1)\rangle - \left|1, \overline{f(1)}\right\rangle\right)\right) \\
&= \frac{1}{2}\left(|+, f(0)\rangle - \left|+, \overline{f(0)}\right\rangle + |-, f(1)\rangle - \left|-, \overline{f(1)}\right\rangle\right) \\
&= \frac{1}{2}\left(|+\rangle\left(|f(0)\rangle - \left|\overline{f(0)}\right\rangle\right) + |-\rangle\left(|f(1)\rangle - \left|\overline{f(1)}\right\rangle\right)\right) \\
&= \frac{1}{2}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\left(|f(0)\rangle - \left|\overline{f(0)}\right\rangle\right)\right. \\
&\quad \left. + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\left(|f(1)\rangle - \left|\overline{f(1)}\right\rangle\right)\right) \\
&= \frac{1}{2^{3/2}}\left((|0\rangle + |1\rangle)\left(|f(0)\rangle - \left|\overline{f(0)}\right\rangle\right)\right. \\
&\quad \left. + (|0\rangle - |1\rangle)\left(|f(1)\rangle - \left|\overline{f(1)}\right\rangle\right)\right)
\end{aligned}
$$

الگوریتم دویچ

ثابت بودن تابع دال بر

- $|f(0)\rangle - |\overline{f(0)}\rangle = |f(۱)\rangle - |\overline{f(۱)}\rangle$ به دلیل $f(0) = f(۱)$
- با فاکتورگیری $|f(0)\rangle - |\overline{f(0)}\rangle$ داریم

$$\frac{1}{2^{3/2}}\Big((|0\rangle + |1\rangle + |0\rangle - |1\rangle)\Big(|f(0)\rangle - \left|\overline{f(0)}\right\rangle\Big)\Big)$$

$$= \frac{1}{2^{3/2}}\left(2\,|0\rangle\left(|f(0)\rangle - \left|\overline{f(0)}\right\rangle\right)\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle\left(|f(0)\rangle - \left|\overline{f(0)}\right\rangle\right)\right)$$

الگوریتم دویچ

نتیجه‌گیری

- بررسی موازی $f(0)$ و $f(1)$
- با اجرای الگوریتم دویچ، عدم اطلاع از مقادیر $f(0)$ و $f(1)$ در خروجی
  - نمایش خاصیت ذاتی بسیاری از الگوریتم‌های کوانتومی
  - استخراج مقدار محدودی از اطلاع

الگوریتم دویچ-جوتزا

تعمیم الگوریتم دویچ به توابع دیگر

تبدیل $f:\{0,۱\} \rightarrow \{0,۱\}$ به $f:\{0,۱\}^n \rightarrow \{0,۱\}$

ورودی رشته‌های n بیتی صفر و یک و خروجی تک بیت صفر یا یک

ورودی از 0 تا $۲^n - ۱$

تابع $f:\{0,۱\} \rightarrow \{0,۱\}$

- متعادل: اگر نصف ورودی‌ها به صفر و نیم دیگر به یک نگاشت شوند.
- ثابت: اگر تمام ورودی‌ها به صفر یا تمام ورودی‌ها به یک نگاشت شوند.

تمرین- چند تابع $f:\{0,۱\}^n \rightarrow \{0,۱\}$ داریم؟ چند مورد متعادل است؟ چند مورد ثابت است؟

الگوریتم دویچ-جوتزا

فرض: تابع داده شده ولی عدم امکان دیدن تعریف آن. همچنین قطعا یا متعادل یا ثابت. مسئله: تعیین نوع آن

- حل با استفاده از الگوریتم دویچ-جوزا
- مسئلهٔ الگوریتم دویچ حالت خاصی از آن با $n = ۱$

حل کلاسیکی مسئله با ارزیابی تابع با ورودی‌های متفاوت

- بهترین پیرنگ: دو ورودی نخست دارای خروجی‌های متفاوت ← معادل تایید متعادل بودن
- در مقابل، جهت شهود بر ثابت بودن نیاز به ارزیابی تابع برای بیشتر از نیمی از ورودی‌های ممکن
  - پس بدترین پیرنگ نیاز به $\frac{۲^n}{۲} + ۱ = ۲^{n-۱} + ۱$ ارزیابی تابع

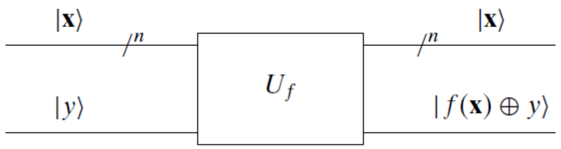
پرسش، آیا امکان بهتری هست؟

الگوریتم دویچ-جوتزا

- در الگوریتم قبلی حل مسئله با با ورود به برهم‌نهی دو حالت ورودی ممکن
- به طریق قیاس، در الگوریتم حاضر، حل مسئله با برهم‌نهی تمامی ۲^n حالت‌های ورودی ممکن

الگوریتم دویچ-جوتزا

داشتن تابع f با ماتریس یگانی با شکل



با ورودی n کیوبیت بالایی و خروجی n کیوبیت بالایی

- $|\boldsymbol{x}\rangle = |x_0 x_۱ \cdots x_{n-۱}\rangle$

کیوبیت ورودی پائین $|y\rangle$

خروجی بالائی U_f برابر با $|\boldsymbol{x}\rangle$ بدون تغییر

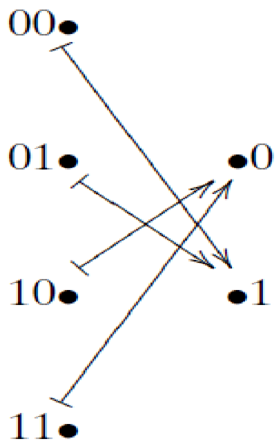
خروجی پائینی U_f تک کیوبیت $|y \oplus f(\boldsymbol{x})\rangle$

- $f(\boldsymbol{x})$ تک بیتی

نشان دهید U_f معکوس خود است

الگوریتم دویچ-جوتزا

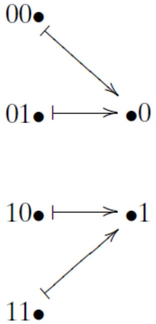
مثال، تابع متعادل از $\{0,1\}^2$ به $\{0,1\}$



الگوریتم دویچ-جوتزا

نمایش تابع با ماتریس یگانی ۸ × ۸

$$
\begin{array}{c}
\\
\mathbf{00,0}\\
\mathbf{00,1}\\
\mathbf{01,0}\\
\mathbf{01,1}\\
\mathbf{10,0}\\
\mathbf{10,1}\\
\mathbf{11,0}\\
\mathbf{11,1}
\end{array}
\begin{array}{c}
\begin{array}{cccccccc}
\mathbf{00,0} & \mathbf{00,1} & \mathbf{01,0} & \mathbf{01,1} & \mathbf{10,0} & \mathbf{10,1} & \mathbf{11,0} & \mathbf{11,1}
\end{array}\\
\begin{bmatrix}
 & 1 & & & & & & \\
1 & & & & & & & \\
 & & & 1 & & & & \\
 & & 1 & & & & & \\
 & & & & 1 & & & \\
 & & & & & 1 & & \\
 & & & & & & 1 & \\
 & & & & & & & 1
\end{bmatrix}
\end{array}
$$



تمرین- تابع متعادل زیر با ماتریس یگانی هشت در هشت نشان دهید.

تمرین- تابع از $\{0,۱\}^۲$ به $\{0,۱\}$ را در نظر بگیرید که همیشه خروجی تک ۱ می‌دهد. ماتریس یگانی هشت در هشت متناظر را طراحی کنید.

الگوریتم دویچ-جوتزا

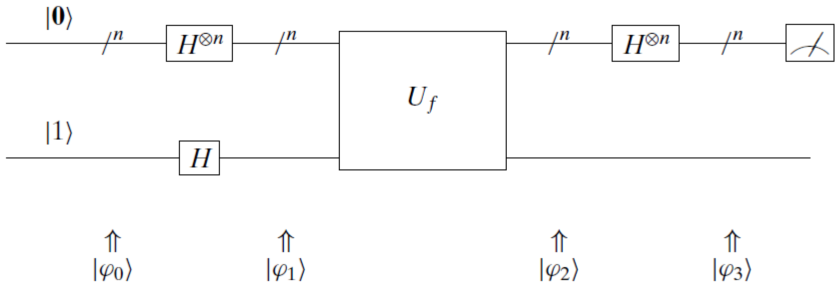
برگشت به مسئله

به دنبال یافتن متعادل یا ثابت بودن تابع

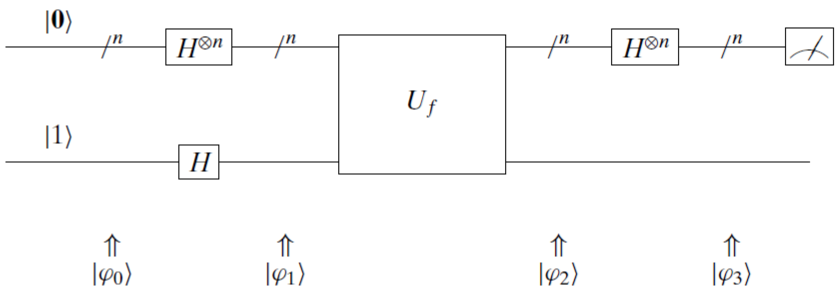
قرار دادن ورودی x به حالت برهم‌نهی تمامی ۲^n ورودی ممکن با احتمال برابر

- چگونه؟
- با ضرب $H^{\otimes n}$ در $|\mathbf{0}\rangle = |00\cdots0\rangle$

درنتیجه، داریم



الگوریتم دویچ-جوتزا



یا

$$(H^{\otimes n} \otimes I)U_f(H^{\otimes n} \otimes H)|\mathbf{0}, 1\rangle.$$

- امکان نوشتن حالت در گام نخست به صورت

$$|\varphi_0\rangle = |\mathbf{0}, 1\rangle,$$

- در گام بعد

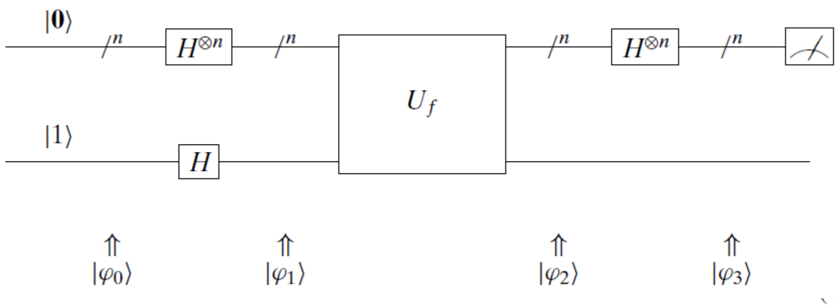
$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle(|0\rangle - |1\rangle)$$

- با اعمال ماتریس U_f

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)$$

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

الگوریتم دویچ-جوتزا



$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle(|0\rangle-|1\rangle)$$

عدم اهمیت $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

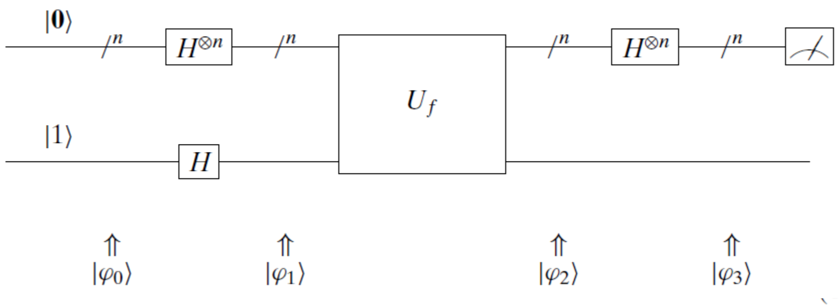
$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle$$

- اعمال $H^{\otimes n}$ به کیوبیت‌های بالایی

$$H^{\otimes n}|y\rangle=\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}(-1)^{y.j}|j\rangle$$

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left[\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}(-1)^{x.j}|j\rangle\right]$$

$$\sum_{j=0}^{2^n-1}\left[\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x.j}\right]|j\rangle$$



الگوریتم دویچ-جوتزا

- جمع نقلی توان‌ها

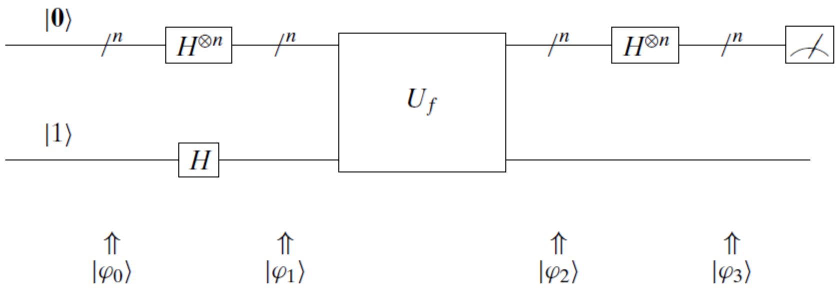
احتمال حالت K-ام

$$\left|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x.j}\right|^2$$

احتمال حالت k=0 متناظر با $|0\rangle^{\otimes n}$

$$\left|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right|^2$$

الگوریتم دویچ-جوتزا

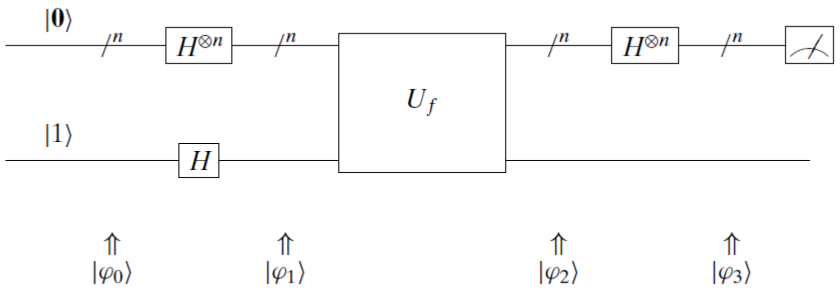


اندازه‌گیری کیوبیت‌های بالایی در گام بعد

به جای اندازه‌گیری بیت بالایی

- احتمال رمبش به حالت $|\mathbf{0}\rangle$ چقدر است؟
- پاسخ با تنظیم $\mathrm{j} = \mathbf{0}$
- $\langle \boldsymbol{j}, \boldsymbol{x} \rangle = \langle \mathbf{0}, \boldsymbol{x} \rangle = 0$
- بنابراین تحویل $|\phi_۳\rangle$ به

$$\left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}|\mathbf{0}\rangle}{2^n}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$



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:

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

در صورت تابع متعادل بودن $f(\boldsymbol{x})$ ، نیمی از ورودی‌ها نیم دیگر را خنثی و کیوبیت‌های بالائی برابر:

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

الگوریتم دویچ-جوتزا

اندازه‌گیری کیوبیت‌های بالایی

- دریافت $|0\rangle$ در صورت ثابت بودن تابع
- در غیر این صورت هر مقدار اندازه‌گیری شدهٔ دیگر معادل متعادل بودن تابع

- سخن کوتاه، حل مسئله در یک تابع ارزیابی برخلاف $۲^{n-۱}+۱$ ارزیابی‌های تابع موردنیاز در رایانش کلاسیک
  - تمرین- در صورتی که تابع نه ثابت و نه متعادل باشد چه رخ خواهد داد؟ الگوریتم چه چیزی را تولید می‌کند؟

منابع

مانوچچی

ؤانگ

نیلسن

شنکار