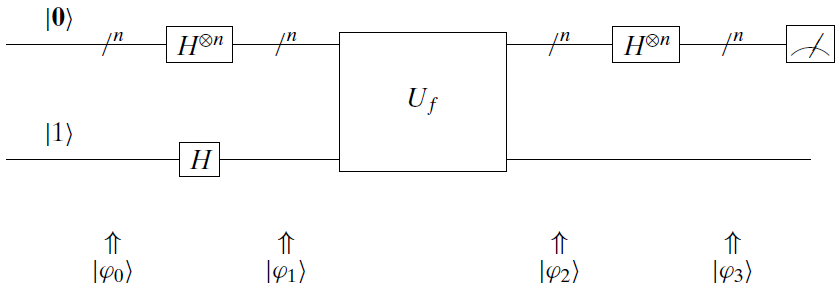
رایانش کوانتومی
الگوریتم تناوب سیمون

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 $f(\boldsymbol{x})$

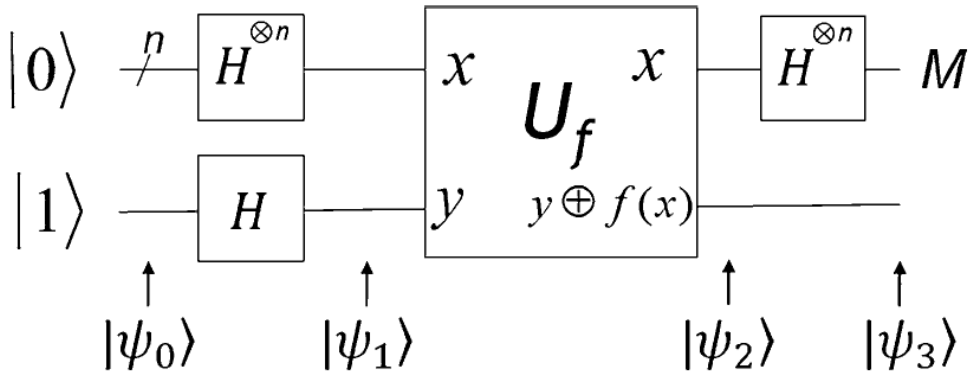
در صورت تابع ثابت بودن $f(\boldsymbol{x})$ به ۱، کیوبیت‌های بالائی برابر:

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

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



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

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 $s \oplus \mathrm{z} = ۱$ یا $z \neq s$ آن‌گاه بزرگی

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

برابر صفر

الگوریتم تناوب سیمون

درباره یافتن الگو در توابع

ترکیبی از رویه‌های کوانتومی و رویه‌های کلاسیکی

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،

$$f(\boldsymbol{x}) = f(\boldsymbol{y}) \Leftrightarrow \boldsymbol{x} = \boldsymbol{y} \oplus \boldsymbol{s}$$

علامت $\oplus$ یاء انحصاری بیت به بیت است. به عبارت اخری، مقادیر تابع با الگوی ثابتی تکرار می‌شوند و اگر با s معین می‌شود. s را تناوب تابع می‌خوانیم.

هدف الگوریتم سیمون تعیین مقدار s

الگوریتم تناوب سیمون

مثال فرض $n = ۳$ و $s = ۱۰۱$

$000 \oplus 101 = 101$ در نتیجه $f(000) = f(101)$.

$001 \oplus 101 = 100$ در نتیجه $f(001) = f(100)$.

$010 \oplus 101 = 111$ در نتیجه $f(010) = f(111)$.

$011 \oplus 101 = 110$ در نتیجه $f(011) = f(110)$.

$100 \oplus 101 = 001$ در نتیجه $f(100) = f(001)$.

$101 \oplus 101 = 000$ در نتیجه $f(101) = f(000)$.

$110 \oplus 101 = 011$ در نتیجه $f(110) = f(011)$.

$111 \oplus 101 = 010$ در نتیجه $f(111) = f(010)$.

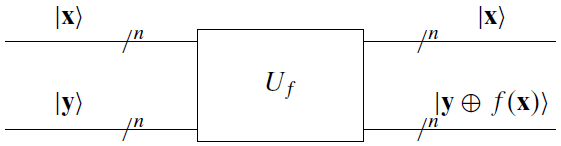
تمرین **f** را با $s = ۰۱۱$ امتحان کنید.

الگوریتم تناوب سیمون

اگر $s = 0^n$ آن‌گاه تابع یک به یک

- در غیر این صورت تابع دو به یک
- چرا؟

تابع به صورت عملیاتی یگانی



نگاشت $|x,y\rangle$ به $|x,y \oplus f(x)\rangle$

U_f معکوس خود

$y = 0^n$ راهی ساده برای ارزیابی $\mathbf{f(x)}$

الگوریتم تناوب سیمون

راه‌حل کلاسیکی:

- نیاز به ارزیابی f روی رشته‌های متفاوت دودوئی

- بررسی خروجی پس از هر ارزیابی
  - اگر x1 و x2 به طوری که f(x1)=f(x2)، حتما

$$x1 = x2 \oplus s$$

  - یافتن s با استفاده از جمع انحصاری هر دو طرف معادله بالا با x2:

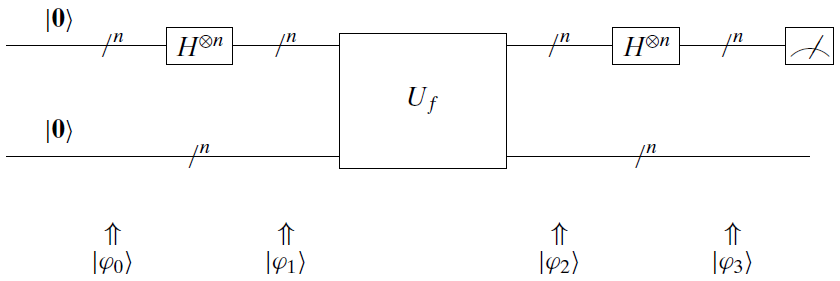
$$x1 \oplus x2 = x2 \oplus s \oplus x2 = s$$

  - در صورت دو به یک بودن تابع نیاز به ارزیابی نیم داده‌ها
  - در صورت ارزیابی بیش از نیم و یافتن تطابق
  - آن‌گاه f یک به یک و $s = 0^n$
  - بدترین حالت نیاز به ارزیابی $۲^{n/۲} + ۱ = ۲^{n-۱} + ۱$
    - نمره اضافه- در صورت الگوریتم تصادفی زمان از چه مرتبه‌ای خواهد بود؟ راهنمایی امکان کمک از پارادوکس تولد
  - امکان بهبود پیچیدگی؟
  - تمرین- فرق تابع پنهان برنشتاین-وزیرانی با سیمون چیست؟

الگوریتم تناوب سیمون

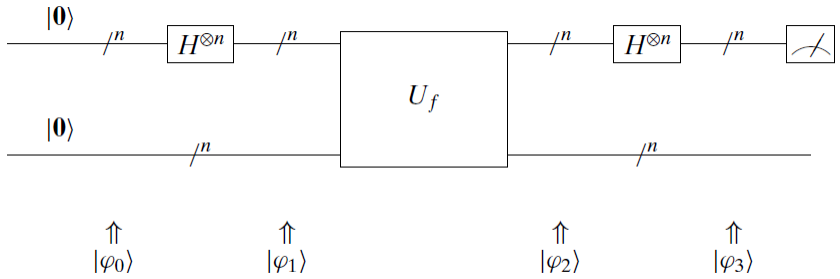
الگوریتم سیمون:

بخش کوانتومی الگوریتم نیاز به تکرار عملیات‌های زیر برای چندین بار:



نمایش ماتریسی

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



الگوریتم تناوب سیمون

آغاز با مقدار

$$\left|0^{\otimes n}, 0^{\otimes n}\right\rangle$$

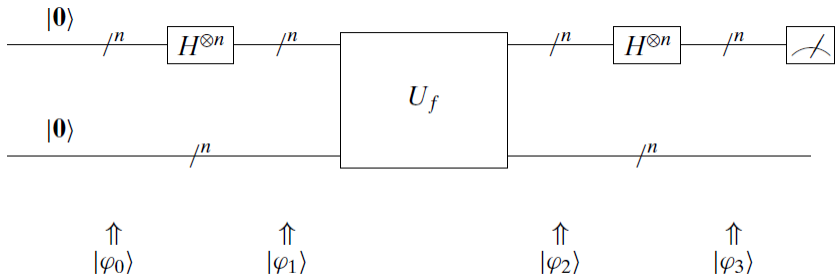
برهم‌نهی ورودی به تمامی ورودی‌های ممکن n کیوبیت نخست

نتیجه به صورت

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x, 0\rangle$$

ارزیابی f روی تمامی ورودی‌های ممکن

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



الگوریتم تناوب سیمون

اعمال $H^{\otimes n}$ به خروجی بالایی

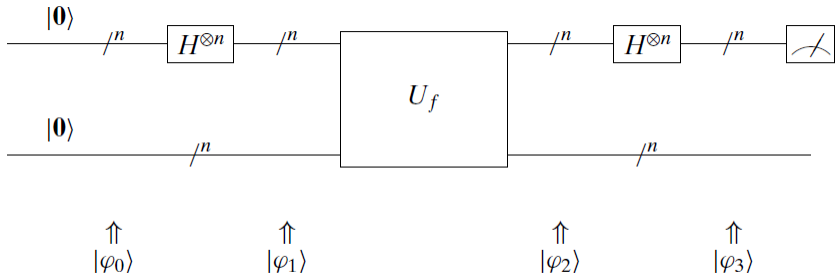
$$\frac{1}{2^n}\sum_{z=0}^{2^n-1}\sum_{x=0}^{2^n-1}(-1)^{x.z}|z\rangle\otimes|f(x)\rangle=\sum_{z=0}^{2^n-1}|z\rangle\left(\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x.z}|f(x)\rangle\right)$$

احتمال اندازه‌گیری حالت $|z\rangle$

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

دو نمونه برای اندازه‌گیری

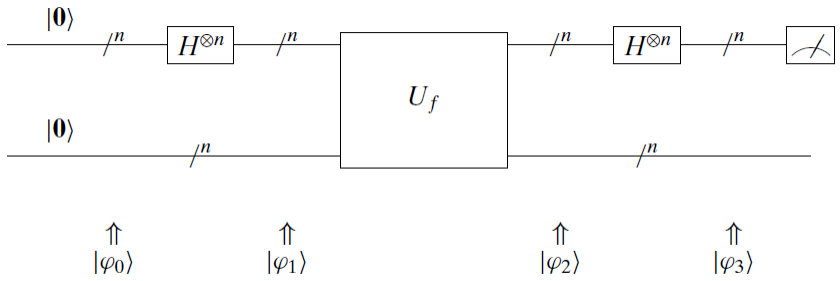
- $s=0^n$ و تابع یک به یک
- $s\neq 0^n$ و تابع دو به یک



الگوریتم تناوب سیمون

- $s = 0^n$ و تابع یک به یک

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



الگوریتم تناوب سیمون

- $s \neq 0^n$ و تابع دو به یک
- وجود x1 و x2 که f(x1)=f(x2)=k

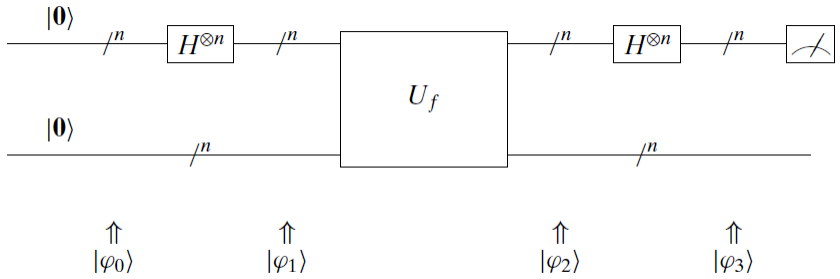
$$\left|\frac{۱}{۲^n}\sum_{x=0}^{۲^n-۱}(-۱)^{x.z}|f(x)\rangle\right|^2 = \left|\frac{۱}{۲^n}\sum_{k}\left((-۱)^{x_1.z}+(-۱)^{x_2.z}\right)|k\rangle\right|^2$$

- $x1 = x2 + s$

$$= \left|\frac{۱}{۲^n}\sum_{k}\left((-۱)^{x_1.z}+(-۱)^{(x_1\oplus s).z}\right)|k\rangle\right|^2$$

$$= \left|\frac{۱}{۲^n}\sum_{k}\left((-۱)^{x_1.z}+(-۱)^{(x_1.z\oplus s.z)}\right)|k\rangle\right|^2$$

$$= \left|\frac{۱}{۲^n}\sum_{k}(-۱)^{x_1.z}(۱+(-۱)^{s.z})|k\rangle\right|^2$$



الگوریتم تناوب سیمون

- $s \neq 0^n$ و تابع دو به یک

$$= \left| \frac{1}{2^n} \sum_k (-1)^{x_1 \cdot z} (1 + (-1)^{s \cdot z}) |k\rangle \right|^2$$

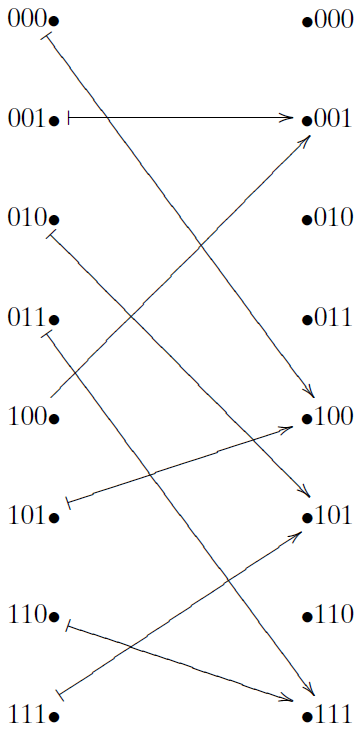
یادآوری اندازه‌گیری z

- z.s=1 احتمال بالا برابر صفر
- z.s=0 احتمال بالا (z) برابر $\frac{1}{2^n}$

دو نمونه برای اندازه‌گیری

- $s = 0^n$ و تابع یک به یک
- $s \neq 0^n$ و تابع دو به یک
  - در هر دو حالت $z.s = 0$

در نتیجه، با اندازه‌گیری کیوبیت‌های بالایی صرفا یافتن رشته‌های دودویی به طوری که $\langle z,s \rangle = 0$



الگوریتم تناوب سیمون

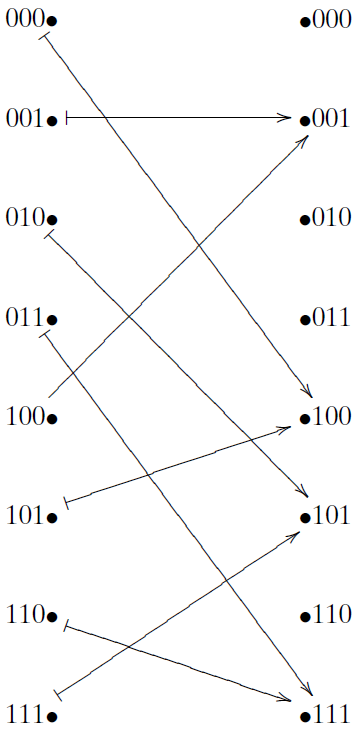
مثال-

با اندازه‌گیری خروجی بالایی، دریافت 000 و ۰۰۱و ۱۰۱ ، و ۱۱۱ با احتمال های برابر

اطلاع از اینکه ضرب داخلی آنها با s مفقود برابر صفر

پس دارای دستگاه مجموعه معادلات زیر

$$\begin{aligned}
&\text{(i)} \quad \langle 000, \mathbf{c} \rangle = 0 \\
&\text{(ii)} \quad \langle 010, \mathbf{c} \rangle = 0 \\
&\text{(iii)} \quad \langle 101, \mathbf{c} \rangle = 0 \\
&\text{(iv)} \quad \langle 111, \mathbf{c} \rangle = 0.
\end{aligned}$$



الگوریتم تناوب سیمون

فرض $\mathbf{s}=s1s2s3$، ان‌گاه

از معادله ii $s_2 = 0$

از معادله iii یا $s1 \oplus s3 = 0$ در نتیجه یا $s1 = s3 = 0$ یا $s1 = s3 = 1$

- به دلیل $s \neq 000$ در نتیجه $s = 101$

پس از چندین بار اجرای الگوریتم سیمون، دریافت n تعداد از z_i-های مختلف به طوری $\langle \boldsymbol{z_i}, \boldsymbol{s} \rangle = 0$

تشکیل دستگاه معادلات خطی از قرار دادن n معادله n مجهوله

- معادلات خطی با استفاده از جمع نقلی $\oplus$ روی رشته‌های دودویی به جای استفاده از جمع ساده +

الگوریتم تناوب سیمون

مثال فرض $n = ۷$ و در نتیجه $f : \{0,۱\}^{۷} \to \{0,۱\}^{۷}$. فرض می‌کنیم الگوریتم را هفت بار اجرا می‌کنیم و به نتایج زیر می‌رسیم:

(i) $\langle 1010110, \mathbf{c} \rangle = 0$
(ii) $\langle 0010001, \mathbf{c} \rangle = 0$
(iii) $\langle 1100101, \mathbf{c} \rangle = 0$
(iv) $\langle 0011011, \mathbf{c} \rangle = 0$
(v) $\langle 0101001, \mathbf{c} \rangle = 0$
(vi) $\langle 0011010, \mathbf{c} \rangle = 0$
(vii) $\langle 0110111, \mathbf{c} \rangle = 0.$

الگوریتم تناوب سیمون

جهت حذف ۱ از ستون نخست، جمع نقلی معادله اول با معادله سوم، در نتیجه

$$\begin{aligned}
&\text{(i)} \quad \langle 1010110, \mathbf{c} \rangle = 0 \\
&\text{(ii)} \quad \langle 0010001, \mathbf{c} \rangle = 0 \\
&\text{(iii)} \quad \langle 0110011, \mathbf{c} \rangle = 0 \\
&\text{(iv)} \quad \langle 0011011, \mathbf{c} \rangle = 0 \\
&\text{(v)} \quad \langle 0101001, \mathbf{c} \rangle = 0 \\
&\text{(vi)} \quad \langle 0011010, \mathbf{c} \rangle = 0 \\
&\text{(vii)} \quad \langle 0110111, \mathbf{c} \rangle = 0.
\end{aligned}$$

جهت حذف ۱ از ستون دوم، جمع نقلی معادله سوم با معادلات پنجم و هفتم، در نتیجه

$$\begin{aligned}
&\text{(i)} \quad \langle 1010110, \mathbf{c} \rangle = 0 \\
&\text{(ii)} \quad \langle 0010001, \mathbf{c} \rangle = 0 \\
&\text{(iii)} \quad \langle 0110011, \mathbf{c} \rangle = 0 \\
&\text{(iv)} \quad \langle 0011011, \mathbf{c} \rangle = 0 \\
&\text{(v)} \quad \langle 0011010, \mathbf{c} \rangle = 0 \\
&\text{(vi)} \quad \langle 0011010, \mathbf{c} \rangle = 0 \\
&\text{(vii)} \quad \langle 0000100, \mathbf{c} \rangle = 0.
\end{aligned}$$

الگوریتم تناوب سیمون

جهت حذف ۱ از ستون سوم، جمع نقلی معادله دوم با معادلات اول و سوم و چهارم و پنجم و ششم، در نتیجه

$$
\begin{aligned}
&\text{(i)} \quad \langle 1000111, \mathbf{c} \rangle = 0 \\
&\text{(ii)} \quad \langle 0010001, \mathbf{c} \rangle = 0 \\
&\text{(iii)} \quad \langle 0100010, \mathbf{c} \rangle = 0 \\
&\text{(iv)} \quad \langle 0001010, \mathbf{c} \rangle = 0 \\
&\text{(v)} \quad \langle 0001011, \mathbf{c} \rangle = 0 \\
&\text{(vi)} \quad \langle 0001011, \mathbf{c} \rangle = 0 \\
&\text{(vii)} \quad \langle 0000100, \mathbf{c} \rangle = 0.
\end{aligned}
$$

جهت حذف ۱ از ستون چهارم، جمع نقلی معادله چهارم با معادلات پنجم و ششم،

همچنین جهت حذف ۱ از ستون پنجم، جمع نقلی معادله هفتم با معادلهٔ نخست، در نتیجه

$$
\begin{aligned}
&\text{(i)} \quad \langle 1000011, \mathbf{c} \rangle = 0 \\
&\text{(ii)} \quad \langle 0010001, \mathbf{c} \rangle = 0 \\
&\text{(iii)} \quad \langle 0100010, \mathbf{c} \rangle = 0 \\
&\text{(iv)} \quad \langle 0001010, \mathbf{c} \rangle = 0 \\
&\text{(v)} \quad \langle 0000001, \mathbf{c} \rangle = 0 \\
&\text{(vi)} \quad \langle 0000001, \mathbf{c} \rangle = 0 \\
&\text{(vii)} \quad \langle 0000100, \mathbf{c} \rangle = 0.
\end{aligned}
$$

الگوریتم تناوب سیمون

جهت حذف ۱ از ستون ششم، جمع نقلی معادله پنجم با معادلات اول و دوم و ششم، در نتیجه

$$
\begin{aligned}
&\text{(i)} \quad \langle 1000010, \mathbf{c} \rangle = 0 \\
&\text{(ii)} \quad \langle 0010000, \mathbf{c} \rangle = 0 \\
&\text{(iii)} \quad \langle 0100010, \mathbf{c} \rangle = 0 \\
&\text{(iv)} \quad \langle 0001010, \mathbf{c} \rangle = 0 \\
&\text{(v)} \quad \langle 0000001, \mathbf{c} \rangle = 0 \\
&\text{(vi)} \quad \langle 0000000, \mathbf{c} \rangle = 0 \\
&\text{(vii)} \quad \langle 0000100, \mathbf{c} \rangle = 0.
\end{aligned}
$$

در نتیجه امکان تفسیر

- (i): $s1 \oplus s6 = 0$
- (ii): $s3 = 0$
- (iii): $s2 \oplus s6 = 0$
- (iv): $s4 \oplus s6 = 0$
- (v): $s7 = 0$
- (vi):
- (vii): $s5 = 0$
- در صورتی s6=0 آنگاه s1=s2=s4=0 و در صورتی که s6=0 آن‌گاه s1=s2=s4=1
- به دلیل $s \neq 0000000$ پس $s = 1101010$

الگوریتم تناوب سیمون

سخن کوتاه، با داشتن تابع متناوب f امکان یافتن تناوب s در n ارزیابی تابع.

مقایسه با $۱ + ۲^{n-۱}$ مرحله لازم در روش کلاسیکی

استفاده از یافتن تناوب تابع در الگوریتم شور

منابع

آرنسن

مانوچچی

ژانگ

نیلسن

شنکار