فهرست مطالب

۱.۰ مقدمه ۲
۲.۰ basis superpos vs comp ۲

۱ آشنایی با مفاهیم اولیه ۳
۱.۱ کیوبیت ۳
۲.۱ basis fourier - basis computayional - vector bloch ۴
۳.۱ گیت‌های کوانتومی ۴
۱.۳.۱ انواع گیت کوانتومی ۵
۲.۳.۱ gate Swap ۸
۴.۱ مدارهای کوانتومی ۸
۱.۴.۱ نحوه‌ی نمایش مدارهای کوانتومی ۱۱

۲ برنامه‌نویسی کوانتومی ۱۳
۱.۲ تفاوت کامپیوتر کلاسیک و کوانتومی ۱۳
۲.۲ Qiskit and computer Quantum IBM ۱۳

۳ الگوریتم‌های کوانتومی ۱۵
۱.۳ موازی سازی کوانتومی ۱۵
۱.۱.۳ مدل محاسباتی استاندارد ۱۹
۲.۱.۳ مدل کوئری ۱۹
۲.۳ Algorithm Deutsch ۲۰
۱.۲.۳ مسئله‌ی دوچ ۲۰
۲.۲.۳ الگوریتم دوچ ۲۱

۳.۳ Algorithm Deutsch-Jozsa ۲۴
۴.۳ oracle ۲۴

۴ شبیه‌سازی پدیده‌های کوانتومی ۲۵
۱.۴ states Bell ۲۵
۲.۴ entanglement ۲۶
۳.۴ coding dense super ۲۶
۴.۴ Teleport ۲۶

۱.۰ مقدمه

در عصر حاضر بواسطه‌ی رشد و توسعه‌ی نظریه‌ی اطلاعات کوانتومی و سرمایه‌گذاری های مالی و انسانی بسیار در این زمینه،شاهد افزایش تعداد علاقمندان به این حوزه هستیم. در این پا .....

۲.۰ basis superpos vs comp

in not input an to Uf applies which ،۱۷.۱ Figure in shown circuit the Consider super- the in prepared is register data the Instead، basis. computational the on acting gate Hadamard a with created be can which ،۲√/(⍰۱| + ⍰۰|) position state: the in resulting ، Uf apply we Then .⍰۰|

فصل ۱

آشنایی با مفاهیم اولیه

۱.۱ کیوبیت

یک کیوبیت[۱]، معادل یک واحد اطلاعات کوانتومی می‌باشد. این مفهوم معادل مفهوم کلاسیک بیت[۲] می‌باشد. به طور کلی هر کیوبیت حاوی دو بیت اطلاعات است. برای تبیین یک کیوبیت از خصوصیات سامانه های کوانتومی، بهره‌می‌بریم. کیوبیت یک سیستم کوانتومی با فضای دوبعدی است. برای تعیین این دوبعد می‌توان ا ز یکی از خصوصیات سامانه های کوانتومی استفاده کرد.

برخلاف بیت ها که مقادیر ثابت ۰ یا ۱ را به خود می‌گیرند؛ یک کیوبیت می‌تواند در یک حالت «برهمنهی کوانتومی» باشد؛ این بدان معناست که یک کیوبیت بواسطه‌ی مشاهده ناظر به یکی از حالات ۰ یا یک تبدیل شود. این مهم‌ترین مزیت استفاده از کیوبیت‌هاست. بیان ریاضی یک کیوبیت ،در حالت برهمنهی، به شرح زیر است:

$$\begin{cases} |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \\ \alpha^2 + \beta^2 = 1 \end{cases}$$

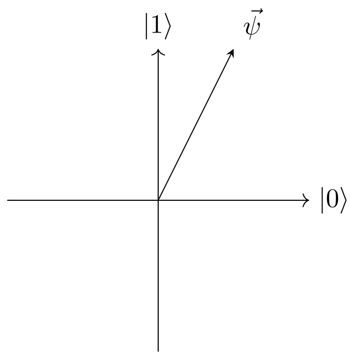
---

[۱] Qubit

[۲] Bit Binary

کت‌ها$\langle 0|$ و $\langle 1|$ بیانگر پایه‌های فضای محاسباتی[۳] هستند؛ و مقادیر α^2 و β^2 بیانگر احتمال وقوع هر یک از این حالات، در صورت مشاهده، می‌باشند.

نمایش بردار ψ به شرح زیر است:



در بسیاری از مواقع برای سهولت در محاسبات، عملگرها و حالات کوانتومی به کمک ماتریس‌ها نمایش داده می‌شوند. فرم ماتریسی هر یک از حالات ذکر شده در بالا به شرح زیر است:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad\qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{۱.۱}$$

برای تعریف کیوبیت ها، راه های زیادی وجود دارد، حالات قطبش فوتون،اسپین الکترون،یا سطوح انرژی اتم،هریک می‌توانند تعیین کننده‌ی بردارهای فضای کیوبیت باشند.

۲.۱ ba- fourier - basis computayional - vector bloch sis

۳.۱ گیت‌های کوانتومی

گیت‌های کوانتومی[۴] یکی از اولین و مهم‌ترین اجزای مدارهای کوانتومی می‌باشند. این گیت‌ها عملگرهایی با قابلیت اثرگذاری روی کیوبیت‌ها می‌باشند. با اعمال یک گیت کوانتومی بر روی یک یا چند کیوبیت،

---

[۳] Computational Basis Vectors

[۴] Quantum Gates

می‌توان تغییرات مدنظر خود را روی کیوبیت اعمال کرد. با کمک این گیت‌ها می‌توان باعث برهم‌نهی کوانتومی یا رمزگذاری داده در داخل یک یا چند کیوبیت شد.

۱.۳.۱ انواع گیت کوانتومی

گیت‌های کوانتومی، دارای انواع مختلف گوناگونی می‌باشند. به طور کلی گیت‌های کوانتومی، عملگرهایی یکه و بازگشت‌پذیر می‌باشند.

گیت هادامارد

مهم‌ترین گیت کوانتومی،گیت هادامارد[۵] است. با اعمال اثر این گیت روی یک کیوبیت، آن کیوبیت به‌یک حالت برهم نهی کوانتومی گذار می‌کند. به عبارت دیگر هر یک از زیرحالات این حالت برهم‌نهی، با احتمال یکسانی قابل رخ دادن هستند.

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \qquad H\left|1\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)$$

این گیت کوانتومی به صورت خطی روی یک دسته کت اثر می‌کند. نمایش ماتریسی این گیت‌کوانتومی به شرح زیر است:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|0\rangle = l\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

---

[۵] Hadamard gate

$$H|1\rangle = l\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

این گیت کوانتومی، یک گیت بازگشت‌پذیر است؛ یعنی اگر این گیت روی یک حالت کوانتومی اثر کند؛ می‌تواند آن را از حالت برهمنهی خارج کند.

برای اعمال این گیت کوانتومی، فقط به یک کیوبیت نیاز داریم. به اصطلاح این گیت،یک Single-Qubit Quantum gate می‌باشد.

نمایش این گیت‌کوانتومی در مدار با علامت زیر است: $—\boxed{H}—$

گیت CNOT

گیت کوانتومی CNOT[۶]، به عنوان گیت منطقی، یاد می‌شود. این گیت کوانتومی معادل گیت NOT کلاسیک می‌باشد. به‌طور معمول، برای اعمال اثر این گیت کوانتومی نیاز به دو کیوبیت داریم. این گیت کوانتومی فقط و فقط در مواقعی که «کیوبیت کنترل[۷]» دارای مقدار $|1\rangle$ باشد، باعث تغییر وضعیت «کیوبیت هدف[۸]» می‌شود.

کیوبیت کنترل: کیوبیت هدف:

خلاصه‌ای از عملکرد این تابع به شرح زیر است:

ببین چرا از این نماد به جای تنسور پراداکت استفاده شده

$\|A$	$B\rangle$		$\|A$	$B \oplus A\rangle$
$\|control\rangle$	$\|target\rangle$	Effect CNOT Gate	$\|control\rangle$	$\|target\rangle$
$\|0\rangle$	$\|0\rangle$	$\Longrightarrow$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\Longrightarrow$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\Longrightarrow$	$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$\Longrightarrow$	$\|1\rangle$	$\|1\rangle$

نمایش ماتریسی این گیت کوانتومی به شکل زیر است:

[۶] gate controlled-X or gate controlled-NOT
[۷] Qubit Controled
[۸] Qubit Target

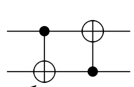
اینا باید اصلاح بشه

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathrm{CNOT}\,|1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\mathrm{CNOT}\,|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |10\rangle$$

نمایش در داخل مدار:



از این گیت کوانتومی، برای بسیاری مدارها و شبیه‌سازی‌های کوانتومی، از جمله تلپورت، درهمتنیدگی و ...، استفاده می‌شود.

گیت توفولی

گیت کوانتومی توفولی،یک نوع خاص از گیت CNOT است. سازوکار این گیت مشابه گیت CNOT می‌باشد؛ با این تفاوت که با در نظر گرفتن وضعیت دو کیوبیت کنترل شده، وضعیت کیوبیت سوم را

تغییر می‌دهد. خلاصه ای از عملکرد این گیت کوانتومی به شرح زیراست:

به بیان دیگر اگر دو کیوبیت کنترل شده، مقدار یک داشته باشند؛ کیوبیت هدف مقدارش تغییر می‌کند. فرم ماتریسی این عملگر به شکل زیر است:

این گیت کوانتومی در مدار کوانتومی به شکل زیر نشان داده می‌شود:

گیت تغییر فاز

گیت تغییر فاز[۹]، یکی از گیت های مهم کوانتومی می‌باشد. این گیت با ضرب کردن یک عدد ثابت در فاز یک کیوبیت، باعث تغییر فاز کیوبیت می‌شود. این گیت کوانتومی در بسیاری از الگوریتم‌های سرچ کوانتومی به‌کار می‌رود. این گیت بدین صورت تعریف می‌شود:

فرم ماتریسی این گیت به شرح زیر است:

این گیت کوانتومی در مدار کوانتومی به شکل زیر نشان داده می‌شود:

گیت دوران

گیت دوران، [۱۰]، باعث دوران حالت کیوبیت، در فضای هیلبرت می‌شود. پایه‌های فضای هیلبرت مذکور بردار های................................ هستند. نمایش این گیت کوانتومی به شرح زیر است:

فرم ماتریسی این گیت به شرح زیر است: نمایش این گیت در مدار کوانتومی به شرح زیراست:

۲.۳.۱ gate Swap

۴.۱ مدارهای کوانتومی

مدارهای کوانتومی[۱۱]، یک دسته از گیت های کوانتومی،که با یک توالی بخصوص قرار گرفته اند، می‌باشند. این کیوبیت ها، با توالی یاد شده، روی یک یا چند دسته کیوبیت، اثر داده می‌شوند.

مدارهای کوانتومی، یکی از اولین مفهوم‌های بکاررفته برای تعریف کامپیوترهای کوانتومی می‌باشند. برای تعریف و شبیه‌سازی هریک از پدیده‌ها و الگوریتم‌های کوانتومی، نیاز به یک مدار به‌خصوص داریم.

---

[۹] gate shift Phase
[۱۰] gate Rotation
[۱۱] circuit quantum

شباهت ها و تفاوت های مدارهای کلاسیک و کوانتومی

gates quantum use they but circuits، classical to similar are circuits Quantum that operations reversible are gates Quantum gates. logic classical of instead qubit. a of state quantum the manipulate to used be can

circuits quantum between differences and similarities some are here Sure، circuits: classical and

Similarities:

op- of sequence a of composed are circuits classical and quantum Both * represented be can circuits Both * data. of set a to applied are that erations implement to used be can circuits Both * notation. similar a using graphically algorithms.

Differences:

unit basic their as bits، quantum are which qubits، use circuits Quantum * of unit basic their as bits، classical are which bits، use circuits Classical data. of operations، reversible are which gates، quantum use circuits Quantum * data. irre- are which gates، logic use circuits Classical operations. basic their as exploit can circuits Quantum * operations. basic their as operations، versible entangle- and superposition as such mechanics، quantum of properties the computers. classical for impossible are that tasks perform to ment،

between differences and similarities the summarizes that table a is Here circuits: classical and circuits quantum

data of unit Basic | |—|—|—| | Circuit Classical | Circuit Quantum | Feature | | Reversibility | | gates Logic | gates Quantum | operations Basic | | Bit | Qubit | Possible | | No | Yes | mechanics quantum Exploits | | Irreversible | Reversible quantum simulating databases، unsorted searching integers، Factoring | tasks | operations logical calculating، Sorting، | systems

questions. other any have you if know me Let helps! this hope I

اجزای مدارهای کوانتومی و سایز آن

They qubits. on performed are that actions the are Operations Operations:
actions. other or initializations، measurements، be can

The circuit. the in gates of number the is circuit quantum a of size The
of size the of terms in measured often is algorithm quantum a of complexity
it. implement to required is that circuit quantum the

Qubits

can They computing. quantum in information of unit basic the are Qubits
be can qubit a that means This .۱ and ۰ states، two of superposition a in be
superposi- quantum called property a is which time، same the at ۱ and ۰ both
is qubit one of state the that means which entangled، be also can Qubits tion.
qubit. another of state the on dependent

Gates

create to used be can They qubits. to applied are that operations are Gates
dif- many are There qubits. entangle and rotations، perform superpositions،
Hadamard the include ones common most the of some but gates، of types ferent
gate. Toffoli the and gate، CNOT the gate،

Operations

mea- be can They qubits. on performed are that actions the are Operations
collapse to used are Measurements actions. other or initializations، surements،
used are Initializations .۱ or ۰ value، definite a into qubit a of state quantum the
.۱ or ۰ value، specific a to qubit a of state the set to

Circuits Quantum

the to similar is that notation graphical a using written are circuits Quantum
quan- a of axis horizontal The computing. classical in used diagrams circuit
The qubits. the represents axis vertical the and time، represents circuit tum
the represent boxes the between lines the and boxes، by represented are gates
qubits. the between connections

Conclusion

oper- and gates، qubits، are circuit quantum a of components basic The are which algorithms، quantum create to used are components These ations. cir- Quantum computer. quantum a on performed be only can that algorithms potential the have they and computation، quantum for tool powerful a are cuits and chemistry، cryptography، including fields، different many revolutionize to learning. machine

۱.۴.۱ نحوه‌ی نمایش مدارهای کوانتومی

the to similar is that notation graphical a using written are circuits Quantum quan- a of axis horizontal The computing. classical in used diagrams circuit The qubits. the represents axis vertical the and time، represents circuit tum the represent boxes the between lines the and boxes، by represented are gates qubits. the between connections

can They computation. quantum for tool powerful a are circuits Quantum Shor's including algorithms، quantum of variety wide a implement to used be unsorted searching for algorithm Grover's and integers factoring for algorithm databases.

فصل ۲

برنامه‌نویسی کوانتومی

۱.۲ تفاوت کامپیوتر کلاسیک و کوانتومی

۲.۲ Qiskit and computer Quantum IBM

فصل ۳

الگوریتم‌های کوانتومی

چه گونه‌ای از مسائل محاسباتی قابل اجرا با مدارهای کوانتومی می‌باشند؟ تفاوت و برتری مدارهای کوانتومی نسبت به مدارهای کلاسیک چیست؟ آیا می‌توان یک حوزه‌ی خاص را تعیین کرد؛ به گونه‌ای که عملکرد کامپیوترهای‌کوانتومی نسبت به کامپیوترهای کلاسیک مزیت داشته باشند؟

در این بخش می‌خواهیم به طور خلاصه این سوالات را پاسخ دهیم و توضیح دهیم چگونه می‌توان از کامپیوترهای کوانتومی به شکلی سودمند استفاده کنیم.

۱.۳ موازی سازی کوانتومی

موازی‌سازی کوانتومی[۱] ، پایه‌واساس بسیاری از الگوریتم‌های کوانتومی است. با گذار یک حالت کوانتومی به حالت برهمنهی کوانتومی، درحین محاسبات کوانتومی یک تابع نظیر f(x)، می‌تواند مقادیر مختلف x را به طور همزمان بررسی کند. این درحالیست که در محاسبات کلاسیک به دلیل ماهیت بیت‌های اطلاعات، تابع f(x) فقط می‌تواند یکی از مقادیر مجاز برای x را بررسی کند.

فرض کنید تابع f ،یک تابع تک‌ـ کیوبیت، به صورت زیر تعریف شده است:

$$f(x) : \{0,1\} \rightarrow \{0,1\}$$

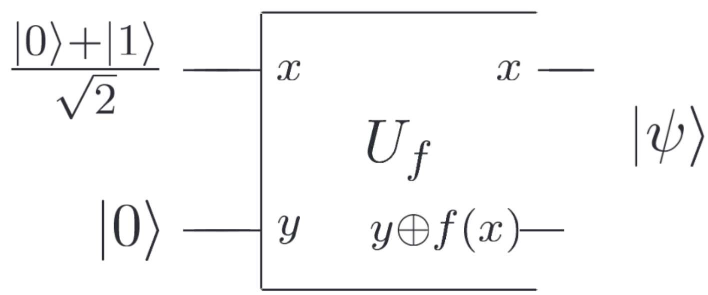
روش مناسب برای محاسبه این تابع در یک کامپیوتر کوانتومی، با در نظر گرفتن دو کیوبیت که در حالت $|x, y\rangle$شروع می شود. با یک توالی مناسب از گیت های منطقی می توان این حالت را به

[۱] parallelism Quantum

$|f(x) \oplus x, y\rangle$ تبدیل کرد که در آن $\oplus$ بیانگر جمع مدوله با پایه۲ می‌باشد.
۲

هریک از دسته‌های کیوبیت، **رجیستر کوانتومی** نامیده‌می‌شوند. اولین رجیستر، «رجیستر داده» و دومین رجیستر «رجیستر هدف» نامیده می‌شود.
ازین پس در این بخش به عامل گذار $|x, y\rangle \to |x, y \oplus f(x)\rangle$، عنوان «تابع U_f» را اطلاق خواهیم کرد. لازم به ذکرست که این تبدیل، یک تبدیل یکه به شمار می‌آید.[۳]

اگر $y = 0$ آنگاه مقدار دومین کیوبیت بعد از اعمال تابع U_f برابر با مقدار f(x) خواهد بود.



شکل ۱.۳: مدار کوانتومی برای ارزیابی $f(0)$ و $f(1)$ به طور همزمان. Uf مدار کوانتومی است که ورودی هایی مانند $|x, y\rangle$ را به $|x, y \oplus f(x)\rangle \to |x, y\rangle$، تصویر می‌کند.

در شکل بالا مقادیر ورودی داده شده به تابع U_f در پایه‌های محاسباتی قرار ندارند. رجیستر داده در حالت برهمنهی قرار دارد. این حالت برهمنهی را می‌توان با اعمال گیت هادامارد بر حالت کوانتومی $|0\rangle$

---

[۲] ex- For .۲ by division a of remainder the returns that operation mathematical a is ۲ Modulo
.۱ of remainder a and ۲ of quotient a has ۲ by divided ۵ because ،۱ is ۲ mod ۵ ample،
would "۳ ⍰ ۵" expression the So، .۲ modulo addition indicate to used often is "⍰" symbol The follows: as evaluated be
a and ۴ of quotient a has ۲ by divided ۸ because is This ۰ = ۲ mod ۸ = ۲ mod (۳ + ۵) = ۳ ⍰ ۵ .۰ of remainder
cryptography، including mathematics، of areas different many in operation useful a is ۲ Modulo checking when example، for life، everyday in used also is It theory. number and science، computer odd. or even is number a whether
:۲ modulo of examples other some are Here
۱ = ۲ mod ۵ ۰ = ۲ mod ۴ ۱ = ۲ mod ۳ ۰ = ۲ mod ۲ ۱ = ۲ mod ۱

[۳] اثبات این مطلب از حوصله‌ی بحث خارج است.

ایجاد کرد. پس از ایجاد این حالت، تابع U_f را به حالت جدید اعمال می‌کنیم:

$$\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$$

این یک حالت استثنایی است! جملات مختلف کسر بالا حاوی اطلاعاتی در مورد f (۰) وf (۱) می‌باشند؛ به‌نحوی که انگار f (x) را برای دو مقدار x به طور همزمان ارزیابی کرده ایم، این ویژگی به "موازی سازی کوانتومی" موسوم می‌باشد. بر خلاف موازی سازی کلاسیک، که در آن هر یک مدارهای متعددی دارند ساخته شده برای محاسبه f (x) به طور همزمان اجرا می شوند، در اینجا برای ارزیابی تابع برای چندین مقدار x به طور همزمان، یک مدار f (x) (با قابلیت برهمنهی کوانتومی)استفاده می شود.

این فرآیند را می توان به راحتی با استفاده از یک عمل کلی به نام تبدیل هادامارد، به توابعی با تعداد بیت دلخواه تعمیم داد. این عمل فقط تعداد n گیت هادامارد است که به طور موازی روی n کوبیت عمل می کنند.

initially qubits with ۲ = n case the is ۱۸.۱ Figure in shown example، For prepared as ⍰۰|، which gives (|۰⍰ + |۱⍰√۲) (|۰⍰ + |۱⍰√۲) = |۰۰⍰ + |۰۱⍰ + |۱۰⍰ + |۱۱⍰ as output. ۲ (۳۸.۱)

برای مثال در شکل زیر؛ دو کیوبیت در حالت $|0\rangle$ آماده شده‌اند. پس از اعمال گیت‌های هادامارد بر روی این رجیستر به خروجی زیر خواهیم رسید:

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{\sqrt{2}}$$

از نماد H ⊗2 به عنوان نشانه‌ی عملکرد موازی دو گیت هادامارد استفاده می‌کنیم؛از علامت ⊗ به عنوان تانسور یاد می‌کنیم. به طور کلی نتایج اعمال موازی گیت هادامارد روی n کیوبیت روی حالت کوانتومی برابرست با:

$$\frac{1}{\sqrt{2}}\sum_{x}|x\rangle$$

denote to H⍰n write we and x، of values possible all over is sum the where superposition equal an produces transform Hadamard the is، That action. this efficiently، extremely this does it Moreover، states. basis computational all of producing a superposition of ۲n states using just n gates.

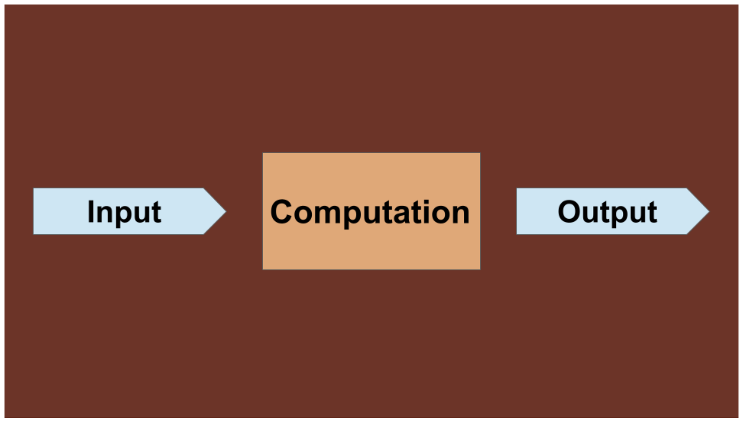
Figure ۱۸.۱. The Hadamard transform H⍰۲ on two qubits. Quantum paral- lel evaluation of a function with an n bit input x and ۱ bit output، f (x)، can thus

|۰⍰⍰n|۰⍰، state qubit ۱ + n the Prepare manner. following the in performed be quan- the by followed qubits، n first the to transform Hadamard the apply then . (x)⍰ |x⍰|f x ∑ √۲n ۱ state the produces This . Uf implementing circuit tum
(۴۰.۱)

func- the of values possible all enables parallelism quantum sense، some In evalu- only apparently we though even simultaneously، evaluated be to f tion single our In useful. immediately not is parallelism this However، once. f ated f ،۱| or ⍰(۰) f ،۰| either only gives state the of measurement example، qubit (x)⍰ f |x، x ∑ state the of measurement case، general the in Similarly، !⍰(۱) computer classical a course، Of x. of value single a for (x) f only give would just than more something requires computation Quantum easily! this do can information extract to ability the requires it useful؛ be to parallelism quantum (x)⍰. f |x، x ∑ like states superposition from (x) f of value one than more about done be may this how of examples investigate we sections two next the Over

۱.۱.۳ مدل محاسباتی استاندارد

پیش از بررسی مدل کوئری، مدل ساده و استاندارد محاسباتی را بررسی می‌کنیم. به تصویر زیر دقت کنید:



شکل ۲.۳: یک واحد محاسباتی که مقادیری را به عنوان ورودی گرفته، پردازش کرده و سپس مقدار/مقادیر خروجی را ارائه کرده است.

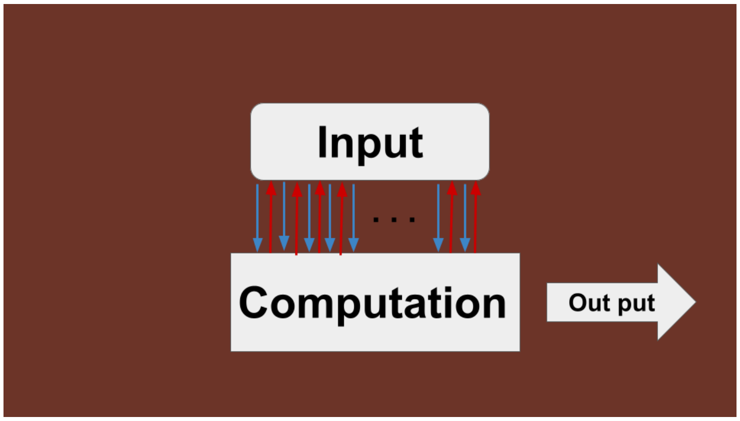
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان درنظر گرفت که ورودی داده شده و خروجی نهایی،هر دو در قالب یک رشته از اعداد باینری، ماتریس و یا هرقالب مدنظر کاربر باشند.

مهم‌ترین نکته درباره‌ی این واحد محاسباتی، **در دسترس بودن کل مقادیر ورودی برای واحد پردازش** است. به عبارت دیگر **واحد پردازش می‌تواند تمامی مقادیر ورودی را دریافت کرده و تشخیص** دهد.

۲.۱.۳ مدل کوئری

در مدل کوئری، داده‌های ورودی توسط یک تابع تولید می‌شوند. واحد محاسباتی دسترسی به تابع تولیدورودی دارد و می‌تواند برای دریافت داده‌های جدید،از تابع یاد شده،درخواست کند.

در این مدل واحد محاسباتی دیگر داده‌ها را در قالب رشته‌ای از اطلاعات دردسترس ندارد؛ بلکه می‌تواند آن‌ها را از بخش input دریافت کند. در گاهی از مواقع به سیستم oracle،input یا جعبه‌ی سیاه می‌گویند. تابع Oracle یا جعبه‌ی سیاه یک سیستم است که ما به عنوان ناظر به سازوکار داخلی آن و تمامی اطلاعات آن دسترسی نداریم و فقط می‌توانیم مقادیر مجاز را به آن داده و مقادیر خروجی را دریافت کنیم.



شکل ۳.۳: شکل بالا نمود مدل محاسباتی‌کوئری است. واحد محاسباتی برای دریافت داده‌های جدید نیاز به درخواست از تابع input دارد. خطوط قرمز و روبه‌بالا نشان از درخواست واحد محاسباتی و خطوط آبی روبه‌پایین نشان از پاسخ واحد inputمی‌باشد.

تابع oracle به صورت زیر تعریف می‌شود:

$$\begin{cases} f : \sum^n = \sum^m \\ Which : m, n \in \mathbb{N} \end{cases}$$

ما در این نظریه کوئری‌ها را می‌شماریم و وضعیت آن‌ها را بررسی می‌کنیم.

الگوریتم‌های کوانتومی

۲.۳ Algorithm Deutsch

books of combnation tell

۱.۲.۳ مسئله‌ی دوچ

الگوریتم Deutsch اولین و ساده‌ترین الگوریتم کوانتومی است. این الگوریتم برای اولین بار در سال ۱۹۸۵ در مقاله‌ای مطرح شد؛ که توسط دیوید دوچ[۴] نوشته شده‌بود. این الگوریتم نقطه‌ی شروعی برای

[۴] Deutsch David

اثبات برتری کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیک است.

مسئله‌ی Deutsch یکی از ساده‌ترین مفاهیم ممکن را مطرح می‌کند. اگر یک تابع به فرم زیر تعریف شود:

$$f : \sum \rightarrow \sum$$

هدف بررسی ثابت بودن یا متعادل[۵] بودن تابع f است. به‌طور کلی، درساده‌ترین حالت، می‌توان چهار وضعیت را برای تابع $f : \sum \rightarrow \sum$ درنظر گرفت:

$$\begin{array}{c|c} a & f_1(a) \\ \hline 0 & 0 \\ 1 & 0 \end{array} \qquad \begin{array}{c|c} a & f_2(a) \\ \hline 0 & 0 \\ 1 & 1 \end{array} \qquad \begin{array}{c|c} a & f_3(a) \\ \hline 0 & 1 \\ 1 & 0 \end{array} \qquad \begin{array}{c|c} a & f_4(a) \\ \hline 0 & 1 \\ 1 & 1 \end{array}$$

شکل ۴.۳:

در شکل بالا توابع f 1 ، f 4 توابع ثابت و توابع f 2 و f 3 توابع متعادل هستند.

مسئله‌ی دوچ	
ورودی	$f : \sum \rightarrow \sum$
خروجی	صفر اگر تابع ثابت بود؛ یک اگر تابع متعادل بود.

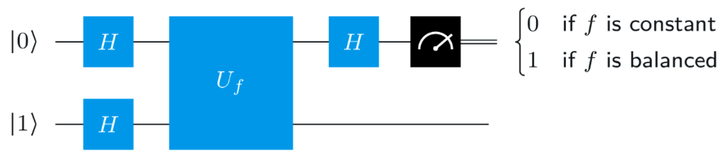
در الگوریتم‌های کلاسیک برای حل این مسئله، حداقل دو حالت باید بررسی شود.

۲.۲.۳ الگوریتم دوچ

حال به بررسی الگوریتم دوچ می‌پردازیم. الگوریتمی که مسئله‌ی دوچ را با یک مدار کوانتومی حل می‌کند:

---

[۵] balanse. or Constante



شکل ۵.۳:

$$
\begin{aligned}
|\pi_1\rangle =& |-\rangle|+\rangle = \frac{1}{2}(|0\rangle - |1\rangle)|0\rangle + \frac{1}{2}(|0\rangle - |1\rangle)|1\rangle \\
|\pi_2\rangle =& \frac{1}{2}(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle)|0\rangle + \frac{1}{2}(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)|1\rangle \\
=& \frac{1}{2}(-1)^{f(0)}(|0\rangle - |1\rangle)|0\rangle + \frac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle)|1\rangle \\
& |0 \oplus a\rangle - |1 \oplus a\rangle = (-1)^a(|0\rangle - |1\rangle)
\end{aligned}
$$

$$
\begin{aligned}
|\pi_1\rangle &= |-\rangle|+\rangle = \frac{1}{2}(|0\rangle - |1\rangle)|0\rangle + \frac{1}{2}(|0\rangle - |1\rangle)|1\rangle \\
|\pi_2\rangle &= \frac{1}{2}(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle)|0\rangle + \frac{1}{2}(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)|1\rangle \\
&= \frac{1}{2}(-1)^{f(0)}(|0\rangle - |1\rangle)|0\rangle + \frac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle)|1\rangle \\
&= |-\rangle \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right)
\end{aligned}
$$

$$
\begin{aligned}
|\pi_2\rangle &= |-\rangle \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right) \\
&= (-1)^{f(0)}|-\rangle \left(\frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}} \right) \\
&= \begin{cases} (-1)^{f(0)}|-\rangle|+\rangle & f(0) \oplus f(1) = 0 \\ (-1)^{f(0)}|-\rangle|-\rangle & f(0) \oplus f(1) = 1 \end{cases}
\end{aligned}
$$

$$|\pi_2\rangle = \begin{cases} (-1)^{f(0)}|-\rangle|+\rangle & f(0)\oplus f(1)=0 \\ (-1)^{f(0)}|-\rangle|-\rangle & f(0)\oplus f(1)=1 \end{cases}$$

$$\begin{aligned} |\pi_3\rangle &= \begin{cases} (-1)^{f(0)}|-\rangle|0\rangle & f(0)\oplus f(1)=0 \\ (-1)^{f(0)}|-\rangle|1\rangle & f(0)\oplus f(1)=1 \end{cases} \\ &= (-1)^{f(0)}|-\rangle|f(0)\oplus f(1)\rangle \end{aligned}$$

$$|\pi_3\rangle = (-1)^{f(0)}|-\rangle|f(0)\oplus f(1)\rangle$$

توضیحات رو بنویس

۳.۳ Algorithm Deutsch-Jozsa

۴.۳ oracle

site qiskit use

فصل ۴

شبیه‌سازی پدیده‌های کوانتومی

۱.۴ Bell states

در این بخش قصد داریم به بررسی پروتکل‌های ابتدایی در نظریه‌ی اطلاعات کوانتومی بپردازیم. تمامی این پروتکل‌ها به تعداد کمی کیوبیت نیاز دارند:؛ و در آزمایشگاه به صورت تجربی پیاده‌سازی شده‌اند. در اغلب موارد، سیستم از دو کیوبیت درهمتنیده تشکیل شده‌است. تابع حالت این سیستم‌ها به شکل زیر تعریف می‌شوند:

$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

برای آماده‌سازی این حالت کوانتومی، در حالت $|0\rangle$ داریم. با اعمال یک گیت هدامارد روی یکی از کیوبیت‌ها و سپس با کنترل آن با گیت CNOT، (به نحوی که کیوبیت دوم هدف قرارگیرد.) می‌توان به یک حالت درهمتنیده رسید. می‌توان این مراحل را به شکل زیر شرح داد:

$$|\psi_{00}\rangle = C_{10}H_1|00\rangle$$

$$|\psi_{xy}\rangle = C_{10}H_1|xy\rangle$$

از آنجایی که چهار حالت ⍰lxy یک مجموعه orthonormal هستند و دروازه‌های Hadamard و cNOT واحدی هستند، چهار حالت درهم تنیده ⍰xy⍰l نیز یک مجموعه orthonormal هستند، که به نام پایه Bell نامگذاری شده‌اند. حال یک دسته‌ی سه‌کیوبیتی را درنظر می‌گیریم:

$$|\psi_{xy}\rangle = C10H1X_1^xX_0^y|00\rangle$$

book؟؟ scince computer quantum of ۱۳۶ page of paragraph last

۲.۴ entanglement

۳.۴ coding dense super

scinse computer quntum

۴.۴ Teleport

book isac فرض کنید آلیس یک کیوبیت در حالت زیر دارد:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

کارول ممکن است با اعمال یک عملگر یکه به یک کیوبیت در حالت استاندارد، کیوبیت را از حالت $|0\rangle$ به حالت $|\psi\rangle$ تبدیل کرده باشد. کارول بدون اعلام نوع عملگر یکه به آلیس، کیوبیت را برای او ارسال می‌کند. حال آلیس می‌خواهد بدون دسترسی داشتن به کیوبیت باب، تغییراتی را در کیوبیت او ایجاد کند؛ این تنها درصورتی ممکن است که کیوبیت باب و آلیس درهمتنیده باشند. هرچند آلیس و باب می‌توانند از طریق راه‌های کلاسیک(نظیر تلفنی صحبت کردن و ...) با یکدیگر ارتباط برقرار کنند؛ ولی نمی‌توانند دسترسی مستقیم به کیوبیت یکدیگر داشته باشند.

کیوبیت باب را می‌توان به حالت زیر تعریف کرد: $|\phi\rangle = 1/\sqrt{2}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

============= اکنون تکنیک های چند صفحه آخر را برای درک چیزی غیرمعمول به کار خواهیم برد. پیش پا افتاده، غافلگیر کننده و بسیار سرگرم کننده - دوربری کوانتومی! تله پورت کوانتومی یک است تکنیک حرکت حالات کوانتومی به اطراف، حتی در غیاب ارتباط کوانتومی کانال nications که فرستنده حالت کوانتومی را به گیرنده پیوند می دهد. در اینجا نحوه عملکرد دوربری کوانتومی آمده است. آلیس و باب مدت ها پیش با هم آشنا شدند اما اکنون زندگی می کنند دور از هم. در حالی که آنها با هم یک جفت EPR تولید کردند که هر کدام یک کیوبیت از EPR را می گرفتند وقتی از هم جدا شدند جفت شوند سال‌ها بعد، باب مخفی است و ماموریت آلیس باید انجام شود او تصمیم می گیرد آن را بپذیرد، یعنی یک کیوبیت ⍰⍰| به باب تحویل دهد. او وضعیت را نمی داند کیوبیت، و علاوه بر این فقط می تواند اطلاعات کلاسیک را برای باب ارسال کند. آیا آلیس باید قبول کند ماموریت؟ به طور شهودی، همه چیز برای آلیس بسیار بد به نظر می رسد. او وضعیت ⍰⍰| آن را نمی داند کیوبیت او

باید برای باب بفرستد و قوانین مکانیک کوانتومی او را از این کار باز می دارد تعیین وضعیت زمانی که او فقط یک نسخه از ⍰⍰| در اختیار دارد. چه بدتر از آن، حتی اگر او حالت ⍰⍰| را می دانست، توصیف دقیق آن به مقدار بی نهایت نیاز دارد. اطلاعات کلاسیک از آنجایی که ⍰⍰| مقادیر را در یک فضای پیوسته می گیرد. بنابراین حتی اگر او انجام دهد بدانید ،⍰⍰| همیشه طول می کشد تا آلیس وضعیت را برای باب توصیف کند. نگاه نمی کند برای آلیس خوبه خوشبختانه برای آلیس، انتقال از راه دور کوانتومی راهی برای استفاده از آن است جفت EPR درهم به منظور ارسال ⍰⍰| به باب، تنها با سربار کوچک کلاسیک ارتباط به طور کلی، مراحل حل به شرح زیر است: آلیس با کیوبیت ⍰⍰| با نصف او از جفت ،EPR و سپس دو کیوبیت در اختیارش را اندازه گیری می کند و به دست می آورد یکی از چهار نتیجه کلاسیک ممکن، ۰۰، ۰۱، ۱۰، و ۱۱. او این اطلاعات را به باب بسته به پیام کلاسیک آلیس، باب یکی از چهار عمل خود را انجام می دهد نیمی از جفت .EPR به طرز شگفت انگیزی، با انجام این کار او می تواند حالت اولیه را بازیابی کند !⍰⍰| مدار کوانتومی نشان داده شده در شکل ۱۳.۱ توصیف دقیق تری از کوانتوم ارائه می دهد دوربری حالتی که باید از راه دور منتقل شود عبارت است از ⍰⍰| = ⍰۱|⍰+⍰۰|α که α و ⍰ ناشناخته هستند. دامنه ها حالت ورودی مدار ⍰۰⍰| است ⍰۰⍰| = ⍰۰۰⍰|⍰⍰|
۱ ‎۲√ [⍰۰۰|)⍰۰|α + ۱۱|⍰) + ⍰۰۰|)⍰۱|⍰ + ۱۱|⍰)] ، (۲۹.۱)

که در آن از این قرارداد استفاده می کنیم که دو کیوبیت اول (در سمت چپ) متعلق به آلیس هستند و کیوبیت سوم به باب. همانطور که قبلا توضیح دادیم، کیوبیت دوم آلیس و کیوبیت باب در حالت EPR شروع کنید. آلیس کیوبیت های خود را از طریق دروازه می فرستد و به دست می آورد ⍰۱⍰| = ۱ ‎۲√ [⍰۰۰|)⍰۰|α + ۱۱|⍰) + ⍰۱۰|)⍰۱|⍰ + ۰۱|⍰)] . (۳۰.۱) سپس اولین کیوبیت را از طریق دروازه هادامارد می فرستد و به دست می آورد ⍰۲⍰| = ۱ ۲ [⍰۰|)α + ۱|⍰)(۰۰|⍰ + ۱۱|⍰) + ⍰۰|)⍰ ۱|⍰)(۱۰|⍰ + ۰۱|⍰)] . (۳۱.۱) این حالت را می توان به روش زیر بازنویسی کرد، به سادگی با گروه بندی مجدد عبارات: ⍰۲⍰| = ۱ ۲ [۰۰|⍰ ⍰۰|α) + (⍰۱| + ۰۱|⍰ ⍰۱|α) + (⍰۰|⍰ ۱۰| + ⍰۱|α) - (⍰۱| + ۱۱|⍰ ⍰۱|α)] (⍰۰|⍰ . (۳۲.۱) این عبارت به طور طبیعی به چهار اصطلاح تقسیم می شود. عبارت اول دارای کیوبیت های آلیس است در حالت ۰۰|⍰ و کیوبیت باب در حالت ⍰۰|α + ⍰۱|⍰ - که حالت اصلی است. .⍰⍰| اگر آلیس یک اندازه گیری را انجام دهد و نتیجه ۰۰ را به دست آورد، سیستم باب این کار را انجام می دهد در حالت بودن .⍰⍰| به طور مشابه، از عبارت قبلی می‌توانیم پست باب را بخوانیم حالت اندازه گیری، با توجه به نتیجه اندازه گیری آلیس: ۰۰ ⍰_ ⍰۳ ⍰| (۰۰)⍰ ⍰ [⍰۰|α + ⍰۱|⍰] (۳۳.۱) ۰۱ ⍰_ ⍰۳ ⍰| (۰۱)⍰ ⍰ [۱|α + «۰|⍰] (۳۴.۱) ۱۰ ⍰_ ⍰۳ ⍰| (۱۰)⍰ ⍰ [⍰۰|α - ⍰۱|⍰] (۳۵.۱) ۱۱ ⍰_ ⍰۳ ⍰| (۱۱)⍰ ⍰ [⍰_ ⍰۱|α ⍰۰|⍰] . (۳۶.۱) بسته به نتیجه اندازه گیری آلیس، کیوبیت باب به یکی از این موارد ختم می شود چهار حالت ممکن البته برای اینکه بدانیم در کدام حالت است باید نتیجه را به باب گفت اندازه گیری آلیس - بعداً

نشان خواهیم داد که این واقعیت است که از دوربری جلوگیری می کند

رام برای انتقال اطلاعات سریعتر از نور استفاده می شود. وقتی باب این معنی را یاد گرفت در نتیجه، باب می‌تواند وضعیت خود را «تثبیت» کند، و با استفاده از روش مناسب |[illegible] بهبود یابد. دروازه کوانتومی به عنوان مثال، در موردی که اندازه گیری ۰۰ را به دست می آورد، باب این کار را نمی کند نیاز به انجام هر کاری اگر اندازه گیری ۰۱ باشد، باب می تواند با اعمال کردن حالت خود را اصلاح کند دروازه X اگر اندازه گیری ۱۰ باشد، باب می تواند وضعیت خود را با اعمال Z ثابت کند دروازه. اگر اندازه‌گیری ۱۱ باشد، باب می‌تواند با اعمال ابتدا یک X و حالت خود را اصلاح کند سپس یک دروازه .Z به طور خلاصه، باب باید تبدیل ZM۱ XM۲ را اعمال کند (به چگونگی آن توجه کنید زمان در نمودارهای مداری از چپ به راست می‌رود، اما در سمت راست در محصولات ماتریسی می‌رود اول اتفاق می افتد) به کیوبیت او، و او حالت |[illegible] را بازیابی می کند. بسیاری از ویژگی های جالب تله پورت وجود دارد که به برخی از آنها اشاره خواهیم کرد به بعد در کتاب. در حال حاضر به اظهار نظر در مورد چند مورد بسنده می کنیم جنبه های. اولا، آیا تله‌پورتاسیون به فرد اجازه نمی‌دهد حالت‌های کوانتومی را سریع‌تر از آن ارسال کند سبک؟ این امر نسبتاً عجیب و غریب خواهد بود، زیرا نظریه نسبیت نشان می دهد که سریعتر از انتقال اطلاعات نور می توان برای ارسال اطلاعات به عقب در زمان استفاده کرد. خوشبختانه، تله‌پورت کوانتومی امکان ارتباط سریع‌تر از نور را فراهم نمی‌کند. زیرا برای تکمیل دوربری، آلیس باید نتیجه اندازه گیری خود را به آن ارسال کند باب از طریق یک کانال ارتباطی کلاسیک.

ما در بخش ۳.۴.۲ نشان خواهیم داد که بدون این ارتباط کلاسیک، از راه دور هیچ اطلاعاتی را منتقل نمی کند. کانال کلاسیک با سرعت نور محدود می شود، بنابراین نتیجه می شود که تله پورت کوانتومی نمی تواند سریعتر از سرعت نور انجام شود و پارادوکس ظاهری را حل کند. معمای دوم در مورد تلهپورتاسیون این است که به نظر می رسد یک کپی از حالت کوانتومی در حال انتقال از راه دور ایجاد می کند، که آشکارا قضیه عدم شبیه سازی مورد بحث در بخش ۵.۳.۱ را نقض می کند. این نقض فقط توهمی است زیرا پس از فرآیند انتقال از راه دور فقط کیوبیت هدف در حالت |[illegible] باقی می ماند و کیوبیت داده اصلی بسته به نتیجه اندازه گیری به یکی از حالت های پایه محاسباتی |۰ یا |۱ می رسد. در کیوبیت اول از تله پورت کوانتومی چه چیزی می توانیم یاد بگیریم؟ خیلی زیاد! این خیلی بیشتر از یک ترفند ساده است که می توان با حالت های کوانتومی انجام داد. تله پورت کوانتومی بر قابلیت تعویض منابع مختلف در مکانیک کوانتومی تاکید می کند و نشان می دهد که یک جفت EPR مشترک به همراه دو بیت کلاسیک ارتباط، منبعی حداقل برابر با یک کیوبیت ارتباط است. محاسبات کوانتومی و اطلاعات کوانتومی روش‌های زیادی را برای تبادل منابع نشان داده‌اند که بسیاری از آنها بر اساس تله‌پورت کوانتومی ساخته شده‌اند. به طور خاص، در فصل ۱۰ توضیح می دهیم که چگونه می توان از تله پورت برای ساخت دروازه های کوانتومی مقاوم در برابر اثرات نویز استفاده کرد و در فصل ۱۲ نشان دادیم که انتقال از راه دور با ویژگی های کدهای تصحیح خطای کوانتومی ارتباط نزدیکی دارد.

علیرغم این ارتباط با موضوعات دیگر، منصفانه است که بگوییم که ما تازه در حال درک این موضوع هستیم که چرا انتقال از راه دور کوانتومی در مکانیک کوانتومی امکان پذیر است. در فصل‌های بعدی سعی می‌کنیم برخی از بینش‌هایی را توضیح دهیم که چنین درکی را ممکن می‌سازد. ۱

oracle a determine to how