

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	۲۰
۲.۱.۳	مدل کوثری	۲۰
۲.۳	Algorithm Deutsch	۲۱
۱.۲.۳	مسئله‌ی دوچ	۲۱
۲.۲.۳	الگوریتم دوچ	۲۲

۲۵	Algorithm Deutsch - Jozsa	۳.۳
۲۵	oracle	۴.۳
۲۷	شبیه‌سازی پدیده‌های کوانتومی	۴
۲۷	states Bell	۱.۴
۲۸	entanglement	۲.۴
۲۸	coding dense super	۳.۴
۲۸	Teleport	۴.۴

۱.۰ مقدمه

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

۲.۰ basis superpos vs comp

Consider the circuit shown in Figure ۱۷.۱, which applies U_f to an input not in superposition. Instead, the computational basis state $|0\rangle$ is prepared in the register. The Hadamard gate acts on the position $|0\rangle$ to create the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, which we then apply U_f to. The resulting state is:

فصل ۱

آشنایی با مفاهیم اولیه

۱.۱ کیوبیت

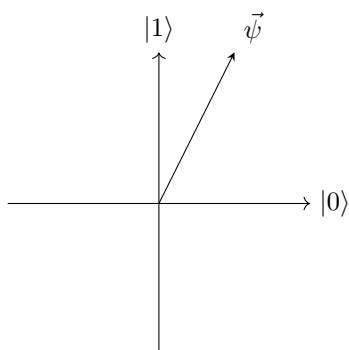
یک کیوبیت^۱، معادل یک واحد اطلاعات کوانتومی می‌باشد. این مفهوم معادل مفهوم کلاسیک بیت^۲ می‌باشد. به طور کلی هر کیوبیت حاوی دو بیت اطلاعات است. برای تبیین یک کیوبیت از خصوصیات سامانه های کوانتومی، بهره می‌بریم. کیوبیت یک سیستم کوانتومی با فضای دوبعدی است. برای تعیین این دوبعد می‌توان از یکی از خصوصیات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

برخلاف بیت ها که مقادیر ثابت ۰ یا ۱ را به خود می‌گیرند؛ یک کیوبیت می‌تواند در یک حالت «برهمتهی 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 برهمتهی، به شرح زیر است:

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

^۱Qubit
^۲Bit Binary

کت‌ها $|0\rangle$ و $|1\rangle$ 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:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (۱.۱)$$

برای تعریف کیوبیت‌ها، راه‌های زیادی وجود دارد، حالات قطبش فوتون، اسپین الکترون، یا سطوح انرژی اتم، هر یک می‌توانند تعیین‌کننده‌ی 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 درهم‌نهی 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 به یک حالت درهم‌نهی کوانتومی گذار می‌کند. به عبارت دیگر هر یک از زیرحالات این حالت درهم‌نهی، با احتمال یکسانی قابل رخ دادن هستند.

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

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

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

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

^۵Hadamard gate

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

این گیت کوانتومی، یک گیت بازگشت پذیر است؛ یعنی اگر این گیت روی یک حالت کوانتومی اثر کند؛ می تواند آن را از حالت برهنه بی خارج کند.

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

نمایش این گیت کوانتومی در مدار با علامت زیر است:



گیت CNOT

گیت کوانتومی CNOT^۶، به عنوان گیت منطقی، یاد می شود. این گیت کوانتومی معادل گیت NOT کلاسیک می باشد. به طور 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» می شود.

کیوبیت کنترل: کیوبیت هدف:

خلاصه ای از عملکرد این تابع به شرح زیر است:

ببین چرا از این نماد به جای تَنسور پُراداکت استفاده شده

$ A\rangle$	$ B\rangle$		$ A\rangle$	$ B \oplus A\rangle$
$ \text{control}\rangle$	$ \text{target}\rangle$	Effect CNOT Gate	$ \text{control}\rangle$	$ \text{target}\rangle$
$ 0\rangle$	$ 0\rangle$	\Rightarrow	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	\Rightarrow	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	\Rightarrow	$ 1\rangle$	$ 0\rangle$
$ 1\rangle$	$ 1\rangle$	\Rightarrow	$ 1\rangle$	$ 1\rangle$

نمایش ماتریسی این گیت کوانتومی به شکل زیر است:

gate controlled-X or gate controlled-NOT^۶

Qubit Controlled^۷

Qubit Target^۸

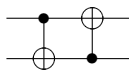
اینا باید اصلاح بشه

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

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

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

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 زیر است:

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 به کار 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 بردارهای 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 زیر است:

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.

^۹gate shift Phase

^{۱۰}gate Rotation

^{۱۱}circuit quantum

شباهت ها و تفاوت های مدارهای کلاسیک و کوانتومی

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

Sure, here are some similarities and differences between quantum circuits

and classical circuits:

****Similarities:****

* Both quantum and classical circuits are composed of a sequence of operations represented by gates. * Both quantum and classical circuits can be used to implement algorithms. * Both quantum and classical circuits use graphical notation.

****Differences:****

* Quantum circuits use qubits, while classical circuits use bits. * Quantum circuits can exploit quantum properties such as superposition and entanglement, while classical circuits cannot. * Quantum circuits are reversible, while classical circuits are not. * Quantum circuits can perform tasks that are impossible for classical computers to perform.

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

and classical circuits:

Feature	Quantum Circuit	Classical Circuit	Basic Unit of Data
Reversibility	Reversible	Irreversible	Bit
Logic gates	Quantum gates	Logic gates	Qubit
Operations	Exploits quantum mechanics	No	Yes
Simulating databases, unsorted searching integers, Factoring, tasks	Yes	No	Yes
Logical calculating, Sorting, systems	Yes	No	Yes

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

اجزای مدارهای کوانتومی و ساینز 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 کامپیوترهای کوانتومی 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

موازی سازی کوانتومی^۱، پایه و اساس بسیاری از الگوریتم‌های کوانتومی است. با گذار یک حالت کوانتومی به حالت برهمه‌ی 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 تک-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 می‌شود. با یک توالی مناسب از گیت‌های منطقی می‌توان این حالت را به

^۱parallelism Quantum

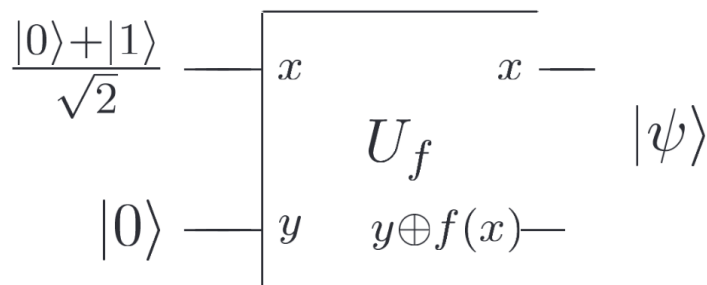
$|f(x) \oplus x, y\rangle$ تبدیل کرد که در آن \oplus بیانگر جمع مدوله با پایه ۲ می‌باشد.

۲

هریک از دسته‌های کیویت، رجیستر کوانتومی نامیده می‌شوند. اولین رجیستر، «رجیستر داده» و دومین رجیستر «رجیستر هدف» نامیده می‌شود.

ازین پس در این بخش به عامل گذار $|x, y \oplus f(x)\rangle \rightarrow |x, y\rangle$ ، عنوان «تابع U_f » را اطلاق خواهیم کرد. لازم به ذکر است که این تبدیل، یک تبدیل یک به یک به شمار می‌آید.^۳

اگر $y = 0$ آنگاه مقدار دومین کیویت 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. U_f مدار کوانتومی است که ورودی‌هایی مانند $|x, y\rangle$ را به $|x, y \oplus f(x)\rangle \rightarrow |x, y\rangle$ ، تصویر می‌کند.

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

Modulo ۲ is a mathematical operation that returns the remainder of a division. For example, ۲ divided by ۵ has a remainder of ۲, so ۲ mod ۵ = ۲. This operation is useful in 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

Here are some other examples of modulo ۲:

$$۱ = ۱ \bmod ۲, ۰ = ۰ \bmod ۲, ۳ = ۱ \bmod ۲, ۴ = ۰ \bmod ۲, ۵ = ۱ \bmod ۲$$

^۳اثبات 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 $f(0)$ و $f(1)$ می‌باشند؛ به نحوی که انگار $f(x)$ را برای دو مقدار x به طور همزمان ارزیابی کرده ایم، این ویژگی به ”موازی سازی کوانتومی“ موسوم می‌باشد. برخلاف موازی سازی کلاسیک، که در آن هر یک مدارهای متعددی دارند ساخته شده برای محاسبه $f(x)$ به طور همزمان اجرا می‌شوند، در اینجا برای ارزیابی تابع برای چندین مقدار x به طور همزمان، یک مدار $f(x)$ (با قابلیت برهمه‌نی کوانتومی) استفاده می‌شود. این فرآیند را می‌توان 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 کیوبیت عمل می‌کنند.

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:

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

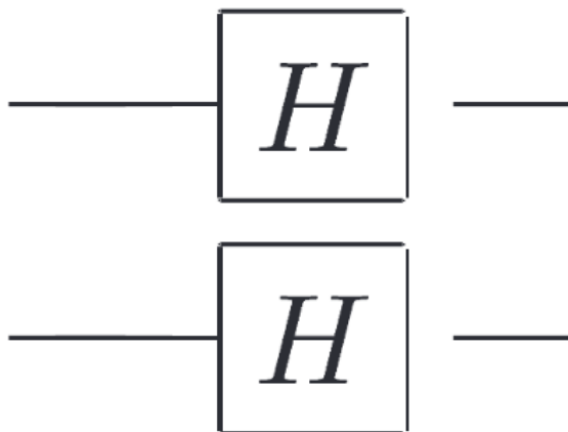
از نماد $H \otimes 2$ به عنوان نشانه‌ی عملکرد موازی دو گیت هادامارد استفاده می‌کنیم؛ از علامت \otimes به عنوان تانسور یاد می‌کنیم. به طور کلی نتایج اعمال موازی گیت هادامارد روی n کیوبیت روی حالت کوانتومی برابرست با:

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

در اینجا، \sum نشان دهنده جمع بر روی همه مقادیر ممکن x است، و $H \otimes n$ را برای نشان دادن این عمل می‌نویسیم. اعمال تبدیل هادامارد روی یک بهمنهی کوانتومی برابر از همه حالت‌های محاسباتی تولید می‌کند؛ و با استفاده از فقط n گیت، یک بهمنهی از $2n$ حالت تولید می‌کند.

تبدیل هادامارد $H \otimes 2$ روی دو بیت کوانتومی پیاده می‌شود. ارزیابی موازی کوانتومی یک تابع $f(x)$ با ورودی n بیتی x و خروجی ۱ بیتی، به روش زیر قابل پیاده‌سازی می‌باشد:

۱. ابتدا حالت $n + 1$ کیوبیت $|0\rangle^{\otimes n} |0\rangle$ را آماده کنید،



شکل ۲.۳: اعمال تبدیل هادامارد $H \otimes n$ روی دو کیوبیت

۲. سپس تبدیل هادامارد را به n کیوبیت اول و به دنبال آن مدار کوانتومی اعمال کنید.

۳. اعمال تابع U_f به کیوبیت‌هایی که در حالت برهم‌نهی قرار دارند.

در نهایت حالت زیر تولید می‌شود:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

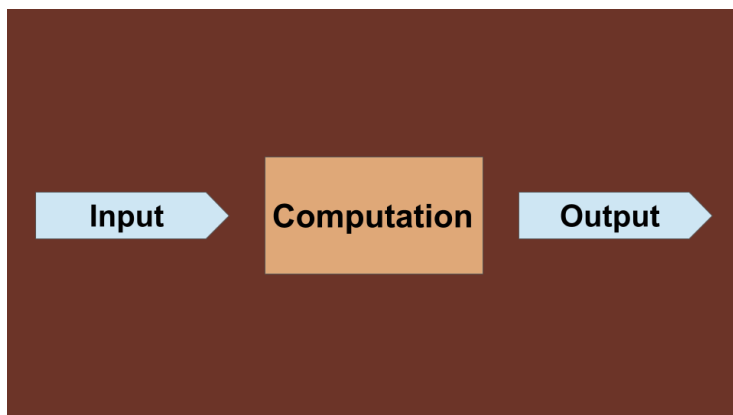
$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

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 $|f(x)\rangle$ either only gives state the of measurement example, qubit
 $|f(x)\rangle$ f $|x\rangle$ state the of measurement case, general the in Similarly, $|f(x)\rangle$
 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
 $|f(x)\rangle$ f $|x\rangle$ 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

به طور کلی موازی سازی کوانتومی امکان ارزیابی همزمان همه مقادیر ممکن تابع f را فراهم می کند، حتی اگر ظاهراً فقط یک بار f را ارزیابی کرده باشیم. با این حال، این موازی سازی بلافاصله مفید نیست. در مثال تک کویتی ما، اندازه گیری حالت فقط $f(0)$ یا $f(1)$ را می دهد! به طور مشابه، در حالت کلی، اندازه گیری حالت $\sum x$ ، $f(x)$ فقط $f(x)$ را برای یک مقدار x خاص می دهد. البته یک کامپیوتر کلاسیک می تواند این کار را به راحتی انجام دهد! محاسبات کوانتومی برای مفید بودن به چیزی بیش از موازی سازی کوانتومی نیاز دارد؛ به توانایی استخراج اطلاعات مربوط به بیش از یک مقدار $f(x)$ از حالت های سوپروپوزیسیون مانند $\sum x$ ، $f(x)$ نیاز دارد. در دو بخش بعدی ما به بررسی مثال هایی از نحوه انجام این کار می پردازیم.

۱.۱.۳ مدل محاسباتی استاندارد

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



شکل ۳.۳: یک واحد محاسباتی که مقداری را به عنوان ورودی گرفته، پردازش کرده و سپس مقدار/مقادیر خروجی را ارائه کرده است.

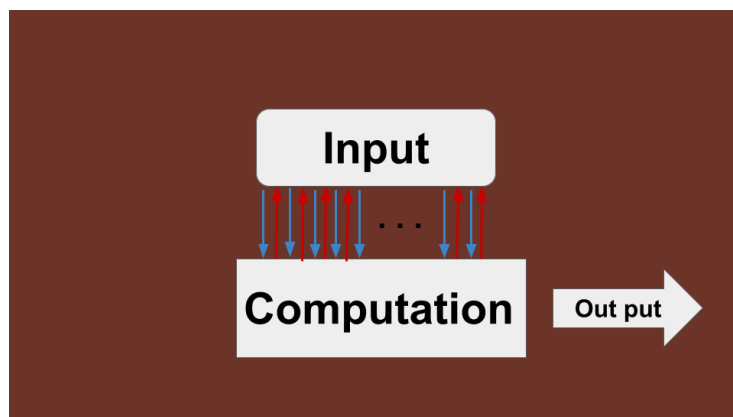
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان در نظر گرفت که ورودی داده شده و خروجی نهایی، هر دو در قالب یک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

در مدل کوثری، داده‌های ورودی توسط یک تابع تولید می‌شوند. واحد محاسباتی دسترسی به تابع تولید ورودی 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 در دسترس 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 ۴.۳: نمودار مدل محاسباتی کوثری 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 input می‌باشد.

تابع oracle به صورت زیر تعریف می‌شود:

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

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

الگوریتم‌های کوانتومی

Algorithm Deutsch ۲.۳

books of combination 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 شده بود. این الگوریتم نقطه‌ی شروعی برای

^۴Deutsch 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:

$$f : \Sigma \rightarrow \Sigma$$

هدف بررسی ثابت بودن یا متعادل^۵ بودن تابع f است. به‌طور کلی، در ساده‌ترین حالت، می‌توان چهار وضعیت را برای تابع $f : \Sigma \rightarrow \Sigma$ در نظر گرفت:

a	$f_1(a)$	a	$f_2(a)$	a	$f_3(a)$	a	$f_4(a)$
0	0	0	0	0	1	0	1
1	0	1	1	1	0	1	1

شکل ۵.۳:

در شکل بالا توابع f_1 ، f_4 توابع ثابت و توابع f_2 و f_3 توابع متعادل هستند.

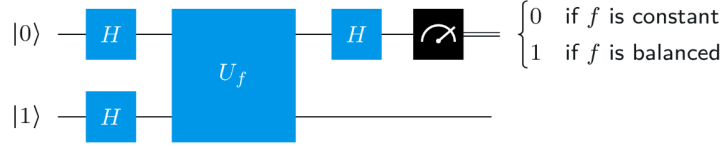
مسئله‌ی دوچ	
ورودی	$f : \Sigma \rightarrow \Sigma$
خروجی	صفر اگر تابع ثابت بود؛ یک اگر تابع متعادل بود.

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:

^۵balance. or Constante



شكل ٦.٣:

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

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

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

$$\begin{aligned}
 |\pi_2\rangle &= \begin{cases} (-1)^{f(0)}|-\rangle|+\rangle & f(0) \oplus f(1) = 0 \\ (-1)^{f(0)}|-\rangle|-\rangle & f(0) \oplus f(1) = 1 \end{cases} \\
 |\pi_3\rangle &= \begin{cases} (-1)^{f(0)}|-\rangle|0\rangle & f(0) \oplus f(1) = 0 \\ (-1)^{f(0)}|-\rangle|1\rangle & f(0) \oplus f(1) = 1 \end{cases} \\
 &= (-1)^{f(0)}|-\rangle|f(0) \oplus f(1)\rangle \\
 |\pi_3\rangle &= (-1)^{f(0)}|-\rangle|f(0) \oplus f(1)\rangle
 \end{aligned}$$

توضیحات رو بنویس

Algorithm Deutsch - Jozsa ۳.۳

oracle ۴.۳

site qiskit use

فصل ۴

شبیه‌سازی پدیده‌های کوانتومی

۱.۴ states Bell

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 $|xy\rangle$ یک مجموعه orthonormal هستند و دروازه‌های Hadamard و CNOT واحدی هستند، چهار حالت درهم‌تنیده $|\psi_{xy}\rangle$ نیز یک مجموعه orthonormal هستند، که به نام پایه Bell نامگذاری شده‌اند. حال یک دسته‌ی سه کیوبیتی را در نظر می‌گیریم:

$$|\psi_{xy}\rangle = C_{10}H_1X_1^xX_0^y|00\rangle$$

book?? science computer quantum of ۱۳۶ page of paragraph last

۲.۴ entanglement

۳.۴ coding dense super

science computer quantum

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 در صورتی 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 غیر معمول 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 سال ها بعد، باب مخفی است و ماموریت آلیس باید انجام شود او تصمیم می گیرد آن را بپذیرد، یعنی یک کیوبیت [۹۹] 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 [۹۹] آن را نمی داند کیوبیت او

که در آن از این قرارداد استفاده می کنیم که دو کیبیت اول (در سمت چپ) متعلق به آلیس هستند و کیبیت سوم به باب. همانطور که قبلاً توضیح دادیم، کیبیت دوم آلیس و کیبیت باب در حالت EPR شروع کنید. آلیس کیبیت های خود را از طریق دروازه می فرستد و به دست می آورد $|\psi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$ (۳۰.۱). سپس اولین کیبیت را از طریق دروازه هادامارد می فرستد و به دست می آورد $|\psi\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ (۳۱.۱). این حالت را می توان به روش زیر بازنویسی کرد، به سادگی با گروه بندی مجدد عبارات: $|\psi\rangle = \frac{1}{2} (|00\rangle + |10\rangle + |01\rangle + |11\rangle)$ (۳۲.۱). این عبارت به طور طبیعی به چهار اصطلاح تقسیم می شود. عبارت اول دارای کیبیت های آلیس است در حالت $|00\rangle$ و کیبیت باب در حالت $|00\rangle + |10\rangle$ - که حالت اصلی است. $|\psi\rangle$ 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. $|\psi\rangle$ به طور مشابه، از عبارت قبلی می توانیم پست باب را بخوانیم حالت اندازه گیری، با توجه به نتیجه اندازه گیری آلیس: $|\psi\rangle = \frac{1}{2} (|00\rangle + |10\rangle + |01\rangle + |11\rangle)$ (۳۳.۱) $|\psi\rangle = \frac{1}{2} (|00\rangle + |10\rangle + |01\rangle + |11\rangle)$ (۳۴.۱) $|\psi\rangle = \frac{1}{2} (|00\rangle + |10\rangle + |01\rangle + |11\rangle)$ (۳۵.۱) $|\psi\rangle = \frac{1}{2} (|00\rangle + |10\rangle + |01\rangle + |11\rangle)$ (۳۶.۱). بسته به نتیجه اندازه گیری آلیس، کیبیت 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 می‌کند

رام برای انتقال اطلاعات سریعتر از نور استفاده می‌شود. وقتی باب این معنی را یاد گرفت در نتیجه، باب می‌تواند وضعیت خود را «تثبیت» کند، و با استفاده از روش مناسب [۹۴] بهبود یابد. دروازه کوانتومی به عنوان مثال، در موردی که اندازه‌گیری ۰۰ را به دست می‌آورد، باب این کار را نمی‌کند نیاز به انجام هر کاری اگر اندازه‌گیری ۰۱ باشد، باب می‌تواند با اعمال کردن حالت خود را اصلاح کند دروازه X اگر اندازه‌گیری ۱۰ باشد، باب می‌تواند 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 $XM_2 ZM_1$ 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 می‌افتد) به کیوبیت او، و او حالت [۹۴] را بازیابی می‌کند. بسیاری از ویژگی‌های 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 می‌کنیم جنبه‌های. اولاً، 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 می‌دهد که سریعتر از انتقال اطلاعات نور می‌توان 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 اندازه‌گیری 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 نمی‌کند. کانال کلاسیک با سرعت نور محدود می‌شود، بنابراین نتیجه می‌شود که تله پورت کوانتومی نمی‌تواند سریعتر از سرعت نور انجام شود و پارادوکس ظاهری را حل کند. معمای دوم در مورد تله‌پورتاسیون این است که به نظر می‌رسد یک کپی از حالت کوانتومی در حال انتقال از راه دور ایجاد می‌کند، که آشکارا قضیه عدم شبیه‌سازی مورد بحث در بخش ۵.۳.۱ را نقض می‌کند. این نقض فقط توهمی است زیرا پس از فرآیند انتقال از راه دور فقط کیوبیت هدف در حالت [۹۴] باقی می‌ماند و کیوبیت داده اصلی بسته به نتیجه اندازه‌گیری به یکی از حالت‌های پایه محاسباتی ۰۱ یا ۱۱ می‌رسد. در کیوبیت اول از تله پورت کوانتومی چه چیزی می‌توانیم یاد بگیریم؟ خیلی زیاد! این خیلی بیشتر از یک ترفند ساده است که می‌توان با حالت‌های کوانتومی انجام داد. تله پورت کوانتومی بر قابلیت تعویض منابع مختلف در مکانیک کوانتومی تاکید می‌کند و نشان می‌دهد 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 می‌دهیم که چگونه می‌توان از تله پورت برای ساخت دروازه‌های کوانتومی مقاوم در برابر اثرات نویز استفاده کرد و در فصل ۱۲ نشان دادیم که انتقال از راه دور با ویژگی‌های 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