

فهرست مطالب

۲	۱.۰ مقدمه
۲	۲.۰ basis superpos vs comp
۳	۱ آشنایی با مفاهیم اولیه
۳	۱.۱ کیوبیت
۴	۲.۱ basis fourier - basis computayional - vector bloch
۴	۳.۱ گیت‌های کوانتومی
۵	۱.۳.۱ انواع گیت کوانتومی
۸	۲.۳.۱ gate Swap
۸	۴.۱ مدارهای کوانتومی
۱۱	۱.۴.۱ نحوه‌ی نمایش مدارهای کوانتومی
۱۳	۲ برنامه‌نویسی کوانتومی
۱۳	۱.۲ تفاوت کامپیوتر کلاسیک و کوانتومی
۱۳	۲.۲ Qiskit and computer Quantum IBM
۱۵	۳ الگوریتم‌های کوانتومی
۱۵	۱.۳ موازی سازی کوانتومی
۱۹	۱.۱.۳ مدل محاسباتی استاندارد
۱۹	۲.۳ مدل کوثری
۲۰	۳.۳ Algorithm Deutsch
۲۰	۱.۳.۳ مسئله‌ی دوچ
۲۱	۲.۳.۳ الگوریتم دوچ

۴.۳	الگوریتم دوچ - جوزا	۲۴
۵.۳	oracle	۲۸
۶.۳	simulation vs comp	۲۹
۴	شبیه سازی پدیده های کوانتومی	۳۱
۱.۴	states Bell	۳۱
۲.۴	entanglement	۳۲
۳.۴	coding dense super	۳۲
۴.۴	Teleport	۳۲

۱.۰ مقدمه

در عصر حاضر بواسطه ی رشد و توسعه ی نظریه ی اطلاعات کوانتومی و سرمایه گذاری 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

book chuang ۱ Chapter

Consider the circuit shown in Figure ۱۷.۱, which applies U_f to an input not in the computational basis. Instead, the data register is prepared in the superposition state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, which can be created with a Hadamard gate acting on the state $|0\rangle$. Then we apply U_f to the resulting state:

فصل ۱

آشنایی با مفاهیم اولیه

۱.۱ کیوبیت

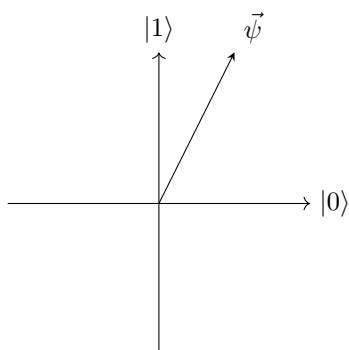
یک کیوبیت^۱، معادل یک واحد اطلاعات کوانتومی می‌باشد. این مفهوم معادل مفهوم کلاسیک بیت^۲ می‌باشد. به طور کلی هر کیوبیت حاوی دو بیت اطلاعات است. برای تبیین یک کیوبیت از خصوصیات سامانه های کوانتومی، بهره می‌بریم. کیوبیت یک سیستم کوانتومی با فضای دوبعدی است. برای تعیین این دوبعد می‌توان از یکی از خصوصیات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

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

Qubit^۱
Bit Binary^۲

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 پراداکت 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

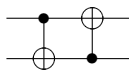
اینا باید اصلاح بشه

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

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

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

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

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		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 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 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 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

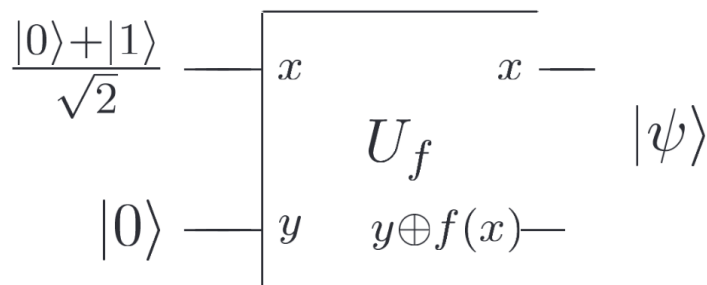
$|f(x) \oplus x, y\rangle$ تبدیل کرد که در آن \oplus بیانگر جمع مدوله با پایه ۲ می‌باشد.

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 برهم‌نهی قرار دارد. این حالت برهم‌نهی را می‌توان با اعمال گیت هادامارد بر حالت کوانتومی $|0\rangle$

Modulo ۲ is a mathematical operation that returns the remainder of a division by ۲. For example, ۵ divided by ۲ has a remainder of ۱, so ۵ mod ۲ = ۱. 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 follows: as evaluated be

cryptology, 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:

$$1 = 1 \bmod 2, 2 = 0 \bmod 2, 3 = 1 \bmod 2, 4 = 0 \bmod 2, 5 = 1 \bmod 2$$

^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 برهمه‌ی 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:

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

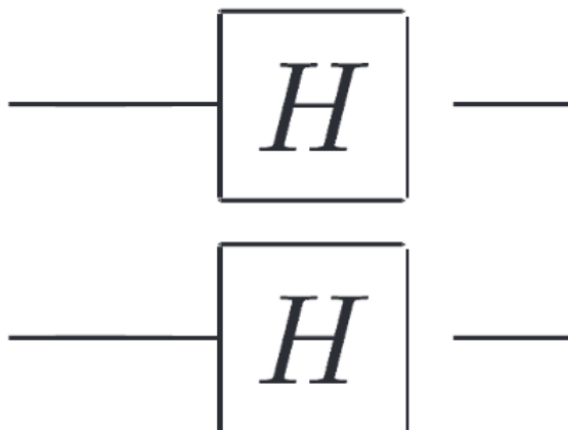
از نماد $H \otimes 2$ به عنوان نشانه‌ی عملکرد موازی دو گیت هادامارد استفاده می‌کنیم؛ از علامت \otimes به عنوان تانسور یاد می‌کنیم. به طور کلی نتایج اعمال موازی گیت هادامارد روی n کیوبیت روی حالت کوانتومی برابرست با:

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

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 برهمه‌نی قرار دارند.

در نهایت حالت زیر تولید می‌شود:

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

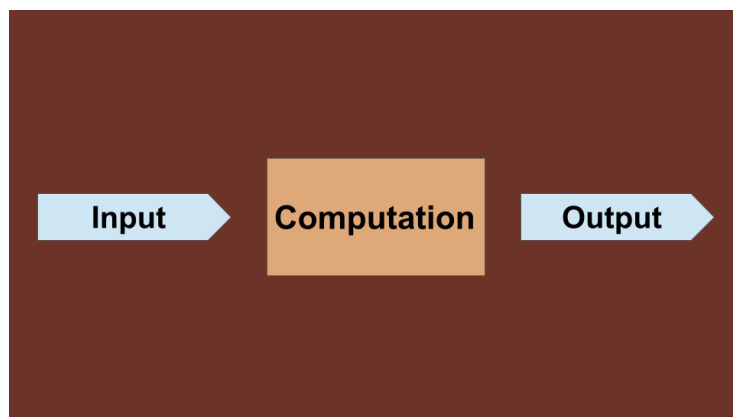
$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

به طور کلی موازی‌سازی کوانتومی امکان ارزیابی همزمان همه مقادیر ممکن تابع f را فراهم می‌کند، حتی اگر ظاهراً فقط یک بار f را ارزیابی کرده باشیم. با این حال، این موازی‌سازی بلافاصله مفید نیست. در مثال تک کیوبیتی ما، اندازه‌گیری حالت فقط $|0, f(0)\rangle$ یا $|1, f(1)\rangle$ را می‌دهد! به طور مشابه، در حالت کلی، اندازه‌گیری حالت $\sum_x |x\rangle |f(x)\rangle$ فقط $f(x)$ را برای یک مقدار x خاص می‌دهد. البته یک کامپیوتر کلاسیک می‌تواند این کار را به راحتی انجام دهد! محاسبات کوانتومی برای مفید بودن به چیزی بیش از موازی‌سازی کوانتومی نیاز دارد؛ به توانایی استخراج اطلاعات مربوط به بیش از یک مقدار $f(x)$ از حالت‌های سوپروپوزیسیون مانند $\sum_x |x\rangle |f(x)\rangle$ نیاز دارد. در بخش‌های بعدی به مثال‌های خواهیم پرداخت که این مسائل را حل کند.

$$\sum_x |x, f(x)\rangle$$

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 مقادیری را به عنوان ورودی گرفته، پردازش کرده و سپس مقدار/مقادیر خروجی را ارائه کرده است.

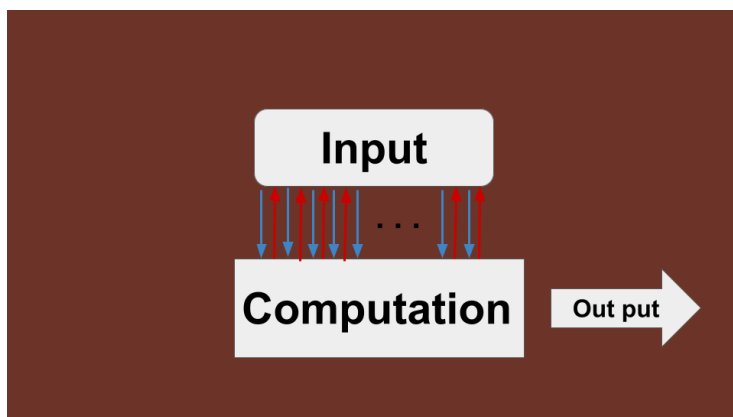
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان در نظر گرفت که ورودی داده شده و خروجی نهایی، هر دو در قالب یک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

۲.۳ 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



شکل ۴.۳: شکل بالا نمود 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.

دریافت کنیم.

تابع oracle به صورت زیر تعریف می‌شود:

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

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

۳.۳ Algorithm Deutsch

books of combnation tell

۱.۳.۳ 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 اثبات برتری کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیک است.

^۴Deutsch David

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:

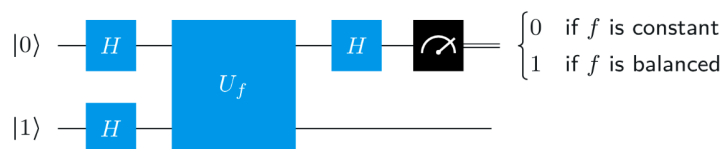
در شکل بالا توابع f_1 ، f_4 توابع ثابت و توابع f_2 و f_3 توابع متعادل هستند.

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.

۲.۳.۳ الگوریتم دوچ

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



شکل ۶.۳:

^۵ balanse. or Constante

یک تغییر ساده در مدار شکل ۳.۱ نشان می‌دهد که چگونه مدارهای کوانتومی می‌توانند با پیاده سازی الگوریتم Deutsch از مدارهای کلاسیک پیشی بگیرند.^۶ الگوریتم Deutsch ترکیبی از موازی سازی کوانتومی با خاصیتی از مکانیک کوانتوم به نام تداخل^۷

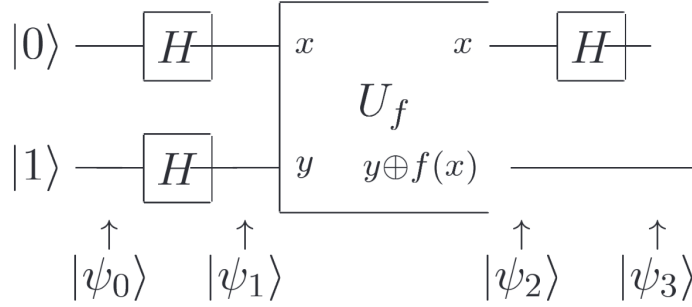
the as qubit first the prepare to gate theHadamard use us let before. As the as y qubit second the prepare us let now but , $\frac{1}{\sqrt{2}}(|\psi_1\rangle + |\psi_0\rangle)$ superposition . $\frac{1}{\sqrt{2}}(|\psi_1\rangle - |\psi_0\rangle)$ superposition a using , $\frac{1}{\sqrt{2}}(|\psi_1\rangle - |\psi_0\rangle)$ state the to applied gate Hadamard in shown circuit, this in happens what see to along states the follow us Let

۱۹.۱ Figure

است. مشابه قبل، ابتدا از گیت هادامارد برای آماده سازی اولین کویت به عنوان superposition $\frac{1}{\sqrt{2}}(|\psi_1\rangle + |\psi_0\rangle)$ استفاده کنیم، اما اکنون کویت دوم y را با اعمال یک گیت هادامارد به حالت $|\psi_1\rangle$ به عنوان superposition $\frac{1}{\sqrt{2}}(|\psi_1\rangle - |\psi_0\rangle)$ آماده کنیم. به شکل زیر دقت کنید:

^۶ ما در واقع یک نسخه ساده شده و بهبود یافته از الگوریتم اصلی را ارائه می‌دهیم.
^۷ algorithm Deutsch the in used is Interference : algorithm deutsch in using is interference how
 that function a is function constant A functions. balanced and constant between distinguish to that function a is function balanced A input. its of regardless value, same the returns always half. other the for ۱ and inputs its of half for ۰ returns first The states. of superposition a in qubits two preparing first by works algorithm Deutsch The second The $|\psi_1\rangle$ and $|\psi_0\rangle$ of superposition equal the is which , $|\psi_1\rangle + |\psi_0\rangle$ state the in prepared is qubit opposite with $|\psi_1\rangle$ and $|\psi_0\rangle$ states the of superposition a is which $|\psi_1\rangle - |\psi_0\rangle$ state the in prepared is qubit phases.
 and gate Hadamard a includes that circuit quantum a through passed then are qubits two The CNOT the and , $|\psi_1\rangle + |\psi_0\rangle$ superposition the into $|\psi_1\rangle + |\psi_0\rangle$ transforms gate Hadamard The gate. CNOT a qubit. second the to qubit first the of state the copies gate is qubit first the If measured. are qubits two the executed, been has circuit quantum the After to orthogonal is $|\psi_1\rangle - |\psi_0\rangle$ state the because is This constant. is f function the then , $|\psi_1\rangle - |\psi_0\rangle$ be to measured interfere. destructively will states two the between interference the so , $|\psi_1\rangle - |\psi_0\rangle$ state the the because is This balanced. is f function the then , $|\psi_1\rangle + |\psi_0\rangle$ be to measured is qubit first the If constructively will states two the between interference the so , $|\psi_1\rangle + |\psi_0\rangle$ state the to parallel is $|\psi_1\rangle + |\psi_0\rangle$ state interfere.

solve to used be can interference quantum how of example simple a is algorithm Deutsch The distinguish can algorithm Deutsch the case, this In classically. solve to difficult is that problem a need would computer classical a while step, single a in functions balanced and constant between steps. of number exponential an take to



شکل ۷.۳: پیاده‌سازی مدار کوانتومی الگوریتم دوچ

حالت ورودی:

$$|\psi_0\rangle = |01\rangle$$

سیستم دو کیوبیتی تشکیل شده، پس از اعمال اثر دو گیت هادامارد می‌دهد:

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

با کمی تأمل می‌توان دریافت که اگر U_f را به حالت $|x\rangle(|0\rangle - |1\rangle)$ اعمال کنیم، سپس به حالت $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$ می‌رسیم. بنابراین اعمال U_f به $|x\rangle(|0\rangle - |1\rangle)$ ما را با یکی از دو امکان زیر مواجه می‌کند:

$$|\psi_2\rangle = \begin{cases} \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{if } f(0) = f(1) \\ \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{if } f(0) \neq f(1) \end{cases}$$

با اعمال آخرین گیت هادامارد روی کیوبیت اول به حالت زیر خواهیم رسید:

$$|\psi_3\rangle = \begin{cases} \pm |0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{if } f(0) = f(1) \\ \pm |1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] & \text{if } f(0) \neq f(1) \end{cases}$$

با در نظر گرفتن شرایط زیر می‌توان $|\psi_3\rangle$ را به شکل زیر بازنویسی کرد:

$$\begin{cases} f(0) = f(1) \implies & f(0) \oplus f(1) = 0 \\ f(0) \neq f(1) \implies & f(0) \oplus f(1) = 1 \end{cases}$$

از این رو:

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

بنابراین با اندازه‌گیری کیوبیت اول می‌توانیم $f(0) \oplus f(1)$ را تعیین کنیم. واقعاً جالب است! مدار کوانتومی به ما توانایی تعیین یک ویژگی جهانی از $f(x)$ ، یعنی $f(0) \oplus f(1)$ را داده است، با استفاده از تنها یک ارزیابی از $f(x)$! این سریعتر از آن چیزی است که با یک دستگاه کلاسیک امکان‌پذیر است، یک دستگاه کلاسیک حداقل به دو ارزیابی نیاز دارد. این مثال تفاوت بین موازی‌سازی کوانتومی و الگوریتم‌های تصادفی کلاسیک را برجسته می‌کند. به سادگی، ممکن است تصور شود که حالت $|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$ مطابقت نزدیکی با یک رایانه کلاسیک تصادفی دارد که هرکدام از حالات $f(0)$ یا $f(1)$ با احتمال $1/2$ اندازه‌گیری می‌کند. تفاوت این است که در یک رایانه کلاسیک این دو گزینه همیشه یکدیگر را حذف می‌کنند. در یک رایانه کوانتومی، امکان دارد که دو گزینه با یکدیگر تداخل داشته باشند تا برخی از خواص کلی تابع f را با استفاده از چیزی شبیه به گیت هادامارد برای بازترکیب گزینه‌های مختلف، مانند آنچه در الگوریتم دوچ انجام شد، به دست آورند. اساس طراحی بسیاری از الگوریتم‌های کوانتومی این است که یک انتخاب هوشمندانه از تابع و تبدیل نهایی اجازه می‌دهد تا اطلاعات جهانی مفیدی در مورد تابع تعیین شود - اطلاعاتی که نمی‌توان به سرعت در یک رایانه کلاسیک به دست آورد.

۴.۳ الگوریتم دوچ - جوزا

algorithm, quantum general more a of case simple a is algorithm Deutsch's known application, The algorithm. Deutsch-Jozsa the as to refer shall we which Ams- in Alice, game. following the as described be may problem, Deutsch's as in Bob, to letter a in it mails and, $1 - 2^n$ to 0 from x number a selects terdam, which result, the with replies and (x) f function some calculates Bob Boston. of one of is which f function a use to promised has Bob Now, 1 or 0 either is balanced, is (x) f else or x , of values all for constant is (x) f either kinds: two half. other the for 0 and x , possible the all of half exactly for 1 to equal is, that constant a chosen has Bob whether certainty with determine to is goal Alice's fast How possible. as little as him with corresponding function, balanced a or succeed? she can

الگوریتم دوچ یک مورد ساده از یک الگوریتم کوانتومی عمومی تر است که به عنوان الگوریتم دوچ-جوزا شناخته می‌شود. کاربرد این الگوریتم، که به عنوان مشکل دوچ شناخته می‌شود، به شرح بازی زیر است:

آلیس، در آمستردام، یک عدد x را از بازه $[0, 2n - 1]$ انتخاب می‌کند و آن را در یک نامه به باب، در بوستون، می‌فرستد. باب یک تابع $f(x)$ را محاسبه می‌کند و نتیجه را که ۰ یا ۱ است، ارسال می‌کند. اکنون، باب قول داده است که از تابعی از دو نوع استفاده کند؛ یا $f(x)$ برای همه مقادیر x ثابت است، یا $f(x)$ متعادل است، یعنی برای دقیقاً نیمی از همه‌های x ممکن برابر با ۱ است و برای نیمی دیگر برابر با ۰ است.

هدف الی این است که با اطمینان تعیین کند که باب یک تابع ثابت یا متعادل را انتخاب کرده است، با او به حداقل ارتباط ممکن. او چگونه می‌تواند به سرعت موفق شود؟

In the classical case, Alice may send only one value of x to Bob, and then Bob will need at least $2n/2 + 1$ queries to determine if f is constant or balanced. The best deterministic algorithm she can use is to query f at $2n/2 + 1$ different points. In the quantum case, Alice can send n qubits to Bob, and he can use a quantum circuit to evaluate f on all 2^n possible inputs simultaneously. This allows Bob to determine if f is constant or balanced with only one query.

در حالت کلاسیک، الی ممکن است فقط یک مقدار x را در هر نامه به باب ارسال کند. در بدترین حالت، الی باید حداقل $2n/2 + 1$ بار از باب سوال کند، زیرا ممکن است $2n/2 + 1$ دریافت کند قبل از اینکه سرانجام ۱ را دریافت کند و به او بگوید که تابع باب متعادل است. بهترین الگوریتم دترمینیستی کلاسیک که می‌تواند استفاده کند بنابراین به $2n/2 + 1$ پرسش نیاز دارد. توجه داشته باشید که در هر نامه، الی n بیت اطلاعات را به باب ارسال می‌کند. علاوه بر این، در این مثال، فاصله فیزیکی برای افزایش مصنوعی هزینه محاسبه $f(x)$ استفاده می‌شود، اما این مورد در مسئله عمومی لازم نیست، جایی که $f(x)$ ممکن است ذاتاً دشوار باشد برای محاسبه.

If Alice and Bob are able to exchange qubits, Alice can use a quantum circuit to evaluate f on all 2^n possible inputs simultaneously. This allows Bob to determine if f is constant or balanced with only one query. The quantum algorithm achieves this by using a quantum circuit that applies a Hadamard gate to all n qubits, then applies a quantum circuit that evaluates f on all 2^n possible inputs simultaneously, and finally applies another Hadamard gate to all n qubits.

اگر باب و الی بتوانند کویت ها را به جای بیت های کلاسیک مبادله کنند، و اگر باب موافقت کند $f(x)$ را با استفاده از تبدیل یونیتاری Uf محاسبه کند، سپس الی می‌تواند هدف خود را در یک مکاتبه

با باب با استفاده از الگوریتم زیر به دست آورد.

store to register qubit n an has Alice algorithm, Deutsch's to Analogously store to Bob, to give will she which register qubit single a and in, query her registers answer and query her both preparing by begins She in. answer the parallelism quantum using (x) f evaluate will Bob state. superposition a in the in states interferes then Alice register. answer the in result the leave and finishes and register. query the on transform Hadamard a using superposition or constant was f whether determine to measurement suitable a performing by balanced.

با توجه به الگوریتم دوچ، الی یک رجیستر n کوبیتی را برای ذخیره پرس و جو خود آماده می کند و یک رجیستر کوبیت واحد را که به باب می دهد تا پاسخ را در آن ذخیره کند. او هر دو رجیستر پرس و جو و پاسخ خود را در یک حالت فوق العاده آماده می کند. باب $f(x)$ را با استفاده از موازی سازی کوانتومی ارزیابی می کند و نتیجه را به الی برمی گرداند. الی سپس با استفاده از تبدیل هادامارد روی رجیستر پرس و جو، حالت های تداخل را در حالت فوق العاده مداخله می کند و با انجام یک اندازه گیری مناسب، تعیین می کند که آیا f ثابت یا متعادل است.

fol- us Let .۲۰.۱ Figure in depicted are algorithm the of steps specific The is (۴۶.۱) $|0\rangle^{\otimes n} |1\rangle = |0\rangle^{\otimes n}$ state input The circuit. this through states the low the describes register query the here but (۴۱.۱) Equation of that to similar transform Hadamard the After state. $|0\rangle^{\otimes n}$ the in prepared all qubits n of state have we register answer the on gate Hadamard the and register query the on

$$[\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)]^{\otimes n} \otimes |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes |0\rangle$$

گام‌های خاص الگوریتم در شکل ۲۰.۱ نشان داده شده است. بیاید با دنبال کردن این مدار، به حالت‌ها پردازیم.

حالت ورودی

$$(۴۶.۱) |0\rangle^{\otimes n} |1\rangle = |0\rangle^{\otimes n}$$

این شبیه حالت معادله (۴۱.۱) است، اما در اینجا رجیستر پرس و جو وضعیت n کوبیت را توصیف می کند که همه در حالت $|0\rangle^{\otimes n}$ آماده شده اند.

پس از تبدیل هادامارد روی رجیستر پرس و جو و گیت هادامارد روی رجیستر پاسخ، ما داریم

$$[\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)]^{\otimes n} \otimes |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes |0\rangle$$

reg- answer the and values. all of superposition a now is register query The is f function the Next, .۱ and ۰ of superposition weighted evenly an in is ister

now Alice (۴۸.۱) giving $(x)^{\otimes n}, f^{\otimes n} y |x, \otimes y^{\otimes n} |x, : U_f$ using Bob (by evaluated stored is evaluation function Bob's of result the which in qubits of set a has terms interferes now She state. superposition qubit the of amplitude the in To register. query the on transform Hadamard a using position super- the in the calculate first to helps it transform Hadamard the of result the determine $\cdot = x$ cases the checking By $|x\rangle^{\otimes n}$. state a on transform Hadamard the of effect $|z\rangle^{\otimes n}/\sqrt{2^n}$. $(-1)^{xz} z \sum = H|x\rangle^{\otimes n}$ qubit single a for that see we separately $1 = x$ and equa- useful very the in succinctly more summarized be can This (۴۹.۱) Thus Using \cdot modulo z , and x of product inner bitwise the is $z \cdot x$ where tion (۱.۵۰) observes now Alice $|x\rangle^{\otimes n}, (1.51)$ evaluate now can we (۴۸.۱) and equation this $x(-1)^f \sum$ is $|0\rangle^{\otimes n}$ state the for amplitude the that Note register. query the $(x)/2^n$.

رجیستر پرس و جو اکنون یک superposition از همه مقادیر است، و رجیستر پاسخ در یک superposition به طور مساوی وزن شده از ۰ و ۱ است.

در مرحله بعد، تابع f ارزیابی می شود (توسط باب) با استفاده از $U_f : |x\rangle^{\otimes n}, f^{\otimes n} y |x, \otimes y^{\otimes n} |x, : U_f$ که (۴۸.۱) را می دهد.

الی اکنون یک مجموعه کویت دارد که در آن نتیجه ارزیابی تابع باب در دامنه کویت super-position state ذخیره می شود. او اکنون با استفاده از تبدیل Hadamard روی رجیستر پرس و جو، عبارات را در super-position تداخل می کند.

برای تعیین نتیجه تبدیل Hadamard، کمک می کند تا ابتدا اثر تبدیل Hadamard را روی یک حالت $|x\rangle^{\otimes n}$ محاسبه کنیم. با بررسی موارد $0 = x$ و $1 = x$ به صورت جداگانه می بینیم که برای یک کویت واحد $|x\rangle^{\otimes n} \sum = H|x\rangle^{\otimes n} (-1)^{xz} z \sum = |z\rangle^{\otimes n}/\sqrt{2^n}$ بنابراین (۴۹.۱)

این را می توان به طور خلاصه در معادله بسیار مفید زیر خلاصه کرد:
(۵۰.۱)

جایی که $z \cdot x$ product inner bitwise z و x است، به \cdot modulo z .

با استفاده از این معادله و (۴۸.۱) اکنون می توانیم $|x\rangle^{\otimes n}$ را ارزیابی کنیم:

(۵۱.۱)

الی اکنون رجیستر پرس و جو را مشاهده می کند. توجه داشته باشید که دامنه برای حالت $|0\rangle^{\otimes n}$ است $(x)/2^n$. $x(-1)^f \sum$

discern to – balanced f and constant f – cases possible two the at look Let's
or $1 +$ is $|0\rangle^{\otimes n}$ for amplitude the constant is f where case the In happens. what

length unit of is $\frac{1}{\sqrt{2}}$ Because takes. (x) f value constant the on depending, $\frac{1}{\sqrt{2}}$ - will observation an and zero, be must amplitudes other the all that follows it and positive the then balanced is f If register. query the in qubits all for $\frac{1}{\sqrt{2}}$ yield amplitude an leaving cancel, $\frac{1}{\sqrt{2}}$ for amplitude the to contributions negative one least at on $\frac{1}{\sqrt{2}}$ than other result a yield must measurement a and zero, of the then $\frac{1}{\sqrt{2}}$ all measures Alice if Summarizing, register. query the in qubit Deutsch-Jozsa The balanced. is function the otherwise constant; is function below. summarized is algorithm

بیاید به دو مورد ممکن - f ثابت و f متعادل - نگاه کنیم تا ببینیم چه اتفاقی می افتد. در صورتی که f ثابت باشد، دامنه برای حالت $\frac{1}{\sqrt{2}}$ برابر است با $\frac{1}{\sqrt{2}}$ یا $\frac{1}{\sqrt{2}}$ ، بسته به مقدار ثابت f (x) که می گیرد. از آنجایی که $\frac{1}{\sqrt{2}}$ طول واحد است، نتیجه می گیریم که تمام دامنه‌های دیگر باید صفر باشند، و یک مشاهده $\frac{1}{\sqrt{2}}$ را برای همه کوبیت‌ها در رجیستر پرس و جو به همراه خواهد داشت. اگر f متعادل باشد، سهم مثبت و منفی دامنه برای $\frac{1}{\sqrt{2}}$ خنثی می شود، و یک دامنه صفر باقی می ماند، و یک اندازه گیری باید نتیجه ای غیر از $\frac{1}{\sqrt{2}}$ را در حداقل یک کوبیت در رجیستر پرس و جو به همراه داشته باشد. به طور خلاصه، اگر الی همه $\frac{1}{\sqrt{2}}$ را اندازه گیری کند، تابع ثابت است؛ در غیر این صورت تابع متعادل است.

الگوریتم Deutsch-Jozsa در زیر خلاصه شده است:

الگوریتم Deutsch-Jozsa

الی یک n کوبیت رجیستر را برای ذخیره پرس و جو خود آماده می کند و یک کوبیت رجیستر واحد را که به باب می دهد تا پاسخ را در آن ذخیره کند. او هر دو رجیستر پرس و جو و پاسخ خود را در یک حالت فوق العاده آماده می کند. باب $f(x)$ را با استفاده از U_f : $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$ ارزیابی می کند. الی با استفاده از تبدیل Hadamard روی رجیستر پرس و جو، عبارات را در - position super تداخل می کند. الی کوبیت های پرس و جو را اندازه گیری می کند.

۵.۳ oracle

site qiskit use

simulation vs comp ۶.۳

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

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 $| \psi \rangle$ در اختیار دارد. چه بدتر از آن، حتی اگر او حالت $| \psi \rangle$ را می دانست، توصیف دقیق آن به مقدار بی نهایت نیاز دارد. اطلاعات کلاسیک از آنجایی که $| \psi \rangle$ مقادیر را در یک فضای پیوسته می گیرد. بنابراین حتی اگر او انجام دهد بدانید، $| \psi \rangle$ همیشه طول می کشد تا آلیس وضعیت را برای باب توصیف کند. نگاه نمی کند برای آلیس خویه خوشبختانه برای آلیس، انتقال از راه دور کوانتومی راهی برای استفاده از آن است جفت EPR درهم به منظور ارسال $| \psi \rangle$ به باب، تنها با سربار کوچک کلاسیک ارتباط به طور کلی، مراحل حل به شرح زیر است: آلیس با کیوبیت $| \psi \rangle$ 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 نیمه از جفت EPR به طرز شگفت انگیزی، با انجام این کار او می تواند حالت اولیه را بازیابی کند! $| \psi \rangle$ 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 $| \psi \rangle = \frac{1}{\sqrt{2}} (| \psi \rangle + | \psi \rangle)$ که α و β ناشناخته هستند. دامنه ها حالت ورودی مدار $| \psi \rangle$ است $| \psi \rangle = \frac{1}{\sqrt{2}} (| \psi \rangle + | \psi \rangle)$ $\sqrt{2}$ $[(| \psi \rangle + | \psi \rangle) + (| \psi \rangle + \alpha | \psi \rangle)]$ ، (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 قبلاً 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 $| \psi \rangle = \frac{1}{\sqrt{2}} [(| \psi \rangle + | \psi \rangle) + (| \psi \rangle + \alpha | \psi \rangle)]$. (۳۰.۱) سپس اولین کیوبیت را از طریق دروازه هادامارد می فرستد و به دست می آورد $| \psi \rangle = \frac{1}{2} [(| \psi \rangle + \alpha | \psi \rangle) + (| \psi \rangle + | \psi \rangle)]$. (۳۱.۱) این حالت را می توان به روش زیر بازنویسی کرد، به سادگی با گروه بندی مجدد عبارات: $| \psi \rangle = \frac{1}{2} [(| \psi \rangle + \alpha | \psi \rangle) + (| \psi \rangle + | \psi \rangle)]$. (۳۲.۱) این عبارت به طور طبیعی به چهار اصطلاح تقسیم می شود. عبارت اول دارای کیوبیت های آلیس است در حالت $| \psi \rangle$ و کیوبیت باب در حالت $| \psi \rangle + \alpha | \psi \rangle$ - 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: ۰۰ $| \psi \rangle = \frac{1}{2} [(| \psi \rangle + \alpha | \psi \rangle) + (| \psi \rangle + | \psi \rangle)]$. (۳۳.۱) $| \psi \rangle = \frac{1}{2} [(| \psi \rangle + \alpha | \psi \rangle) + (| \psi \rangle + | \psi \rangle)]$. (۳۴.۱) $| \psi \rangle = \frac{1}{2} [(| \psi \rangle + \alpha | \psi \rangle) + (| \psi \rangle + | \psi \rangle)]$. (۳۵.۱) $| \psi \rangle = \frac{1}{2} [(| \psi \rangle + \alpha | \psi \rangle) + (| \psi \rangle + | \psi \rangle)]$. (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 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 [۹۹] 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 [۹۹] 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 [۹۹] باقی می‌ماند و کیوبیت داده اصلی بسته به نتیجه اندازه‌گیری به یکی از حالت‌های پایه محاسباتی ۰ یا ۱ 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