فهرست مطالب

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

book chuang ۱ Chapter

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 in on acting gate Hadamard a with created be can which ،۲√/(⟩۱| + ⟩۰|) position ⟩۰|. Then we apply Uf ، resulting in the 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، بهره‌می‌بریم. کیوبیت یک سیستم کوانتومی با فضای دوبعدی است. برای تعیین این دوبعد می‌توان ا ز یکی از خصوصیات سامانه های کوانتومی استفاده کرد.

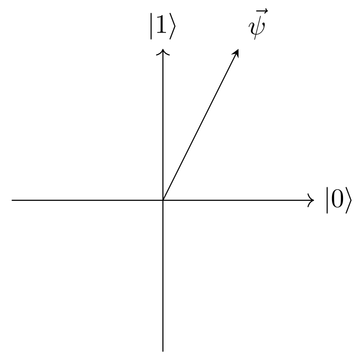
برخلاف بیت ها که مقادیر ثابت ۰ یا ۱ را به خود می‌گیرند؛ یک کیوبیت می‌تواند در یک حالت «برهمنهی کوانتومی» باشد؛ این بدان معناست که یک کیوبیت بواسطه‌ی مشاهده ناظر به یکی از حالات ۰ یا یک تبدیل شود. این مهم‌ترین مزیت استفاده از کیوبیت‌هاست. بیان ریاضی یک کیوبیت ،در حالت برهمنهی، به شرح زیر است:

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

[۱] Qubit
[۲] Bit Binary

کت‌ها$|0\rangle$ 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:

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

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.

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

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

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

نمایش ماتریسی این گیت کوانتومی به شکل زیر است:

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

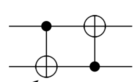
اینا باید اصلاح بشه

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

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

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

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 simulation vs comp

بسیاری از مسائل کوانتومی و بسیاری از الگوریتم‌های کوانتومی قابل شبیه‌سازی روی کامپیوترهای کوانتومی می‌باشند. بنابرین یک سوال به‌واقع مهم مطرح می‌شود: **چرا به یک کامپیوتر کوانتومی نیاز داریم؟**

در هنگام محاسبات کوانتومی، کامپیوترهای کلاسیک دارای محدودیت‌هایی هستند. به طور مشابه کامپیوترهای کوانتومی نیز دارای معایبی هستند؛ که قابل بحث و بررسی هستند. دراین بخش به این مزایا و معایب هرکدام از کامپیوترها می‌پردازیم و در ادامه به اهداف تعریف شده برای کامپیوترهای کوانتومی می‌پردازیم.

۳.۲ 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 تک-کیوبیت، به صورت زیر تعریف شده است:

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

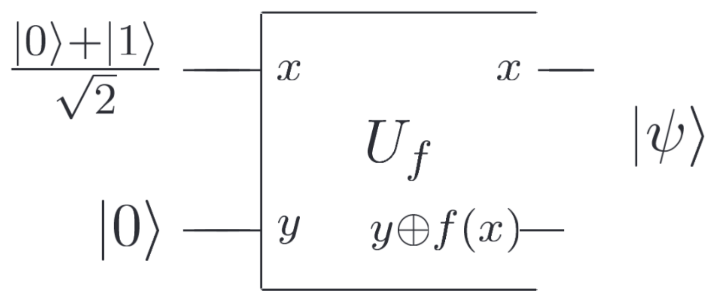
روش مناسب برای محاسبه این تابع در یک کامپیوتر کوانتومی، با در نظر گرفتن دو کیوبیت که در حالت $|x, y\rangle$ شروع می شود. با یک توالی مناسب از گیت های منطقی می توان این حالت را به

[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 $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$، عنوان «تابع U_f» را اطلاق خواهیم کرد. لازم به ذکرست که این تبدیل، یک تبدیل یکه به شمار می‌آید.[۳]

اگر $\mathrm{y} = 0$ 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 $|x, y \oplus f(x)\rangle$ $\rightarrow$ $|x, y\rangle$، 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 $|0\rangle$

[۲] Modulo ۲ is a mathematical operation that returns the remainder of a division by ۲. For ex- ample، ۵ mod ۲ is ۱، because ۵ divided by ۲ has a quotient of ۲ and a remainder of ۱.

The symbol "□" is often used to indicate addition modulo ۲. So، the expression "۵ □ ۳" would be evaluated as follows:

۵ □ ۳ = (۵ + ۳) mod ۲ = ۸ mod ۲ = ۰ This is because ۸ divided by ۲ has a quotient of ۴ and a remainder of ۰.

Modulo ۲ is a useful operation in many different areas of mathematics، including cryptography، computer science، and number theory. It is also used in everyday life، for example، when checking whether a number is even or odd.

Here are some other examples of modulo ۲:

۱ mod ۲ = ۱ ۲ mod ۲ = ۰ ۳ mod ۲ = ۱ ۴ mod ۲ = ۰ ۵ mod ۲ = 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.

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:

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

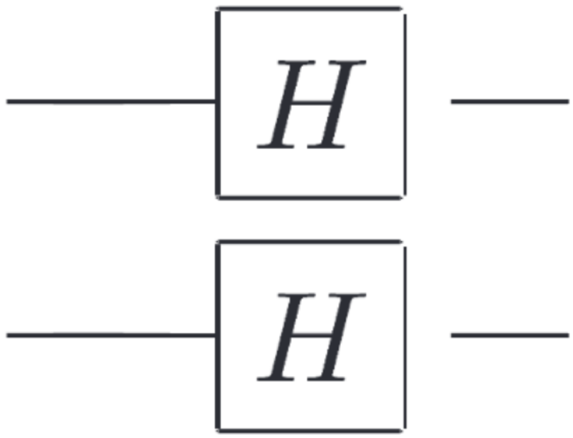
از نماد $\mathrm{H}\otimes 2$ به عنوان نشانه‌ی عملکرد موازی دو گیت هادامارد استفاده می‌کنیم؛از علامت $\otimes$ به عنوان تانسور یاد می‌کنیم. به طور کلی نتایج اعمال موازی گیت هادامارد روی n کیوبیت روی حالت کوانتومی برابرست با:

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

در اینجا، $\sum$ نشان دهنده جمع بر روی همه مقادیر ممکن x است، و ما$\mathrm{H}\otimes n$ را برای نشان دادن این عمل می نویسیم. اعمال تبدیل هادامارد روی یک بهمنهی کوانتومی برابر از همه حالت های محاسباتی تولید می کند؛ و با استفاده از فقط n گیت، یک برهمنهی از $2n$ حالت تولید می کند.

تبدیل هادامارد $\mathrm{H}\otimes 2$ 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.

درنهایت حالت زیر تولید می‌شود:
(x)⍰ ۱√۲n∑x|x⍰|f

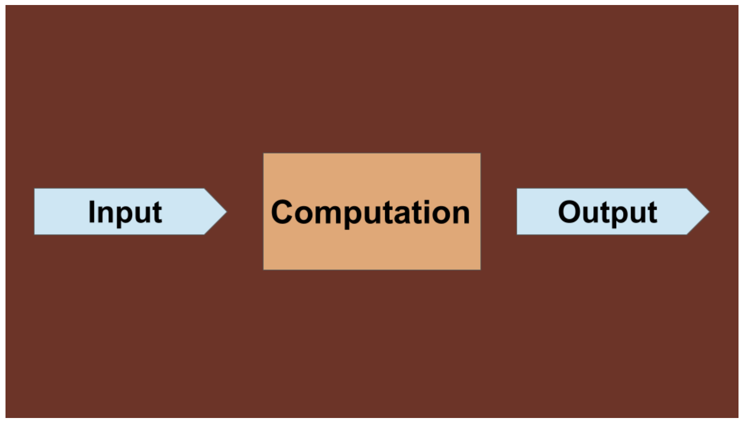
$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$$

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 کوبیتی ما، اندازه‌گیری حالت فقط $|0, f(0)\rangle$ یا $|1, f(1)\rangle$ را می‌دهد! به طور مشابه، در حالت کلی، اندازه‌گیری حالت ∑x ،f |x ⍰(x) 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 سوپرپوزیسیون مانند ∑x ،f |x ⍰(x) نیاز دارد. در بخش های 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 کوئری، 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.

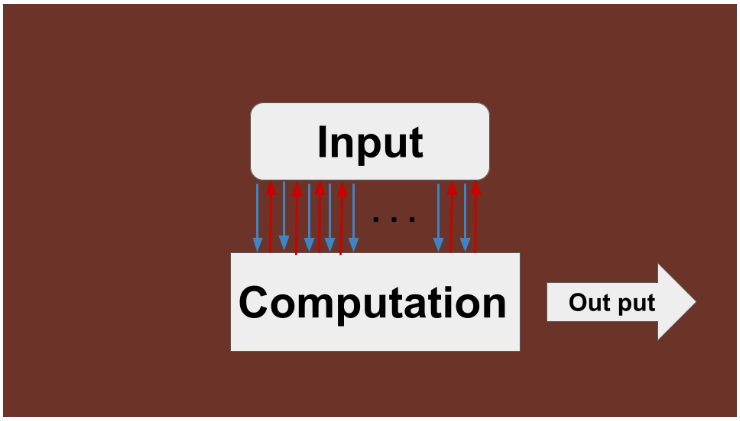
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان درنظر گرفت که ورودی داده شده و خروجی نهایی،هر دو در قالب یک رشته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

۲.۳ 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



شکل ۴.۳: شکل بالا نمود مدل محاسباتی کوئری 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.

دریافت کنیم.

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.

۳.۳ معرفی و پیاده سازی الگوریتم دوچ

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 شده‌بود. این الگوریتم نقطه‌ی شروعی برای 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:

[۴] Deutsch David

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

هدف بررسی ثابت بودن یا متعادل[5] بودن تابع f است. به‌طور کلی، درساده‌ترین حالت، می‌توان چهار وضعیت را برای تابع $f : \sum \rightarrow \sum$ درنظر گرفت:

a	$f_1(a)$
0	0
1	0

a	$f_2(a)$
0	0
1	1

a	$f_3(a)$
0	1
1	0

a	$f_4(a)$
0	1
1	1

شکل ۵.۳:

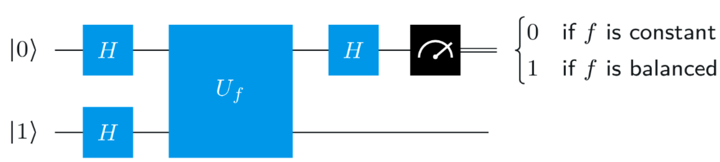
در شکل بالا توابع f 1 ، f 4 توابع ثابت و توابع f 2 و f 3 توابع متعادل هستند.

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

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

۲.۳.۳ الگوریتم دوچ

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



شکل ۶.۳:

[5] Constante or balanse.

یک تغییر ساده در مدار شکل ۳.۱ نشان می دهد که چگونه مدارهای کوانتومی می توانند 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] است. مشابه قبل،ابتدا از گیت هادامارد برای آماده سازی اولین کوبیت به عنوان superposition (|۰⍰ + |۱⍰)/√۲ استفاده کنیم، اما اکنون کوبیت دوم y را با اعمال یک گیت هادامارد به حالت |۱> به عنوان superposition (|۰⍰ - |۱⍰)/√۲ آماده کنیم. به‌شکل زیر دقت کنید:

[۶] ما در واقع یک نسخه ساده شده و بهبود یافته از الگوریتم اصلی را ارائه می دهیم.

[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

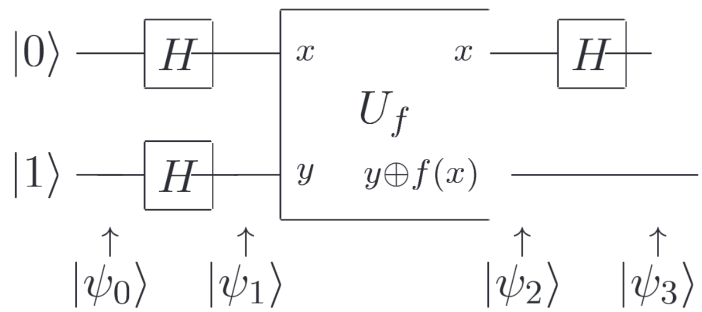
first The states. of superposition a in qubits two preparing first by works algorithm Deutsch The second The .⍰۱| and ⍰۰| of superposition equal the is which ،⍰+| state the in prepared is qubit opposite with ⍰۱| and ⍰۰| states the of superposition a is which |⍰⍰، state the in prepared is qubit phases.

and gate Hadamard a includes that circuit quantum a through passed then are qubits two The CNOT the and ،⍰۱| + ⍰۰| superposition the into ⍰+| 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 |⍰⍰ state the because is This constant. is f function the then ،⍰۰| be to measured the state ⍰۰|، so the interference between the two states will destructively interfere.

the because is This balanced. is f function the then ،⍰۱| be to measured is qubit first the If constructively will states two the between interference the so ،⍰۱| state the to parallel is |⍰⍰ 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 to take an exponential number of steps.



شکل ۷.۳: پیاده‌سازی مدارکوانتومی 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 Uf را به حالت ⍰|۰)⍰lx⍰ - |۱⍰)/√۲ اعمال کنیم، سپس به حالت f(۱ -) ⍰|۰)⍰lx(x) - |۱⍰)/√۲ می رسیم. بنابرین اعمال Uf به ⍰۱⍰| ما را با یکی از دو امکان زیر مواجه می کند:

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

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 درنظر 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 اندازه گیری کیوبیت اول می توانیم $f(0)\oplus f(1)$ 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 ،۱ - ۲n to ۰ 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، .۱ or ۰ either is balanced، is (x) f else or x، of values all for constant is (x) f either kinds؛ two half. other the for ۰ and x، possible the all of half exactly for ۱ 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 توضیح ساده از یک الگوریتم کوانتومی عمومی‌تر است که به عنوان الگوریتم دوچ-جوزا شناخته می‌شود. کاربرد این الگوریتم، که به عنوان مشکل دوچ شناخته می‌شود، به شرح زیر است:

آلیس، در آمستردام، یک عدد x را از بازه $[0, 2^n - 1]$ 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 یک مدل تابع استفاده خواهد کرد؛ این تابع یا$f(x)$ که برای همه مقادیر x ثابت است، یا $f(x)$ متعادل است، یعنی حاصل آن برای دقیقاً نیمی از همه هایx ممکن برابر با ۱ است و برای نیمی دیگر برابر با ۰ است.

هدف آلیس این است که با اطمینان و بکار بستن کمترین گام‌های ممکن تعیین کند که باب یک تابع ثابت یا متعادل را انتخاب کرده است. او چگونه می‌تواند به سرعت موفق شود؟

در حالت کلاسیک، آلیس ممکن است فقط یک مقدار x را در هر نامه به باب ارسال کند. در بدترین حالت، الی باید حداقل $\frac{2^n}{2} + 1$ بار از باب سوال کند، زیرا ممکن است قبل از دریافت یک، $\frac{2^n}{2}$ مرتبه پاسخ 0 را دریافت کند. آلیس باید یک را دریافت کند؛تا بتواند به او بگوید که تابع باب متعادل است.

یعنی در بهترین الگوریتم کلاسیک که می تواند استفاده کند بنابراین به$\frac{2^n}{2} + 1$ پرسش نیاز دارد. توجه داشته باشید که در هر نامه، آلیس n بیت اطلاعات را به باب ارسال می کند. علاوه بر این، در این مثال، فاصله فیزیکی باب و آلیس و به تبع آن افزایش هزینه محاسبه $f(x)$ و دشواری‌های احتمالی اجرای تابع $f(x)$ درنظر گرفته نشده‌است.

اگر باب و آلیس بتوانند کوبیت ها را به جای بیت های کلاسیک مبادله کنند، و اگر باب موافقت کند $f(x)$ را با استفاده از تبدیل یکه‌ی U_f محاسبه کند، سپس آلیس می تواند هدف خود را در یک مکاتبه با باب و با استفاده از الگوریتم زیر به دست آورد.

با توجه به الگوریتم دوچ، آلیس 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 برهمنهی آماده می کند. باب f(x) را با استفاده از موازی سازی کوانتومی ارزیابی می کند و نتیجه را به آلیس برمی گرداند. آلیس سپس با استفاده از اعمال تبدیل هادامارد روی رجیستر پرس و جو(n-کیوبیتی)، حالات برهمنهی تداخل می‌دهد و با انجام یک اندازه گیری مناسب، تعیین می کند که آیا f ثابت یا متعادل است.

گام‌های خاص الگوریتم در شکل ۲۰.۱ نشان داده شده است. بیایید با دنبال کردن این مدار، به بررسی حالات ایجاد شده بپردازیم. حالت ورودی ⍰۰⍰| = ⍰۱|n⍰⍰|۰ (۴۶.۱)؛ شبیه حالت معادله (۴۱.۱) است، اما در اینجا رجیستر پرس و جو وضعیت n کوبیت را توصیف می‌کند که همه در حالت ۰⍰| آماده شده‌اند. پس از اعمال تبدیل هامادارد روی رجیستر پرس و جو و روی رجیستر پاسخ، می‌توان نوشت:

[۲√􏰀۱| - 􏰀۰| ∑x􏰀۰،۱n|x􏰀√۲n[= |􏰀۱􏰀

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)􏰀، f 􏰀 y |x، 􏰀 y􏰀 |x، : Uf 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 ۰ = x cases the checking By |x􏰀. state a on transform Hadamard the of effect |z􏰀/√۲. (-۱)xz z ∑ = H|x􏰀 qubit single a for that see we separately ۱ = x and equa- useful very the in succinctly more summarized be can This (۴۹.۱) Thus Using .۲ modulo z، and x of product inner bitwise the is z · x where tion(۱.۵۰) observes now Alice |􏰀۳􏰀،(۱.۵۱) evaluate now can we (۴۸.۱) and equation this x(-۱)f ∑ is |۰􏰀􏰀n state the for amplitude the that Note register. query the (x)/۲n.

رجیستر پرس و جو اکنون یک برهمنهی از همه مقادیر ممکن به‌شمار می‌آید؛ درحالی که رجیستر پاسخ در یک برهمنهی به طور مساوی وزن شده از ۰ و ۱ محسوب می‌شود[۸].

در مرحله بعد، تابع f توسط باب و به شکل Uf : |x، 􏰀y􏰀 ↦ |x، y 􏰀 f􏰀(x) ارزیابی می شود ، که (۴۸.۱) را می دهد.

آلیس اکنون یک مجموعه کوبیت دارد که در آن نتیجه اعمال تابع باب در دامنه کوبیت حالت برهمنهی ذخیره می شود. او اکنون با استفاده از تبدیل هادامارد روی رجیستر پرس و جو، عبارات را در حالت برهمنهی کوانتومی تداخل می کند.

برای تعیین نتیجه تبدیل هادامارد، بهترست ابتدا اثر تبدیل هادامارد را روی یک حالت |x􏰀 محاسبه کنیم. با بررسی موارد x = ۰ و x = ۱ به صورت جداگانه می بینیم که برای یک کوبیت واحد H|x􏰀 = ∑z (-۱)xz |z􏰀/√۲ می‌باشد. بنابراین (۴۹.۱)

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

(۵۰.۱)

جایی که z · x bitwise inner product x و z است، به modulo ۲.

با استفاده از این معادله و (۴۸.۱) اکنون می توانیم |􏰀۳􏰀 را ارزیابی کنیم:

---

[۸] یعنی احتمال رخ‌دادن صفر و یک یکسان است.

(۵۱.۱)

آلیس اکنون رجیستر پرس و جو را مشاهده می کند. توجه داشته باشید که دامنه برای حالت n⊗⊗|۰
است ∑ f(-۱)x .n۲/(x)

از استاد بپرس اشکاااااللل

discern to – balanced f and constant f – cases possible two the at look Let's or ۱+ is |۰⊗⊗n for amplitude the constant is f where case the In happens. what length unit of is |⊗۳⊗ Because takes. (x) f value constant the on depending ،۱- 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 ۰s yield amplitude an leaving cancel، |۰⊗⊗n for amplitude the to contributions negative one least at on ۰ than other result a yield must measurement a and zero، of the then ۰s 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

بیایید 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 n⊗⊗|۰ برابر است با +۱ یا -۱، بسته به مقدار ثابت f (x) که می‌گیرد.

از آنجایی که ⊗۳⊗| طول واحد است، نتیجه می‌گیریم که تمام دامنه‌های دیگر باید صفر باشند، و یک مشاهده ۰ را برای همه کوبیت‌ها در رجیستر پرس و جو به همراه خواهد داشت.

اگر f متعادل باشد، سهم مثبت و منفی دامنه برای n⊗⊗|۰ خنثی می‌شود، و یک دامنه صفر باقی می‌ماند، و یک اندازه‌گیری باید نتیجه‌ای غیر از ۰ را در حداقل یک کوبیت در رجیستر پرس و جو به همراه داشته باشد.

به طور خلاصه، اگر الی همه ۰ را اندازه گیری کند، تابع ثابت است؛ در غیر این صورت تابع متعادل است.

الگوریتم Deutsch-Jozsa در زیر خلاصه شده است:

the performs which Uf box black A (۱) Inputs: Deutsch–Jozsa Algorithm: ،۰ ⊗ (x) f and ۱ - ۲n ، . . . . ،۰ ⊗ x for (x)⊗، f ⊗ |x⊗y ⊗ |x⊗y⊗ transformation (x) f else or x، of values all for constant either is (x) f that promised is It .۱ for ۰ and x، possible the all of half exactly for ۱ to equal is، that balanced، is evalu- One Runtime: constant. is f if only and if ۰ Outputs: half. other the ⊗ .۲ state initialize |۰⊗⊗n|۱⊗ .۱ Procedure: succeeds. Always . Uf of ation

Hadamard using superposition create [۲√ ⍰۱| - ⍰۰|] |x⍰ x=۰ ∑۱- ۲n √۲n ۱ ⍰ .۴ Uf using f function calculate [۲√ ⍰۱| - ⍰۰|] (x)|x⍰ (-۱)f x ∑ ⍰ .۳ gates .۵ transform Hadamard perform [۲√ ⍰۱| - ⍰۰|] √۲n (x)|z⍰ (-۱)x·z+f x ∑ z ∑ computer quantum a that shown We've z output final obtain to measure z ⍰ compared f function the of ation evalu- one with problem Deutsch's solve can impres- appears This evaluations. ۱ + ۲n/۲ for requirement classical the to is lem prob- Deutsch's First، caveats. important several are there but sive، Second، applications. known no has it problem؛ important especially an not an ways some in is algorithms quantum and classical between comparison the is function the evaluating for method the as comparison، oranges and apples probabilistic a use to allowed is Alice if Third، cases. two the in different quite randomly few a for (x) f evaluate to Bob asking by then computer، classical is f whether probability high with determine quickly very can she x chosen than realistic more perhaps is scenario probabilistic This balanced. or constant caveats، these Despite considering. been have we scenario deterministic the quan- impressive more for seeds the contains algorithm Deutsch–Jozsa the principles the understand to attempt to enlightening is it and algorithms، tum behind its operation. الگوریتم Deutsch–Jozsa: ورودی‌ها: (۱) یک جعبه سیاه Uf که تبدیل زیر را انجام می‌دهد ⍰|x⍰|y ⍰ |x⍰|y ⍰ f ⍰(x)، برای x ⍰ ۰، ...، ۲n - ۱ و f (x) ⍰ ۰، ۱. قول داده شده است که f (x) برای همه مقادیر x ثابت است یا f (x) متعادل است، یعنی برای دقیقاً نیمی از همه های x ممکن برابر با ۱ و برای نیمی دیگر ۰ است. خروجی: ۰ اگر و فقط اگر f ثابت باشد. زمان اجرا: یک ارزیابی .Uf همیشه موفق می شود. روش:

⍰۱|n⍰⍰۰| حالت را initialize کنید ⍰ ۱ √۲n ۲n -۱∑ x=۰ ⍰|x [|۰⍰ - |۱⍰ √۲] ایجاد superposition با استفاده از دروازه‌های Hadamard ⍰ ∑ x f(۱-) ⍰|x(x) [|۰⍰ - |۱⍰ √۲] تابع f را با استفاده از Uf محاسبه کنید ⍰ ∑ z ∑ x f+x·z(۱-) ⍰|z(x) √۲n [|۰⍰ - |۱⍰ √۲] تبدیل Hadamard را انجام دهید ⍰ z اندازه گیری کنید تا خروجی نهایی z را بدست آورید ما نشان داده‌ایم که یک کامپیوتر کوانتومی می‌تواند مشکل Deutsch را با یک ارزیابی حل کند – ارزشیابی تابع f در مقایسه با نیاز کلاسیک برای ۲n/۲ + ۱ ارزیابی. این به نظر چشمگیر است، اما چند نکته مهم وجود دارد. اول، مشکل Deutsch نیست یک مشکل مهم است؛ هیچ کاربرد شناخته شده ای ندارد. دوم، مقایسه بین الگوریتم های کلاسیک و کوانتومی تا حدودی مقایسه سیب و پرتقال است، زیرا روش برای ارزیابی تابع در دو مورد بسیار متفاوت است. سوم، اگر آلیس مجاز باشد از یک کامپیوتر کلاسیک

احتمالی استفاده کند، سپس با درخواست از باب برای ارزیابی f (x) برای چند x به صورت تصادفی می تواند بسیار سریع تعیین کند با احتمال بالا اینکه f ثابت یا متعادل است. این سناریو احتمالی است شاید واقع بینانه تر از سناریوی determinstic که ما در نظر گرفته ایم. علیرغم این ظرافت ها، الگوریتم Deutsch–Jozsa حاوی بذرهای الگوریتم های کوانتومی بیشتر و چشمگیرتر است، و درک اصول پشت آن روشنگر است. عملکرد آن.

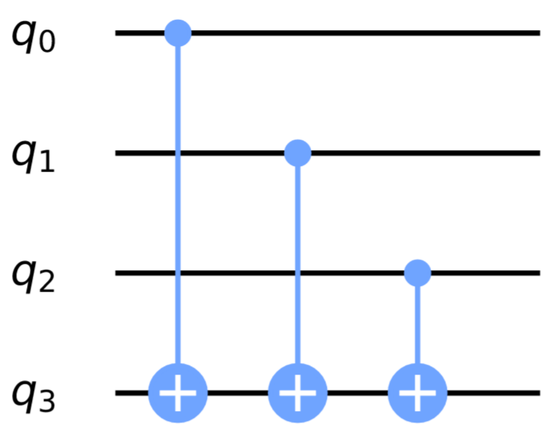
۵.۳ ساخت یک اوراکل کوانتومی

بیایید راه های مختلفی را ببینیم که می توانیم یک اوراکل کوانتومی ایجاد کنیم.

برای یک تابع ثابت، ساده است:

اگر $f(x) = ۰$، گیت را به کیوبیت در ثبات ۲ اعمال کنید. اگر $f(x) = ۱$، گیت را به کیوبیت در ثبات ۲ اعمال کنید.

برای عملکرد متعادل، مدارهای مختلفی وجود دارد که می توانیم ایجاد کنیم. یکی از راه‌هایی که می‌توانیم متوازن بودن مدار خود را تضمین کنیم، انجام یک CNOT برای هر کیوبیت در ثبات ۱، با کیوبیت موجود در ثبات ۲ به عنوان هدف است. مثلا:



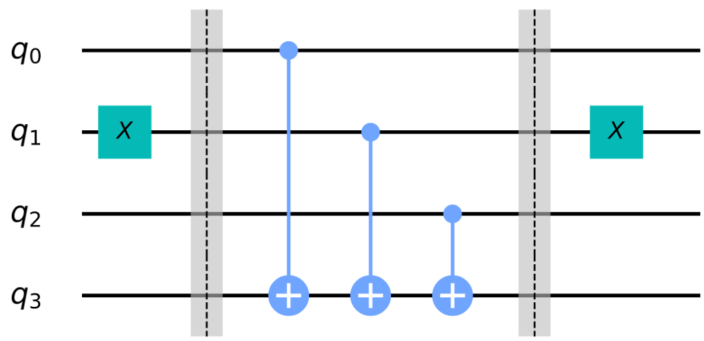
شکل ۸.۳:

در تصویر بالا، سه کیوبیت بالا، رجیستر ورودی را تشکیل می دهند و کیوبیت پایین، ثبات خروجی است. در جدول زیر می‌توانیم ببینیم کدام حالت‌های ورودی کدام خروجی را می‌دهند: ما می توانیم نتایج

حالاتی ورودی که به خروجی صفر منجر می‌شوند	حالاتی ورودی که به خروجی صفر منجر می‌شوند
۰۰۰	۰۰۱
۰۱۱	۱۰۰
۱۰۱	۰۱۰
۱۱۰	۱۱۱

جدول ۱.۳: This is a simple table.

را تغییر دهیم و در عین حال تعادل آنها را با قرار دادن کنترل های انتخاب شده در X-Gates حفظ کنیم. برای مثال، مدار و جدول نتایج آن را در زیر ببینید:



شکل ۹.۳:

حالاتی ورودی که به خروجی صفر منجر می‌شوند	حالاتی ورودی که به خروجی صفر منجر می‌شوند
۰۰۱	۰۰۰
۰۱۰	۰۱۱
۱۰۰	۱۰۱
۱۱۱	۱۱۰

جدول ۲.۳: This is a simple table.

فصل ۴

شبیه‌سازی پدیده‌های کوانتومی

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.

۱.۴ states Bell

در اغلب موارد، سیستم از دو کیوبیت درهمتنیده تشکیل شده‌است. تابع حالت این سیستم‌ها به شکل زیر تعریف می‌شوند:

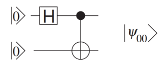
$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

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:

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

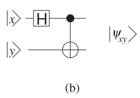
$$|\psi_{xy}\rangle = C_{10}H_1|xy\rangle$$

از آنجایی که چهار حالت $|xy\rangle$ یک مجموعه متعامد هستند و گیت‌های هادامارد و cNOT یکه هستند، چهار حالت درهم تنیده $|\psi_{xy}\rangle$ نیز یک مجموعه متعامد هستند، که به نام پایه Bell نامگذاری شده‌اند. می‌توان رابطه‌ی بالا را یک حالت کلی تعمیم داد:



(آ)
b

شکل ۱.۴: $y = x$



(آ)
b

شکل ۲.۴: $y = 3\sin x$

شکل ۳.۴: (a) A circuit that creates the entangled state ⍰۰۰⍰| = ۱√۲ (|۰۰⍰ + |۱۱⍰) from the unentangled computational-basis state |۰۰⍰. (b) A circuit that creates the four orthonormal entangled Bell states |⍰xy⍰ from the unentangled computational-basis state |xy⍰

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

درنظر داشته باشید که حالات بل قابل تبدیل به یکدیگرند؛ با کمک رابطه‌ی تعمیم یافته می‌توان از هر حالت بل به حالت $|00\rangle$ رسید. توضیحات درباره‌ی تبدیلات بنویس

این روابط به شکل‌های متعدد قابل بیان است که از حوصله‌ی بحث خارج است.

۲.۴ entanglement

۳.۴ رمزگذاری متراکم کوانتومی

رمزگذاری متراکم کوانتومی[۱] یک کاربرد ساده اما شگفت‌انگیز از مفاهیم ابتدایی مکانیک کوانتومی است. این کاربرد، همه ایده‌های اساسی و ابتدایی مکانیک کوانتومی را به روشی ملموس و غیرقابل‌توضیح ترکیب می‌کند، بنابراین مثالی ایده‌آل از اهداف و وظایف پردازش اطلاعات است که می‌توان با استفاده از مکانیک کوانتومی انجام داد.

رمزگذاری متراکم شامل دو طرفین است که به طور معمول به عنوان «آلیس» و «باب» شناخته می‌شوند، که از هم فاصله زیادی دارند. هدف آنها انتقال برخی اطلاعات کلاسیک از آلیس به باب است. فرض کنید آلیس قصد دارد دوبیت داده‌ی کلاسیک را برای باب ارسال کند، اما فقط مجاز است یک کوبیت به باب ارسال کند. آیا می‌تواند به هدف خود برسد؟

رمزگذاری متراکم به ما می‌گوید که پاسخ این سؤال بله است. فرض کنید آلیس و باب در ابتدا یک جفت کوبیت در حالت درهم‌تنیده زیر به اشتراک می‌گذارند:

|؟؟ = |۰۰؟ + |۱۱؟ √۲ . (۱۳۳.۲)

==========

بیانات چی بیتی آلیس می‌تواند با استفاده از این جفت کوبیت‌های درهم‌تنیده، دو بیت کلاسیک را به باب منتقل کند. او این کار را با اعمال یک تبدیل واحد به کوبیت خود انجام می‌دهد، بسته به اینکه می‌خواهد کدام دو بیت کلاسیک را به باب ارسال کند. به عنوان مثال، اگر آلیس می‌خواهد بیت‌های ۰۰ را به باب ارسال کند، او تبدیل ۱ را به کوبیت خود اعمال می‌کند.

این تبدیل واحد باعث می‌شود که کوبیت آلیس و کوبیت باب در یکی از چهار حالت بل اورتوگونال قرار گیرند. اگر آلیس کوبیت خود را در حالت |۰۰؟ قرار دهد، کوبیت باب به طور خودکار به حالت |۰۰؟ تبدیل می‌شود. این بدان معناست که آلیس دو بیت اطلاعات (۰ و ۰) را به باب منتقل کرده است.

باب سپس کوبیت خود را اندازه‌گیری می‌کند و مقدار ۰ یا ۱ را به دست می‌آورد. بسته به مقداری که باب اندازه‌گیری می‌کند، او می‌تواند دو بیت کلاسیک که آلیس به او ارسال کرده است را بازیابی کند.

رمزگذاری متراکم یک پروتکل کوانتومی بسیار کارآمد است که می‌تواند دو بیت کلاسیک را با ارسال یک کوبیت منتقل کند. این پروتکل می‌تواند در کاربردهای مختلفی مانند رمزنگاری کوانتومی و ارتباطات کوانتومی استفاده شود.

==========

همانطور که در شکل ۳.۲ قابل ملاحظه است؛ آلیس و باب، هرکدام یک کیوبیت در اختیار دارند. توجه داشته باشید که Ψ یک حالت ثابت است؛ نیازی نیست که آلیس برای آماده‌سازی این حالت،

[۱] Quantum super dense coding

کوبیتی را به باب ارسال کند. در عوض، ممکن است یک طرف ثالث قبلاً حالت درهم‌تنیده را آماده کند، یکی از کوبیت‌ها را به آلیس و دیگری را به باب ارسال کند.

با ارسال تک کوبیت آلیس به باب، معلوم می‌شود که آلیس می‌تواند دو بیت اطلاعات کلاسیک را به باب منتقل کند. در اینجا روشی که او استفاده می‌کند؛ آورده شده است. اگر او بخواهد رشته‌بیت :

- "00" را ارسال کند $\Longleftarrow$ هیچ کاری روی کیوبیت خود انجام ندهد.
- "01" را ارسال کند $\Longleftarrow$ تبدیل دگرگونی فاز[۲] را روی کیوبیت خود اثر می‌دهد.
- "10" را ارسال کند $\Longleftarrow$ گیت کوانتومی NOT، X، را به کوبیت خود اعمال می‌کند.
- "11" را ارسال کند $\Longleftarrow$ تبدیل iY را به کوبیت خود اعمال می‌کند.

چهار حالت حاصل به راحتی قابل مشاهده هستند:
۰۰ : ⍰⍰| ⍰ |۰۰⍰ + |۱۱⍰ ۲√ (۱۳۴.۲) ۰۱ : ⍰⍰| ⍰ |۰۰⍰ - |۱۱⍰ ۲√ (۱۳۵.۲) ۱۰ : ⍰⍰|
⍰ |۱۰⍰ + |۰۱⍰ ۲√ (۱۳۶.۲) ۱۱ : ⍰⍰| ⍰ |۰۱⍰ - |۱۰⍰ ۲√ . (۱۳۷.۲)

همانطور که در بخش ۶.۳.۱ اشاره کردیم، این چهار حالت به عنوان پایه بل، حالت‌های بل، یا جفت‌های EPR شناخته می‌شوند، به احترام چندین تن از پیشگامان که اولین بار از نوآوری درهم‌تنیدگی قدردانی کردند. توجه داشته باشید که حالت‌های بل یک پایه متعامد هستند، و بنابراین می‌توانند با اندازه‌گیری کوانتومی مناسب از یکدیگر متمایز شوند. اگر آلیس کوبیت خود را به باب بفرستد، و باب هر دو کوبیت را در اختیار داشته باشد، سپس با انجام اندازه‌گیری در پایه بل، باب می‌تواند تعیین کند که کدام یک از چهار رشته بیت ممکن را آلیس ارسال کرده است.

به طور خلاصه می‌توان گفت: آلیس، با تعامل و اثرگذاری تنها روی یک کوبیت، قادر به انتقال دو بیت اطلاعات به باب است. البته دو کوبیت در پروتکل دخیل هستند، اما آلیس هرگز نیازی به تعامل با کوبیت دوم ندارد. از نظر کلاسیک، وظیفه‌ای که آلیس انجام می‌دهد، اگر فقط یک بیت کلاسیک ارسال می‌کرد، غیرممکن بود.

علاوه بر این، پروتکل رمزگذاری متراکم، تا حدی در آزمایشگاه تأیید شده است. یک نکته کلیدی را می‌توان در این مثال زیبا مشاهده کرد: اطلاعات فیزیکی است، و نظریه‌های فیزیکی شگفت‌انگیز مانند مکانیک کوانتوم ممکن است توانایی‌های پردازش اطلاعات شگفت‌انگیزی را پیش‌بینی کنند.

بیانات چی پی تی: پروتکل سوپردنس کدینگ یک پروتکل کوانتومی است که آلیس می‌تواند از آن برای انتقال دو بیت کلاسیک به باب با ارسال یک کوبیت استفاده کند. پروتکل به شرح زیر است:

---
[۲] flip phase

آلیس و باب یک جفت کوبیت درهم‌تنیده را با هم به اشتراک می‌گذارند. آلیس می‌خواهد دو بیت کلاسیک، ۰۰ یا ۰۱ را به باب ارسال کند. آلیس یک عمل واحد بر روی کوبیت خود اعمال می‌کند که بسته به بیت‌هایی که می‌خواهد به باب ارسال کند متفاوت است. آلیس کوبیت خود را به باب می‌فرستد. باب کوبیت را اندازه‌گیری می‌کند و دو بیت کلاسیکی که آلیس به او ارسال کرده است را دریافت می‌کند. اگر آلیس یک عمل واحد بر روی کوبیت خود اعمال نکند، باب فقط می‌تواند یک بیت کلاسیک را دریافت کند. با این حال، اگر آلیس عمل واحد مناسب را اعمال کند، می‌تواند دو بیت کلاسیک را با ارسال یک کوبیت انتقال دهد.

پروتکل سوپردنس کدینگ یک مثال عالی از قدرت مکانیک کوانتوم در انتقال اطلاعات است. این پروتکل نشان می‌دهد که می‌توان با استفاده از قوانین مکانیک کوانتوم، اطلاعات را به روش‌های غیرممکن در فیزیک کلاسیک انتقال داد.

۴.۴ دوربری

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: $|\phi\rangle = 1/\sqrt{2}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

Alice's of state unknown the duplicating prohibits theorem no-cloning he
possible be to out turns it But nearby. or her from away far either Qbit، first
to |⍰⍰ state the assigning in telephone the over cooperate to Bob and Alice for
violated not is theorem no-cloning The pair. entangled the of member Bob's
of either from |⍰⍰ state the of traces all obliterates Alice so doing in because
– Bob to Alice from state the teleporting called – process The Qbits. own her
each For shared. formerly Bob and Alice tanglement en- the eliminates also
term The state. ۱-Qbit single a just teleport can they pair، entangled shared
Qbit Bob's by acquired assignment state the that emphasizes tion" "teleporta-
Here his. to Qbit her from transported been has it Alice's؛ to applies longer no
shares she pair entangled the and Qbit first Alice's works. teleportation how is
،(|۱⍰b |۱⍰a + |۰⍰b (|۰⍰a ۲√۱ (state ۳-Qbit the by characterized are Bob with
Bob's and Alice's in Qbits the for symbols state the given have I where (۲۱.۶)
to Qbit her of state unknown the teleport To . b and a subscripts possession
her using gate، cNOT a applies first Alice pair، entangled the of member Bob's
entangled shared the of member her and control the as |⍰⍰ state the in Qbit first
+ |۰⍰b (|۰⍰a ۲√۱ α|۰⍰a state ۳-Qbit the produces This target. the as pair
a applies she Next (۲۲.۶) .(|۱⍰b |۰⍰a + |۰⍰b (|۱⍰a ۲√۱ ⍰|۱⍰a + (|۱⍰b |۱⍰a
α state the Qbits three all giving Qbit، first her to H transformation Hadamard

۲√۱ (|۱⍰a - (|۰⍰a ۲√۱ ⍰ + (|۱⍰b |۱⍰a + |۰⍰b (|۰⍰a ۲√۱ (|۱⍰a + (|۰⍰a ۲√۱
(α|۰⍰b |۰⍰a |۱⍰a ۲ ۱ + (⍰|۱⍰b + (α|۰⍰b |۰⍰a |۰⍰a ۲ ۱ = (|۱⍰b |۰⍰a + |۰⍰b (|۱⍰a
.(⍰|۰⍰b - (α|۱⍰b |۱⍰a |۱⍰a ۲ ۱ + (⍰|۰⍰b + (α|۱⍰b |۱⍰a |۰⍰a ۲ ۱ + (⍰|۱⍰b -
in remarked (As possession. her in Qbits both measures Alice Now (۲۳.۶)
immediately gates، Hadamard and cNOT of application an such ،۴.۶ Section
the If basis.") Bell the in "measuring called is gates، measurement by followed
possessed originally |⍰⍰ state the acquire indeed will Qbit Bob's ،۰۰ is result
the if But .(⍰۰| to reduced be then would state (whose Qbit first Alice's by
Qbit Bob's of state the then ۱۱ or ،۰۱ ،۱۰ is measurement Alice's of result
of each In (۲۴.۶) . ⍰|۰⍰b - α|۱⍰b or ، ⍰|۰⍰b + α|۱⍰b ، ⍰|۱⍰b - α|۰⍰b becomes
of state the stores re- that transformation unitary a is there cases three these
(which Z apply can we case first the In |⍰⍰. state original Alice's to Qbit Bob's
(which X case، second the in ،(⍰۱| of sign the changes but alone ⍰۰| leaves
I T A T R O P E L TE ۵ . ۶ ZX. case، third the in and ،(⍰۱| and ⍰۰| interchanges
member Bob's to Qbit her of state the transfer to do need Alice all So ۱۵۱ N O
of results the him to report and Bob telephone to is pair entangled their of
been already has state the whether knows then He measurements. two her
must he transformation unitary what or (۰۰ is result Alice's (if transferred
transfer the plete com- to order in pair entangled the of member his to apply
quantum to resemblance the Note three.) other the of one is result Alice's (if
information the acquires Alice measurement a making by correction: error
anybody without state، quantum ular partic- a reconstruct to Bob for needed
be to appears This is. actually state the what about information any acquiring
α numbers complex two by described is Qbit a of state general A remarkable.
requirement the by only constrained values، of continuum a on take that ⍰ and
state whose pair، entangled standard a of aid the with Yet، .۱ = |⍰|۲ + |α|۲ that
described Qbit a with Bob provide to able is Alice ⍰، and α on depend not does
information classical of bits two only of price the at state، unknown the by
entanglement the of loss the and measurements) two her of results the (giving
pair. their of

the Bob to communicate not does process teleportation the course of But the learn to able more no is Bob ⍰. and α in encoded be can that information than |⍰⍰، state the assigned now Qbit، his manipulating from ⍰ and α of values state same the assigned was that Qbit her was it when do to able was Alice of stage crucial a at produced be could state Alice's hand other the On |⍰⍰. him enable could Bob to transfer its and computation، quantum elaborate an computer، quantum far-away own his on computation the with continue to dense Like teleportations. such by objective nontrivial a achieve can one s elementary an manipulating by constructed be also can teleportation coding، –(۲۱.۶) in analysis the of any through going without diagram، circuit classical of |x⍰ = |⍰⍰ state the exchanges that circuit a shows (a)۵.۶ Figure .(۲۴.۶) .۱ or ۰ = x whether of regardless Cbit، Bob's of ⍰۰| state the with Cbit Alice's As Cbits. two the between coupling physical direct by achieved is transfer The arbitrary for exchange this perform to continues it circuit quantum linear a be can protocol teleportation entire The ⍰|۱⍰. + α|۰⍰ = |⍰⍰ superpositions، with ،(a)۵.۶ Figure in gates two the expanding appropriately by constructed direct the eliminate to is expansion the of aim The Qbit. ancillary an of aid the in gates cNOT two the through Qbits Bob's and Alice's between interaction the and Bob، to Alice from message telephoned the of favor in ،(a)۵.۶ Figure (which Qbits entangled of pair shared their produce to necessary interaction |⍰⍰). state the in Qbit her acquired even has Alice before well place take can

۱

oracle a determine to how