
بسم الله الرحمن الرحيم

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

بررسی کمینه‌ها در مسائل پیچیدگي ارتباطی کوانتومي در حوزه پردازش موازی

گزارش پروژه

محیا جمشیدیان

اساتید راهنما

دکتر مریم موزرانی

دکتر رامین جوادی

۹ شهریور ۱۳۹۹

فهرست مطالب

فصل اول

مقدمه

مباحث نظری مربوط به پیچیدگی ارتباطی، پس از طرح اولیه آن‌ها توسط Yao در سال ۱۹۷۹، در حیطه‌های مختلفی استفاده شده‌اند. این کاربردها، در زمینه‌های متنوعی مانند الگوریتم‌های جریانی، نظریه بازی‌ها طراحی مدارهای VLSI و ... یافت می‌شوند. در نتیجه، این کاربردهای متنوع تحقیقات زیادی را در این زمینه شامل شده است.

محاسبات کوانتومی، مبحث جدیدی در علوم کامپیوتر است که با وجود عمر کوتاه، تغییرات زیادی را در تصور و درک ما نسبت به نظریه محاسبات و پیچیدگی محاسباتی ایجاد کرده است. طراحی و انتشار این الگوریتم‌ها ـ مانند الگوریتم شور [1] برای به‌دست آوردن عوامل اول یک عدد دلخواه در زمان بهینه ـ محققان را به پرسش این سوال دعوت می‌کند که آیا در مباحث و حوزه‌های دیگر پیچیدگی محاسباتی نیز، امکان یافت الگوریتم‌های بهینه‌تری وجود دارد یا خیر؟

در ادامه، پس از معرفی این حوزه‌ها و مباحث نظری پایه‌ای موردنیاز، به بررسی چند مسئله به شکل بالا

[1] Shore

می‌پردازیم و تلاش می‌کنیم با شبیه‌سازی آن‌ها، از پیچیدگی و زمان اجرای آن‌ها مطلع شویم.

فصل‌های دوم تا چهارم، به مباحث تئوری بنیادین پیچیدگی ارتباطی ـ پیچیدگی قطعی، غیرقطعی و تصادفی ـ می‌پردازند. سپس در فصل پنجم، کاربرد خاصی از آن‌ها در حالت کلاسیک مطرح شده و نتایخ به مشاهده‌شده را برای به‌دست آوردن نتایجی در آن زمینه‌ها بیان خواهند شد.

از فصل ششم، مکانیک کوانتومی معرفی خواهد شد. این فصل مقدمه تاریخی و نظری روی اصول مکانیک کوانتومی و پدیده‌های غیرمنتظره آن‌هاست. در این فصل، دانش کلی‌ای در مورد جبرخطی و ریاضیات موردنیاز فرض شده است و به همین دلیل، در پیوست اول مقدمه‌ای بر مبانی ریاضی مکانیک کوانتومی آورده شده است.

در دو فصل بعد، الگوریتم‌های کوانتومی را بررسی می‌کنیم. فصل هفتم در مورد الگوریتم‌های معروف را مطرح می‌کند و فصل هشتم، حالت توزیع‌شده و ارتباطی آن‌ها را بررسی خواهد کرد. در نهایت، فصل آخر شبیه‌سازی چندی از این الگوریتم‌ها را دربرخواهد داشت.

فصل دوم

پیچیدگی ارتباطی

مدل پیچیدگی ارتباطی در ابتدا در سال ۱۹۷۰ توسط Yao معرفی شد و هدف آن این است که یک مساله را به صورت توزیع‌شده[1] حل کند. منظور از حل به صورت توزیع‌شده آن است که افراد مختلف، با در دست داشتن آرگومان‌های مختلف از یک مساله مشخص، با همکاری هم به حل مساله بپردازند. مهم‌ترین نکته در این مدل این است که افراد دخیل در مخابره، قدرت محاسباتی نامحدود دارند و تنها فاکتور مورد بررسی، مقدار پیام‌های رد و بدل شده میان آن‌هاست. مطالب این فصل با اقتباس از [۱۰، ۱۱، ۱۴–۱۶] تهیه شده است.

۲ـ۱ تعریف

یک پروتکل قطعی پیچیدگی ارتباطی، پروتکلی مانند π است که در هر مرحله، یکی از دو طرف مخابره، پیامی یک بیتی به دیگری می‌فرستد. آلیس (A) ورودی $x \in X$ را در اختیار دارد و باب (B) ورودی $y \in Y$. هدف این پروتکل این خواهد بود که این دو نفر با هم خروجی $z \in Z$ را محاسبه کنند، به صورتی که:

$$val(\pi(x,y)) = f(x,y) \quad \forall x \in X, y \in Y$$

که در آن f یک تابع دانسته توسط دو طرف است.

[1] Distributed

درخت پروتکل: معادل با تعریف بالا، می‌توان یک درخت پروتکل باینری در نظر گرفت که رئوسش تصمیم‌ها (بیت‌های ارسال شده) توسط بازیکنان و برگ‌هایش خروجی‌ها هستند:

- هر یک از رئوس غیر برگ درخت یا به آلیس تعلق دارند و یا باب.
- هر راس داخلی v که به آلیس تعلق دارد، معادل با تابع $A_v : X \to \{0,1\}$ است که بیت فرستاده‌شده توسط آلیس را وقتی به این راس برسد، با توجه به ورودی وی تعیین می‌کند.
- هر راس داخلی v که به باب تعلق دارد، معادل با تابع $B_v : X \to \{0,1\}$ است که بیت فرستاده‌شده توسط باب را وقتی به این راس برسد، با توجه به ورودی وی تعیین می‌کند.
- هر برگ این درخت (l) یک مقدار $val(l) \in Z$ دارد.

هر جفت ورودی $x \in X, y \in Y$ در مدل قطعی، یک مسیر یکتا از ریشه تا یک برگ را تعیین می‌کنند. هزینه یک پروتکل، معادل با عمق درخت (بلندترین مسیر از ریشه تا برگ) است که با $D(f)$ مشخص می‌شود.

از آنجایی که آلیس می‌تواند کل رشته‌اش را برای باب بفرستد و این حداکثر مکالمه مورد نیاز بین دو طرف است، برای یک تابع $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$، $D(f) \leq n+1$ است.

نکته قابل توجه این است که همواره می‌توان یک درخت پروتکل را متوازن کرد. به عبارت دیگر، یک درخت پروتکل با Nتا برگ با درخت پروتکل دیگری با عمق $O(log\ N)$ معادل است. به بیان دیگر، عمق درخت به عنوان یک شاخص برای اندازه‌گیری پیچیدگی ارتباطی، به جز یک ضریب ثابت، با لگاریتم تعداد برگ‌های درخت معادل است.

۲ـ۲ تکنیک‌های کمینه‌یابی

زمانی که صحبت از پیچیدگی به میان می‌آید، لازم است که مشخص شود یک مساله مشخص حداقل به چه مقدار زمان یا حافظه برای رسیدن به جواب نیاز دارد. در مورد مسائل پیچیدگی ارتباطی، پیچیدگی مورد نظر همان تعداد بیت مخابره شده بین افراد مکالمه است. منظور از کمینه[1] برای این نوع پیچیدگی، کمترین تعداد بیت‌هایی است که بین دو نفر جابه‌جا خواهد شد تا پاسخ مساله p با سایز ورودی n بر دو طرف آشکار باشد. در مورد پیچیدگی ارتباطی و کمینه‌هایش در ابتدای راه قرار داریم ولی در حال حاضر تکنیک‌های سومندی برای مشخص کردن کمینه یک مساله تعریف و استفاده شده‌اند که ابتدا مفاهیم اولیه پیش‌نیاز را مطرح خواهیم کرد و در ادامه به بررسی هر یک از ابزارها می‌پردازیم.

[1] lower-bound

۲ـ۲ـ۱ ماتریس مشخصه

با توجه به تابع از قبل مشخص $f : X \times Y \to \{0,1\}$، ماتریس مشخصه[1] تابع f به صورت زیر است:

$$M_f = [f(x,y)]_{x\in X, y\in Y}$$

اگر $X = \{x_1, x_2, ..., x_m\}$ و $Y = \{y_1, y_2, ..., y_n\}$، شکل ماتریس M_f موردنظر به صورت زیر است:

$$\begin{bmatrix} f(x_1,y_1) & f(x_1,y_2) & \cdots & f(x_1,y_n) \\ f(x_2,y_1) & f(x_2,y_2) & \cdots & f(x_2,y_n) \\ \vdots & \vdots & \ddots & \vdots \\ f(x_m,y_1) & f(x_m,y_2) & \cdots & f(x_m,y_n) \end{bmatrix}$$

توجه کنید که که در مبحث پیچیدگی ارتباطی، می‌توانیم از تمامی هزینه‌ها به جز بیت‌های مخابره شده صرف نظر کنیم، چرا که برای هر یک از شرکت کنندگان قدرت محاسباتی بی‌نهایت در نظر گرفته‌ایم.

۲ـ۲ـ۲ پروتکل، درخت و مستطیل‌ها

قبلا در مورد نمایش درختی یک پروتکل صحبت کردیم، اینجا می‌خواهیم ارتباط بین پروتکل، درخت و مستطیل را نشان می‌دهیم. به منظور تفهیم بهتر، فرض کنید که $X = Y = \{00, 01, 10, 11\}$ و تابع

X \ Y	00	01	10	11
00	0	0	0	1
01	0	0	0	1
10	0	0	0	0
11	0	1	1	1

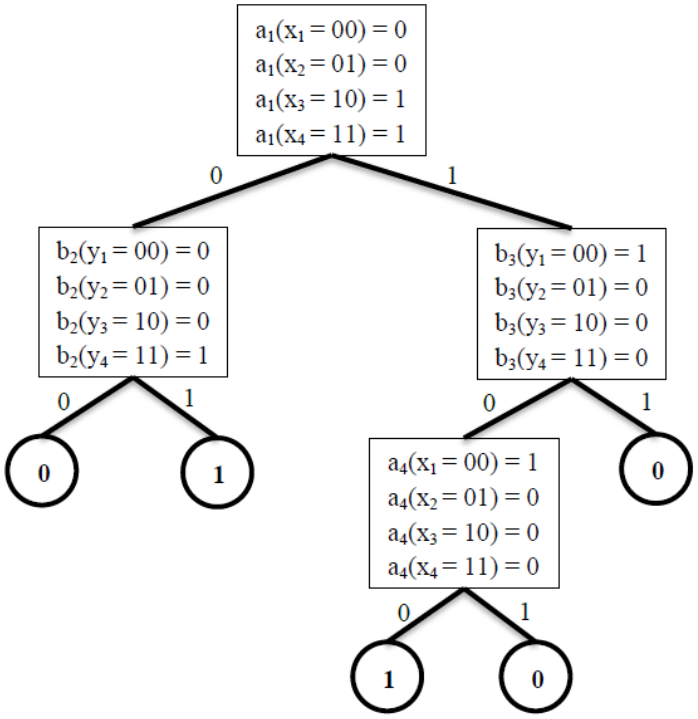
شکل ۲ـ۱: ماتریس مشخصه یک تابع دلخواه $f : X \times Y \to \{0,1\}$ با $X = Y = \{00, 01, 10, 11\}$.

$f : X \times Y \to \{0,1\}$ به واسطه ماتریس مشخصه خود در ۲ـ۲ـ۲ داده شده باشد. یک پروتکل معتبر برای f در شکل ۲ـ۲ـ۲ نشان داده شده است.

۲ـ۲ـ۳ قطعه بندی

تعریف ۱. تابع $f : X \times Y \to \{0,1\}$ را در نظر بگیرید. یک زیر مجموعه $S \subseteq X \times Y$ از fـ تک‌رنگی[2] است اگر تابع f روی S ثابت باشد.

[1] Characteristic Matrix
[2] f-monochromatic



شکل ۲ـ۲: یک پروتکل صحیح برای مخابره تابع مشخص‌شده در زیرقسمت ۲ـ۲ـ۲

قضیه ۱. مجموعه ورودی‌های $(x, y) \in X \times Y$ که به یک برگ مشخص از درخت پروتکل ختم می‌شود، یک مستطیل است.

نتیجه: هر پروتکل قطعی برای تابع f، مجموعه $X \times Y$ را به مستطیل‌های fـتک‌رنگی جدا از هم قطعه‌بندی[1] می‌کند. در واقع، حداکثر تعداد مستطیل‌ها 2^C است که C هزینه ارتباطی پروتکل است (ارتفاع درخت).

بیشینه‌ای که در نتیجه فوق مطرح شده‌است از جایی برمی‌آید که درختی با ارتفاع C نمی‌تواند بیشتر از 2^C برگ داشته باشد.

توجه کنید که هر پروتکل، ماتریس مشخصه را به تعدادی مستطیل قطع بندی خواهد کرد ولی هر قطعه‌بندی لزوما معادل یک پروتکل نیست. به عنوان مثال، در شکل ۲ـ۲ـ۳ نمی‌توان یک پروتکل پیدا کرد چرا که هیچ برشی نیست که بتواند یک زیرماتریس را به دو ماتریس دیگر تبدیل کند (اولین قدم پروتکل اجرایی نیست).

[1] partition

X \ Y	00	01	10	11
00	0	0	0	1
01	0	0	0	1
10	0	0	0	0
11	0	1	1	1

شکل ۲ـ۳: قطع‌بندی‌ای که نمی‌تواند به یک پروتکل نظیر شود. هیچ برشی در قطعه‌بندی وجود ندارد که با انتخاب آن، ماتریس به دو زیرماتریس تبدیل شود.

۲ـ۲ـ۴ مجموعه گول‌زننده

به عنوان یک روش برای محاسبه کردن کمینه پیچیدگی ارتباطی یک مساله، می‌توانیم از ابزاری به نام مجموعه گول زننده[1] استفاده کنیم.

تعریف ۲. تابع $f : X \times Y \to \{0,1\}$ داده شده است. یک مجموعه $S \subseteq X \times Y$ را مجموعه گول زننده می‌نامند اگر یک مقدار $z \in \{0,1\}$ وجود داشته باشد به طوری که:

- برای هر $(x,y) \in S$ داشته باشیم $f(x,y) = z$.
- برای هر دو عضو متفاوت (x_1,y_1) و (x_2,y_2) در S، یا $f(x_1,y_2) \neq z$ یا $f(x_2,y_1) \neq z$.

قضیه ۲. پیچیدگی ارتباطی تابع f از نامساوی زیر پیروی می‌کند،

$$D(f) \geq log_2|S|$$

که S هر مجموعه گول زننده‌ای برای f است.

اثبات. هیچ دوعضوی از مجموعه گول‌زننده S طبق تعریف نمی‌توانند عضو یک مستطیل در قطعه‌بندی باشند، درنتیجه حداقل به تعداد اعضای S، مستطیل fـتک‌رنگی داریم. طبق نتیجه قبل، حکم ثابت می‌شود.

□

[1] Fooling Set

مثال ۱. تابع مساوی را در نظر بگیرید. از قبل می‌دانیم حداکثر تعداد بیت‌هایی که باید برای این مساله مخابره شود n است. حال می‌خواهیم نشان دهیم که این تعداد، حداقل هم هست. تعریف تابع مساوی: EQ_n $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ به صورت زیر خواهد بود

$$EQ_n(x,y) = \begin{cases} 1 & \text{x=y} \\ 0 & \text{در غیر این صورت} \end{cases} \qquad (۱-۲)$$

ماتریس مشخصه این تابع همان ماتریس همانی $2^n \times 2^n$ است.

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

مجموعه گول زننده در این حالت همه مقادیر 1 تابع f است. چرا که هیچ دوتایی از ورودی‌هایی که خروجی 1 دارند، در یک مستطیل نمی‌توانند باشند.

۲-۲-۵ کران اندازه مستطیل

کران اندازه مستطیل[1] یک روش دیگر برای اثبات کردن کمینه‌های توابع بولی مورد استفاده در پیچیدگی ارتباطی است. ایده پشت این ماجرا، ثابت کردن آن است که اندازه هر مستطیل کوچک است، در نتیجه باید تعداد زیادی مستطیل برای پوشاندن کل ماتریس مشخصه داشته باشیم.

ایده: تابع $f : X \times Y \to \{0,1\}$ داده شده است. روی اعضای $f^{-1}(1)$ یک توزیع احتمال μ تعریف می‌کنیم به طوری که برای هر مستطیل R شامل مقادیر 1، $\mu(R)$کوچک باشد. به همین طریق می‌توانیم برای مقادیر 0 هم این روند را تکرار کنیم.

مثال ۲. نشان می‌دهیم که مجموعه گول‌زننده یک مدلی از کران اندازه مستطیل است. فرض کنید که مجموعه گول‌زننده S را داشته باشیم و $|S| = t$. حال μ را یک توزیع یکنواخت روی اعضای S درنظر بگیرید. در نتیجه

$$\mu(x,y) = \begin{cases} 1/t & (x,y) \in S \\ 0 & \text{در غیر این صورت} \end{cases} \qquad (۲-۲)$$

نشان دادیم که هیچ دو عضوی از مجموعه S نمی‌توانند در یک مستطیل fـتک‌رنگی باشند. در نتیجه، برای هر مستطیل R داریم $\mu(R) \leq 1/t$ و در نهایت باید $\frac{1}{\frac{1}{t}}$ برگ در درخت پروتکل وجود داشته باشد و این گواهی بر این است که $D(f) \geq \lceil \log_2 t \rceil$.

[1] Rectangle Size Bounds

۲ـ۲ـ۶ کمینه رتبه ماتریس [1]

قضیه ۳. تابع $f : X \times Y \to \{0,1\}$ داده شده است. داریم $D(f) \geq \log_2(2 \times rank_F(M_f - 1))$ بر روی هر میدان F.

اثبات. در قسمت‌های قبل نشان دادیم که پیچیدگی ارتباطی تابع مساوی برابر n است. حال با استفاده از رتبه، این را نشان می‌دهیم:

از آنجایی که ماتریس مشخصه تابع مساوی ماتریس همانی $2^n \times 2^n$ است، و رتبه این ماتریس برابر 2^n است، طبق قضیه قبل پیچیدگی ارتباطی این مساله n است. □

[1] Matrix Rank

فصل سوم

پیچیدگی ارتباطی غیرقطعی

در این بخش، سعی بر این است که مشابه تئوری پیچیدگی محاسباتی، مدل غیرقطعی[1] را در پیچیدگی ارتباطی نیز تعریف کنیم. مطالب این فصل با اقتباس از [۲، ۱۰، ۱۱، ۱۴–۱۶] تهیه شده است.

برای هر تابع بولی $f : X \times Y \to \{0,1\}$، یک پروتکل غیرقطعی دو بخش خواهد داشت. در ابتدا، یک پیشگو[2] که به ورودی هر دو طرف دسترسی دارد یک رشته a را به هر دو طرف می‌دهد. در مرحله دوم، بازیکنان با در اختیار داشتن این رشته و ورودی‌های خودشان، پروتکل را مانند قسمت قطعی ادامه می‌دهند و در مورد مقدار تابع تصمیم می‌گیرند. اگر خروجی را با $\Pi(x,y,a)$ نشان دهیم، این پروتکل مقدار f را به درستی محاسبه می‌کند اگر:

$$f(x,y) = 1 \ \Rightarrow \exists a, \Pi(x,y,a) = 1$$

$$f(x,y) = 0 \ \Rightarrow \forall a, \Pi(x,y,a) = 0$$

هزینه این پروتکل، جمع حداکثر طول رشته a و حداکثر تعداد بیت‌های مخابره شده بین دو طرف است. هزینه غیرقطعی محاسبه f که با $N^1(f)$ نشان داده می‌شود، حداقل هزینه پروتکلی‌ست که f را محاسبه می‌کند. متناظر

[1] Non-deterministic
[2] Oracle

با این تعریف، هزینه co-nondeterministic برای تابع f به همین شکل بیان و با $N^0(f)$ نشان داده می‌شود.

مثال ۳. تابع نامساوی را درنظر بگیرید. تعریف رسمی این تابع به شکل زیر می‌باشد:

$$NEQ_n(x,y) = \begin{cases} 0 & \text{x=y} \\ 1 & \text{در غیر این صورت} \end{cases} \qquad (۱-۳)$$

و ماتریس مشخصه آن نیز به این شکل است:

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}$$

هزینه محاسبه غیرقطعی این تابع $(N^1(NEQ))$ برابر $O(\log n)$ است. برای مشاهده این موضوع، دقت کنید که اگر دو ورودی متفاوت باشند، پیشگو می‌تواند شماره بیت اختلاف را به عنوان رشته اولیه به هر دو طرف ارسال کند. در نتیجه، هزینه کل پروتکل برابر طول رشته کمک اولیه $(O(\log n))$ و هزینه چک کردن آن بیت خواهد بود. (آلیس بیت مشخص شده را برای باب ارسال می‌کند، باب مشاهده می‌کند که رشته‌ها متفاوت هستند. این عمل به یک بیت مخابره نیاز دارد.)

در جهت دیگر، مشاهده کنید که اگر دو ورودی با هم مساوی باشند، هیچ رشته اولیه‌ای وجود ندارد که پیشگو بتواند در ابتدا به هر دو طرف ارسال کند و فرآیند چک کردن تساوی را آسان‌تر نماید. پس برای این تابع، $N^0(NEQ) = O(n)$ خواهد بود.

۳ـ۱ پوشش‌ها

مشابه ارتباط پیچیدگی قطعی با مستطیل‌ها، پیچیدگی غیرقطعی ارتباط مستقیمی با پوشش‌ها[1] دارد.

تعریف ۳. برای هر $z \in \{0,1\}$، یک zـپوشش[2] برای f، مجموعه‌ای از مستطیل‌های $R_1, \ldots, R_N$ است که ممکن است اشتراک داشته باشند، به طوری که $f^{-1}(z) = \cup R_i$. حداقل سایز یک پوشش-z برای f را با $C^z(f) = N$ نشان .می‌دهیم

قضیه ۴. برای $z \in \{0,1\}$ داریم: $N^z(f) = \log C^z(f) + O(1)$ به عبارت دیگر، ارتباط هزینه مخابره غیرقطعی با پوشش‌ها معادل مخابره قطعی با مستطیل‌هاست.

---
[1] Covers
[2] z-Cover

۳ـ۲ کلاس‌های پیچیدگی

یکی از بزرگ‌ترین مسائل باز موجود در پیچیدگی محاسباتی، درستی تساوی $\mathbf{P} = \mathbf{NP} \cap \mathbf{coNP}$ است. در این قسمت، سعی می‌کنیم تعاریف مشابهی برای کلاس‌های متناظر آن‌ها بیان کنیم و این تساوی را در پیچیدگی ارتباطی اثبات کنیم.

تعریف ۴. برای یک تابع دودویی $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ داریم:

- $D(f) = polylog(n) \;\Rightarrow\; f \in \mathbf{P}^{CC}$
- $N^1(f) = polylog(n) \;\Rightarrow\; f \in \mathbf{NP}^{CC}$
- $N^0(f) = polylog(n) \;\Rightarrow\; f \in \mathbf{coNP}^{CC}$

که در آن $polylog(n) = O(\log^c n)$ است.

لم ۱. برای هر تابع دودویی، $D(f) = O(N^0(f)N^1(f))$

قضیه ۵.

$$P^{CC} = NP^{CC} \cap coNP^{CC}$$

اثبات. مشاهده جهت اول، مشخص است. مجموعه P^{CC} زیر مجموعه هر دو مجموعه NP^{CC} و $coNP^{CC}$ است و پس زیرمجموعه اشتراک آن‌ها نیز خواهد بود.
برای اثبات قسمت دوم، مشاهده می‌کنیم که از آن‌جایی که طبق تعریف، اگر تابعی هم در NP^{CC} و هم در $coNP^{CC}$ باشد، پس $N^1(f) = O(\log^{c_1} n)$ و $N^0(f) = O(\log^{c_2} n)$ خواهد بود. حال از لم ۱ استفاده می‌کنیم.

$$D(f) = O(N^0(f)N^1(f)) \Rightarrow D(f) = O(N^0(f)N^1(f)) = O(\log^{c_1} n \ \log^{c_1} n) = O(\log^c n)$$

□

۳ـ۳ تکنیک‌های کمینه‌یابی

تکنیک‌های کمینه‌یابی برای پیچیدگی غیرقطعی به طور مستقیم از لم قبل نتیجه می‌شوند.

$$N^1(f) \geq \Omega(\frac{D(f)}{N^0(f)})$$

و یا از معادل آن استفاده می‌کنند:

لم ۲. برای هر تابع دودویی، نتایج زیر برقرار است:

$$D(f) = O(N^1(f)\log(\text{rank}(M_f))) \Rightarrow N^1(f) \geq \Omega(\frac{D(f)}{\log(\text{rank}(M_f))})$$

$$D(f) = O(N^0(f)\log(\text{rank}(M_f))) \Rightarrow N^0(f) \geq \Omega(\frac{D(f)}{\log(\text{rank}(M_f))})$$

۳ـ۴ نتیجه‌گیری

تا به حال، چندی از ملاک‌های سنجش پیچیدگی ارتباطی را بررسی کردیم. ارتباط کلی آن‌ها به شکل زیر است:

$$2^{\Theta(\sqrt{D(f)})} \leq C(f) \leq C^D(f) \leq C^P(f) \leq 2^{\Theta(D(f))} \qquad (۲ـ۳)$$

- $C^P(f)$ کم‌ترین تعداد برگ‌های درخت پروتکل برای تابع f است.
- $C^D(f)$ کم‌ترین تعداد مستطیل‌ها در یک تقسیم‌بندی برای تابع f است.
- $C^z(f)$ حداقل سایز یک پوشش-z برای تابع f است.
- $C(f) = C^0(f) + C^1(f)$

نامساوی اول مستقیما از لم ۱ نتیجه می‌شود. دو نامساوی اول نیز در فصل قبل اثبات شده‌اند.

فصل چهارم

پیچیدگی ارتباطی تصادفی

استفاده از تصادف در بسیاری از حوزه‌های الگوریتمی، کاربرد زیادی دارد و پیچیدگی ارتباطی نیز از این امر مستثنا نیست. در این قسمت، سه مدل پیچیدگی تصادفی را بررسی خواهیم کرد و علاوه بر ارتباط آن‌ها، چند تکنیک به‌دست آوردن کمینه را نیز در نظر خواهیم گرفت. [۱۰، ۱۱، ۱۴–۱۶]

۴ـ۱ مدل سکه خصوصی

این مدل بر فرض این که هر یک از بازیکنان به مقدار نامحدودی از بیت‌های رندوم دسترسی دارند. این مدل نیز مانند مدل قطعی، با یک درخت پروتکل قابل نمایش است.

تعریف درخت پروتکل برای مدل سکه خصوصی[1] به شکل زیر خواهد بود. در هر راس درخت (v)، توابع مشخص‌کننده مسیر A_v, B_v توابع تصادفی هستند. به بیان دیگر، $A_v : X \to [0,1]$ احتمال انتخاب فرزند سمت راست را مشخص می‌کند. برای تعریف دقیق محاسبه یک تابع f، بیت‌های رندوم آلیس و باب را به ترتیب با r_A, r_B نمایش می‌دهیم.

[1] Private Coin

تعریف ۵. می‌گوییم پروتکل تصادفی Π تابع $f : X \times Y \to Z$ را با خطای ϵ محاسبه می‌کند اگر:

$$\Pr_{r_A, r_B}[\Pi(x, y; r_A, r_B) = f(x, y)] \geq 1 - \epsilon \quad \forall x \in X, y \in Y. \tag{۱-۴}$$

هزینه پروتکل تصادفی مثل حالت قطعی، برابر تعداد بیت‌های مبادله‌شده (عمق درخت پروتکل) خواهد بود. حداقل هزینه پروتکلی که f را با خطای ϵ محاسبه می‌کند را با $R_\epsilon(f)$ نمایش می‌دهیم. به علاوه، در مسائل مربوط به پیچیدگی محاسباتی $\epsilon = \frac{1}{3}$ در نظر گرفته می‌شود و داریم $R(f) = R_{\frac{1}{3}}(f)$.
در تمام پروتکل‌های تصادفی، می‌توان با تکرار پروتکل و انتخاب پر تکرارترین پاسخ، احتمال جواب درست را افزایش داد. در نتیجه:

$$R_\epsilon(f) = O(\log \frac{1}{\epsilon}).R(f) \tag{۲-۴}$$

۴-۲ مدل سکه عمومی

این مدل، فرض می‌کند بیت‌های عمومی نامحدود در اختیار آلیس و باب، مشترک هستند. این بیت‌های مشترک را با r نمایش‌داده و داریم:

تعریف ۶. می‌گوییم پروتکل تصادفی Π تابع $f : X \times Y \to Z$ را با خطای ϵ و سکه‌های عمومی[1] محاسبه می‌کند اگر:

$$\Pr_{r}[\Pi(x, y; r) = f(x, y)] \geq 1 - \epsilon \quad \forall x \in X, y \in Y. \tag{۳-۴}$$

هزینه حداقل پروتکلی که تابع f را با سکه عمومی محاسبه می‌کند را با $R^{pub}_\epsilon(f)$ نمایش می‌دهیم. به شکل مشابه، از تکرار برای افزایش دقت این مدل نیز می‌توان استفاده کرد.

مثال ۴. حال از مدل‌های بررسی‌شده، برای طراحی پروتکل‌هایی برای تابع تساوی استفاده می‌کنیم.

- مدل سکه خصوصی:

۱. آلیس یک عدد اول به صورت تصادفی از مجموعه $\{2, \ldots, 2n\}$ انتخاب می‌کند.

۲. آلیس عدد اول انتخاب شده (p) و مقدار $x \mod p$ را به باب ارسال می‌کند.

۳. باب چک می‌کند که آیا $y \mod p$ برابر با عدد دریافتی هست یا خیر. اگر برابر بود ۱ و اگر برابر نبود صفر برمی‌گرداند.

[1] Public Coin

مشخص است که اگر دو عدد با هم برابر باشند، نتیجه این پروتکل همواره درست خواهد بود. ولی اگر $x \neq y$ باشد، ممکن است اعداد اولی وجود داشته باشند به صورتی که $x \mod p = y \mod p$. پس در این حالت، خطا وجود خواهد داشت. حال تلاش می‌کنیم مقدار خطا را محاسبه کنیم.

فرض کنید که مجموعه $\{p_1, p_2, \ldots, p_k\}$ مجموعه تمام اعداد اولی باشد که $x \mod p_i = y \mod p_i$. در نتیجه:

$$x \mod P = y \mod P \quad P = p_1 p_2 \ldots p_k$$

حال از آنجایی که $p_i \geq 2$ است، $P \geq 2^k$ خواهد بود. ولی P نمی‌تواند بیش‌تر از 2^n باشد، چون $x \neq y$ است. پس $2^k \leq 2^n$ است و $k \leq n$ خواهد بود. حال از آنجایی که عدد اول از مجموعه‌ای به اندازه $2n$ انتخاب شده است، احتمال این که یکی از این اعداد اول به تصادف انتخاب شود کمتر از $\frac{1}{2}$ خواهد بود. (و این احتمال با تکرار می‌تواند کمتر شود.)

هزینه این پروتکل $O(\log n)$ است. توجه کنید که حداقل مقدار مخابره برای حالت قطعی، $O(n)$ است.

- مدل سکه عمومی: ($r = r_1 \ldots r_m$ بیت‌های تصادفی مشترک هستند.)

۱. آلیس مقدار زیر را محاسبه کرده و برای باب را ارسال می‌کند:

$$\sum_{i=1}^{n} x_i r_i \mod 2$$

۲. باب مقدار زیر را محاسبه کرده، با مقدار فرستاده شده توسط آلیس مقایسه می‌کند. اگر برابر بودند ۱ و در غیر این صورت صفر خروجی می‌دهد.

$$\sum_{i=1}^{n} y_i r_i \mod 2$$

همچنان مشخص است که اگر این دو ورودی با هم برابر باشند، جواب حتما درست است. ولی اگر تساوی برقرار نباشد، به احتمال $1/2$ ممکن است جواب اشتباه تشخیص داده شود و مثل حالت قبل، می‌توان با تکرار احتمال خطا را کم کرد. نکته دیگر، این است که در این مدل، فقط با فرستادن یک بیت اطلاعات نتیجه مشخص می‌شود و پیچیدگی برابر با $O(1)$ خواهد بود.

همان‌طور که از مثال بالا مشخص است، مدل سکه عمومی از سکه خصوصی قوی‌تر است، یعنی با مدل عمومی می‌توان بدون هزینه اضافی مدل خصوصی را شبیه‌سازی کرد، ولی نه برعکس. در نتیجه:

$$R_\epsilon^{pub}(f) \leq R_\epsilon(f)$$

شبیه‌سازی مدل عمومی با مدل خصوصی نیز ممکن است، ولی با مقداری هزینه همراه خواهد بود. لم نیومن[1] نتیجه این شبیه‌سازی را بیان می‌کند.

قضیه ۶. اگر $f : \{0,1\}^n \times \{0,1\}^n \to Z$ باشد، برای هر مقدار $\epsilon, \delta \geq 0$ داریم:

$$R_{\epsilon+\delta}(f) \leq R^{pub}_{\epsilon}(f) + O(\log n + \log \frac{1}{\delta}) \qquad (۴\text{ـ}۴)$$

۴ـ۳ مدل توزیعی

تا به حال در تمام مدل‌های بررسی شده، عنصر تصادف در عملکرد پروتکل بوده است. در مدل توزیعی[2] ورودی را تصادفی فرض می‌کنند.

تعریف ۷. فرض کنید μ یک توزیع روی $X \times Y$ است. می‌گوییم پروتکل تصادفی توزیعی Π تابع $f : X \times Y \to Z$ را با خطای ϵ و تحت μ محاسبه می‌کند اگر:

$$\Pr_{(x,y)\sim\mu}[\Pi(x,y) = f(x,y)] \geq 1 - \epsilon \quad \forall x \in X, y \in Y. \qquad (۵\text{ـ}۴)$$

تکنیک‌های کمینه مدل‌های تصادفی که در بخش بعد بررسی خواهند شد، یک توزیع «دشوار» روی ورودی‌ها پیدا می‌کنند و نشان می‌دهند که هیچ پروتکل قطعی و بهینه‌ای نمی‌تواند تابع مورد نظر را تحت این توزیع محاسبه کند. این تکنیک بر قضیه زیر که توسط Yao اثبات شده است مبتنی‌ست:

قضیه ۷. اگر $f : X \times Y \to Z$ و $\epsilon \geq 0$ باشد، داریم:

$$\max_{\mu} D^{\mu}_{\epsilon} = R^{pub}_{\epsilon}(f) \qquad (۶\text{ـ}۴)$$

۴ـ۴ کمینه‌یابی

۴ـ۴ـ۱ ناهمگنی

همانطور که در قسمت قبل بیان شد، استفاده از یک توزیع سخت، و نشان دادن کمینه‌ای برای پروتکل قطعی‌ای که ورودی را تحت آن توزیع محاسبه می‌کند، با کمینه محاسبه همان تابع توسط یک پروتکل تصادفی سکه عمومی برابر است. برای استفاده از این نکته، مفهوم جدیدی را تعریف می‌کنیم:

تعریف ۸. اگر $f : X \times Y \to Z$ و μ یک توزیع روی $X \times Y$ باشد، می‌توان برای هر مستطیل R ناهمگنی

[1] Newman's lemma
[2] Distributional

[1] را به صورت زیر تعریف کرد:

$$disc_\mu(f,R) = |\mu(R \cap f^{-1}(0) - \mu(R \cap f^{-1}(1)| \qquad (۷\text{ـ}۴)$$

و

$$disc_\mu(f) = \max_R \ disc_\mu(f,R). \qquad (۸\text{ـ}۴)$$

به صورت غیررسمی، معیار ناهمنگی پایین یعنی مستطیل‌های بزرگ تعداد تقریبا برابری صفر و یک دارند. این معیار را به یک شکل مشابه نیز می‌توان تعریف کرد. در نظر بگیرید که S یک ماتریس $|X| \times |Y|$ است و هر درایه آن به شکل زیر محاسبه می‌شود:

$$S_{x,y} = \mu(x,y)(-1)^{f(x,y)}.$$

و برای محاسبه معیار ناهمنگی:

$$disc_\mu(f,R) = \left| \sum_{(x,y)\in R} S_{x,y} \right| \qquad (۹\text{ـ}۴)$$

۴ـ۴ـ۲ محدودکردن مقیاس ناهمگنی و کمینه‌یابی

قضیه ۸. اگر برای یک تابع باینری f، توزیع μ وجود داشته باشد به صورتی که $disc_\mu(f) \leq 2^{-c}$ باشد، $R^{pub}_\epsilon = \Omega(c)$ خواهد بود.

با توجه به قضیه بالا، نیاز است که تکنیکی برای محدود کردن مقدار ناهمنگی بیابیم و از آن برای به‌دست آوردن کمینه‌هایی روی پیچیدگی تصادفی عمومی به‌دست آوریم. معروف ترین این تکنیک‌ها، تکنیک مقدار ویژه[2] است.

لم ۳. برای هر ماتریس متقارن M، ناهمگنی مستطیل $A \times B$ حداکثر برابر با $\lambda_{max}(M)\sqrt{|R|}$ است، که در آن λ_{max} بزرگ‌ترین مقدار ویژه تابع است. به بیان دیگر:

$$disc_\mu(f,R) \leq \lambda_{max}(M)\sqrt{|A||B|} \qquad (۱۰\text{ـ}۴)$$

و از این تکنیک می‌توان برای به‌دست آوردن مقدار ناهمگنی برای بعضی از مسائل که ماتریس متقارن دارند استفاده کرد.

---
[1] Discrepancy
[2] eigenvalue

فصل پنجم

کاربرد پیچیدگی ارتباطی در پردازش موازی

در این بخش به بررسی محل تقاطع دو علم پردازش موازی و پیچیدگی ارتباطی می‌پردازیم. برای آن که متوجه باشیم چرا پژوهشگران فعال در حوزه پردازش موازی به پیچیدگی ارتباطی اهمیت می‌دهند، لازم است مقداری در مورد پردازش موازی اطلاعات کسب کنیم. در دنیای پردازش موازی، محاسبات داخلی رایگان و محاسبات بین افراد گران است. سه پیچیدگی اصلی در دنیای پردازش موازی شامل تعداد پیغام‌های رد و بدل شده (پیچیدگی پیامی [1])، تعداد بیت‌های ردوبدل شده (پیچیدگی بیتی [2]) و تعداد دورهای مخابره برای یک مساله و تعدادی کاربر در یک محیط همگام (پیچیدگی دوری[3]) می‌باشد. نکته قابل توجه برای این دو دانش از جایی برمی‌آید که پیچیدگی ارتباطی از دل پردازش موازی استخراج شده‌است و همچنین در بسیاری از مسائل با هم دیگر برابر هستند. لازم است در ادامه انواع مدل‌های پیچیدگی ارتباطی kـ نفره را بررسی کنیم.

[1] Message Complexity
[2] Bit Complexity
[3] Round Complexity

۵ـ۱ مدلهای پیچیدگی ارتباطی kنفره

۵ـ۱ـ۱ مدل تخته‌سیاه

در این مدل، بازیکنان با یکدیگر از طریق یک تخته سیاه ارتباط برقرار می‌کنند. هر بازیکن در نوبت خودش حق نوشتن روی تخته سیاه را دارد و پروتکل تصمیم می‌گیرد که نوبت چه کسی است. همه بازیکنان می‌توانند تخته را مشاهده کنند. در این مدل و در هنگام شبیه‌سازی، هر بیتی که نوشته می‌شود به $k-1$ بازیکن دیگر مخابره می‌شود.

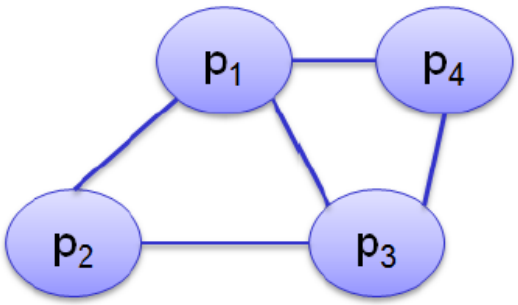
۵ـ۱ـ۲ مدل نفر_به_نفر

یک گراف ارتباطی[1] مشخص می‌کند که هر بازیکن به چه کسی متصل است و بدون واسطه می‌تواند پیام مخابره کند. برای راحتی کار، گراف‌های ارتباطی را گراف‌های کامل در نظر می‌گیرند که در آن هر دو بازیکن با هم ارتباط دارند.

همگام: در این مدل، مخابرات در دورهای مجزا انجام می‌شود. در هر دور، هر بازیکن یک پیغام می‌فرستد و پیغام‌های ورودی را دریافت می‌کند.

ناهمگام: در این مدل، هیچ دور مخابره‌ای وجود ندارد و هر پیغام در مواقع نیاز فرستاده می‌شود. در این مدل هر بازیکن یک صف دارد که پیغام‌های ورودی در آن قرار می‌گیرد.

شکل ۵ـ۱: مثالی از یک مدل نفر_به_نفر ۴تایی



۵ـ۱ـ۳ مدل هماهنگ‌کننده

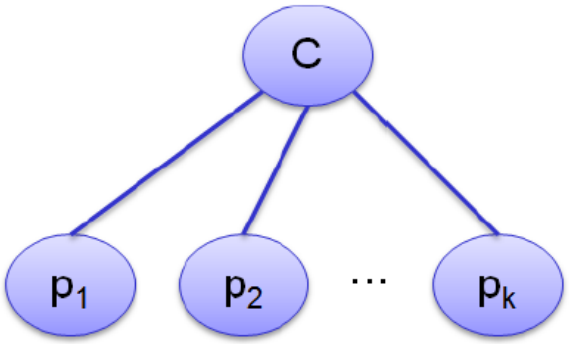
در این مدل، که یک حالت خاص از مدل نفر_به_نفر است، تمامی k بازیکن به یک نفر و فقط یک نفر دیگر متصل هستند (در مجموع $k+1$ بازیکن) و بازیکنان از طریق این یک هماهنگ‌کننده با هم در ارتباط هستند.

[1] Communication Graph

همگام: در هر دور، هر بازیکن یک پیغام به هماهنگ‌کننده می‌فرستد و هماهنگ‌کننده به آنها پاسخ می‌دهد.

ناهمگام: ارتباط دو نفره بین هرکس از طریق هماهنگ‌کننده و در هر زمان انجام می‌شود.

شکل ۵ـ۲: مثالی از یک مدل هماهنگ‌کننده kـتایی



۵ـ۲ قرینه‌سازی

قرینه‌سازی[1] یک تکنیک برای یافتن کمینه در بازی‌های kـنفره است. [۱۳] به طور خلاصه، این روش شامل کاهش پروتکل $f_k(x_1, x_2, ..., x_k)$ به پروتکل $f_2(x, y)$ است. هدف از این تکنیک این است که نشان دهیم محاسبه f_k حداکثر به اندازه k برابر f_2 است. در این مدل، توجه ما روی یک مدل هماهنگ‌کننده با وضعیت تصادفی سکه عمومی[2] است.

۵ـ۲ـ۱ تکنیک

با توجه به یک پروتکل P_k که تابع f_k را محاسبه می‌کند، یک پروتکل P_2 که تابع f_2 را محاسبه می‌کند می‌سازیم. در مرحله اول باید یک توزیع سخت[3] از ورودی‌های f_2 داشته باشیم. آلیس و باب، با استفاده از این توزیع، k ورودی $I_1, I_2, ..., I_k$ را بسازد. به هر k ورودی که از آن توزیع سخت استخراج شده است، قرینه گفته می‌شود اگر هر دوتای آنها را بتوان با هم جابه جا کرد بدون آن که توزیع را عوض کنیم. در این مرحله، آلیس و باب با استفاده از این k ورودی، پروتکل P_k را محاسبه می‌کنند.

شبیه‌سازی. آلیس یکی از بازیکنان را به صورت رندوم انتخاب می‌کند. چون وضعیت تصادفی عمومی است، باب می‌داند که آلیس کدام بازیکن را انتخاب کرده‌است پس او بقیه بازیکنان را برمی‌دارد و سپس هر دو رفتار بازیکنان را شبیه‌سازی می‌کنند. فرض کنید که آلیس بازیکن P_i را انتخاب کرده‌است. در در نتیجه هر پیغامی

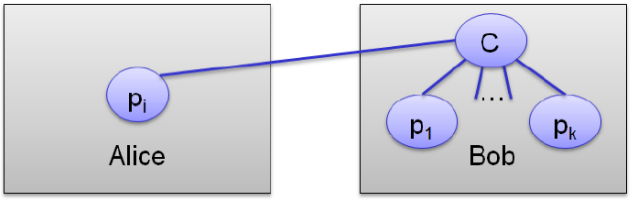
[1] Symmetrization
[2] Public Coin Randomization
[3] Hard Distribution

که بین بازیکن iم و بقیه بازیکنان رد و بدل می‌شود، بین آلیس و باب هم رد و بدل می‌شود. بقیه پیغام‌ها در این مدل به عنوان پیچیدگی ارتباطی حساب نمی‌شوند.

کمینه. هزینه پروتکل P_2 را $Cost(P_2)$ و هزینه پروتکل P_k را $Cost(P_k)$ بنامید. از آنجایی که ورودی‌ها قرینه هستند، از نظر امید ریاضی، P_2 حداکثر $1/k$ کل بیت‌هایی را مخابره می‌کند که P_k می‌کرده است. این بدین علت است که به صورت یکنواخت، امکان انتخاب هر بازیکن دیگر برای آلیس وجود داشت، در نتیجه امید ریاضی یالی که آلیس در مدل گرافی معادل انتخاب کرده‌است، $1/k$ کل یال‌ها اطلاعات رد و بدل می‌کرده است. در نتیجه

$$E[Cost(P_2)] \leq (1/k)E[Cost(P_k)] \qquad (۱-۵)$$

شکل ۵-۳: شبیه‌سازی مدل k-تایی



۵-۲-۲ پیشنیازها

همانطور که در قسمت ۴-۳ بیان شد، پیچیدگی ارتباطی توزیعی [1] D^{μ}_{ϵ} با خطای ϵ و توزیع ورودی μ به صورت زیر تعریف می‌شود:

$$D^{\mu}_{\epsilon} = \min_{P} \max_{x} Cost(P(x))\mu(x) \qquad (۲-۵)$$

در حالی که $Cost(P(x))$ هزینه پروتکل P بر روی ورودی x است. به عبارتی دیگر، D^{μ}_{ϵ} بدترین حالت مخابره برای یک ورودی (بدترین ورودی) برای بهترین پروتکل است.

از آنجایی که مخابره k-نفره k برابر امید مخابره ۲ نفره است، مفهومی از امید باید در پیچیدگی ارتباطی تعریف شود. امید پیچیدگی ارتباطی توزیعی $E[D^{\mu}_{\epsilon}]$ با خطای ϵ و توزیع μ به صورت زیر است

$$E[D^{\mu}_{\epsilon}] = \min_{P} E_x[Cost(P(x))\mu(x)]. \qquad (۳-۵)$$

[1] Distributional communication complexity

در نتیجه این تعریف و قضیه مین‌ومکس یائو[1] می‌توان گفت:

$$R_\epsilon \geq D^\mu_\epsilon \geq E[D^\mu_\epsilon] \qquad (۴\text{ـ}۵)$$

حال با اتکا به قضیه نظریه اطلاعاتی زیر، تعدادی مثال مطرح می‌کنیم. [۱۳]

قضیه: فرض کنید آلیس و باب هر کدام یک ورودی یکنواخت n بیتی دارند. برای آن‌که آلیس با احتمال $(1-\epsilon)$ ورودی باب را بداند، لازم است امیداً باب $(1-\epsilon)n$ بیت بفرستد.

۵ـ۳ مثال

۵ـ۳ـ۱ $k-XOR$: هماهنگ‌کننده

مساله $k-XOR$ در مدل هماهنگ‌کننده به صورت زیر است:

۱. بازیکن‌ها $p_1, p_2, p_3, ..., p_k$ هستند.

۲. ورودی‌ها رشته‌های n بیتی به صورت $I_1, I_2, I_3, ..., I_k$ هستند.

۳. خروجی یک رشته n بیتی است که بیت iم، XOR بیت iم ورودی‌هاست.

هدف استفاده از پروتکل P_k برای طراحی پروتکل P_2 است. بعد از آن، از کمینه پروتکل $2-XOR$ استفاده می‌کنیم تا یک کمینه روی مخابره kـنفره بیابیم.

ساخت ورودی‌های قرینه برای P_k: اول از همه باید یک توزیع سخت برای ورودی مخابره دونفره پیدا کنیم که به اندازه کافی برای یافت کمینه این مخابره سخت باشد. برای این کار توزیع یکنواخت به اندازه کافی سخت است. در نتیجه، آلیس به صورت یکنواخت تصادفی بازیکن p_i را انتخاب می‌کند و I_i را برابر با ورودی خودش یعنی x قرار می‌دهد. باب نیز به صورت تصادفی $k-1$ رشته n بیتی را به صورتی می‌سازد که

$$\{I_j \,|\, j \neq i\} \quad s.t.\ XOR(I_1, I_2, ..., I_{i-1}, I_{i+1}, ..., I_k) = y \qquad (۵\text{ـ}۵)$$

که در آن y ورودی باب است. ورودی‌ها به وضوح قرینه هستند. آلیس بازیکن iم و باب همه $k-1$ بازیکن دیگر و همینطور هماهنگ‌کننده را شبیه‌سازی می‌کند.

کمینه: از آنجایی که ورودی‌ها قرینه هستند، امید مقدار مخابره بین p_i و هماهنگ‌کننده $1/k$ برابر کل مخابره پروتکل P_k است. در نتیجه، $Cost(P_2) \leq (1/k)E[Cost(P_k)]$ است و یا $Cost(P_k) \geq kE[Cost(P_{2)}]$. حال لازم است یک کمینه برای $kE[Cost(P_{2)}]$ بیابیم.

[1] Yao's Minmax Theorem

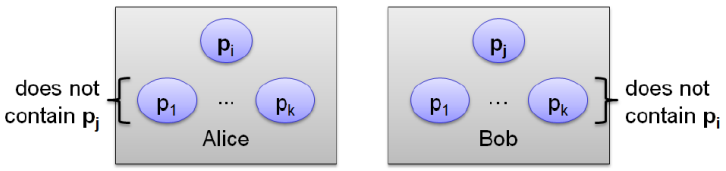
با داشتن $XOR(x,y)$، آلیس می‌تواند ورودی باب یعنی y را بازیابی کند. طبق قضیه نظریه اطلاعاتی، باب باید امیداً n بیت بفرستد که یعنی $kE[Cost(P_2)] \geq n$ و در نتیجه، $Cost(P_k) \geq nk$.

۵ـ۳ـ۲ تخته‌سیاه: $k-XOR$

مساله مثال قبل را در نظر بگیرید. مدل ارتباطی را به مدل تخته‌سیاه عوض کنید. ساخت ورودی‌ها و شبیه‌سازی با تغییر مدل نیز تغییر می‌یابند.

آماده‌سازی شبیه‌سازی: آلیس و باب هرکدام به صورت یکنواخت تصادفی بازیکن p_i و p_j را انتخاب می‌کنند $(i \neq j)$. آلیس همه بازیکن‌ها به جز بازیکن j را شبیه‌سازی می‌کند. همینطور باب، همه بازیکن‌ها به جز بازیکن i را شبیه‌سازی می‌کند. در نتیجه، هر بازیکنی به جز i و j توسط هر دو طرف شبیه‌سازی می‌شود.

شکل ۵ـ۴: شبیه‌سازی دوتایی آلیس و باب برای پروتکل kتایی $k-XOR$ در مدل تخته‌سیاه



ساخت ورودی قرینه مانند حالت قبل، توزیع یکنواخت یک توزیع سخت محسوب می‌شود. آلیس مقدار I_i را برابر با x قرار می‌دهد. باب نیز مقدار I_j را برابر با y قرار می‌دهد. بقیه ورودی‌ها به صورت تصادفی با استفاده از سکه عمومی مشترک مقداردهی می‌شوند. مشخص است که ورودی‌های ساخته شده قرینه هستند.

اجرای شبیه‌سازی: هربار بازیکن iم بیتی را روی تخته می‌نویسد، بقیه افراد باید مقدار نوشته شده را بتوانند بخوانند. اما از آنجایی که باب p_i را شبیه سازی نمی‌کند، تا زمانی که آلیس همان‌چیزی که p_i می‌نویسد را روی تخته‌سیاه ننویسید، یک بازیکن مانند p_j از مخابرات p_i آگاه نمی‌شود. پس هرگاه در پروتکل P_k، p_i اطلاعاتی را مخابره کند، آلیس نیز باید آن را مخابره کند. این مساله برای باب و بازیکن p_j نیز صادق است. ولی مخابرات بقیه بازیکنان نیازی به نوشته شدن روی تخته‌سیاه ندارد چرا که هر دو طرف آن‌ها را شبیه‌سازی می‌کنند.

پیچیدگی ارتباطی: از آنجایی که ورودی‌ها قرینه هستند و آلیس و باب تنها زمانی مخابره می‌کنند که دوتا از بازیکنان مخابره می‌کنند، امید مقدار مخابره برای P_2 حداکثر $\frac{k}{2}$ برابر مخابره برای P_k است. در نتیجه، $E[Cost(P_2)] \leq (2)Cost(P_k)$ است که برابر است با $Cost(P_k) \geq (k/2)E[Cost(P_2)]$. طبق قضیه نظریه اطلاعات، $E[Cost(P_2)] = n$. در نهایت، $Cost(P_k) \geq \frac{nk}{2}$.

۵ـ۳ـ۳ $k-DISJ$ بدون قرینه‌سازی

مساله اشتراک[1] به صورت گسترده در مخابرات دوتایی استفاده شده‌است و بسیاری از مسائل به این مساله کاهش یافته‌اند. این درحالی است که نسخه kـتایی این مساله، یعنی مساله‌ای که k بازیکن خروجی ۱ می‌دهند اگر و تنها اگر همه بازیکنان در یک عضو اشتراک داشته باشند، این خاصیت را ندارد. برای این که این مساله را نشان دهیم، یک پروتکل با پیچیدگی $O(nk)$ طراحی می‌کنیم. درنهایت مساله‌ای را معرفی می‌کنیم که کمینه بیشتری دارد. [۴]

در مرحله اول، همه بازیکنان درخت پوشای کمینه گراف ارتباطی را به صورت محلی محاسبه می‌کنند. یک بازیکن دلخواه مانند p_{root} را به عنوان ریشه درخت در نظر بگیرید. هر بازیکنی که برگ است، ورودی خود را به پدر خود می‌فرستد. پدر، اشتراک مجموعه خود و فرزندانش را محاسبه می‌کند و برای پدر خود می‌فرستد. این درخت پوشای کمینه دقیقا $k-1$ یال دارد که هر کدام n بیت داده جابه‌جا می‌کنند. در پایان پروتکل، p_{root} اشتراک همه را می‌داند و می‌تواند خروجی را به همه اطلاع دهد. پیچیدگی ارتباطی این پروتکل، $(k-1)(n+1)$ است.

حال مساله‌ای مانند $k-DIST$، که در آن بازیکنان خروجی 1 می‌دهند اگر و تنها اگر هردوتایی از ورودی‌ها متمایز باشد، در نظر بگیرید. می‌توان نشان داد که پروتکل بهینه برای این مساله وقتی است که همه بازیکنان ورودی‌شان را برای یک دیگر می‌فرستند. در یک گراف ارتباطی با قطر d، یعنی بلندترین کوتاه‌ترین مسیر، تعداد مخابره مورد نیاز برای آگاه شدن همه از ورودی یک‌دیگر برابر با $O(nkd)$ است. اگر گراف کامل باشد، d برابر با 1 است و بزگترین مقدار می‌تواند k باشد که کمینه $O(nk^2)$ را می‌دهد.

از دیگر مسائل سخت می‌توان به مسائلی اشاره کرد که در یک مخابره kتایی، هر بازیکن یک زیرگراف مانند H_k از یک گراف مانند G را داشته باشند و بخواهند تصمیم بگیرند که درجه یک راس مشخص در G چند است، آیا G دور دارد یا خیر، مثلث دارد یا خیر، متصل است یا خیر و آیا دوبخشی است یا خیر. [۴]

[1] Disjointness

فصل ششم

مکانیک کوانتومی

دراین فصل می‌خواهیم برای کسانی که آشنایی قبلی با مکانیک کوانتومی ندارند، اصول و ساختمان این نظریه را توضیح دهیم. مطالب این بخش از [۵، ۸، ۱۲] اقتباس شده است.

۶ـ۱ مقدمه‌ای در مورد مشاهده و اندازه‌گیری

نخستین کاری که برای شناختن یک شی انجام می‌دهیم آن است که سعی می‌کنیم خاصیت‌های معینی از آن را مثل رنگ، اندازه، جرم، سرعت یا تکانه و یا بار الکتریکی و نظایر آن را اندازه بگیریم. بعضی از این خصوصیات بطور مستقیم و بعضی از آن‌ها با واسطه‌های تجربی و نظری مشخص می‌شوند. به عنوان مثال برای اندازه‌گیری سرعت باریکه‌ای از ذرات باردار می‌توانیم آن‌ها را از دو میدان مغناطیسی و الکتریکی عمود بر هم بگذرانیم. دراین دستگاه اندازه‌گیری اندازه میدان الکتریکی و مغناطیسی را چنان تغییر می‌دهیم که مسیر باریکه ذرات هیچ انحرافی حاصل نکند. دراین صورت بااستفاده از قوانین الکترومغناطیس و با اعتماد به این قوانین که در مجموعه وسیعی از پدیده‌ها مشاهدات متقابل به صحت آنها مطمئن شده‌ایم، سرعت ذرات را به صورت رابطه $v = \frac{E}{B}$ استنتاج می‌کنیم. طبیعی است که دراینجا اندازه‌گیری سرعت کاملا به صورت غیرمستقیم و با اتکا بر یک چارچوب نظری بدست آمده‌است. درهمین آزمایش می‌توانیم سرعت ذرات دیگری که انحراف‌های دیگری

پیدا می‌کنند نیز پیدا کنیم. بنابراین، این دستگاه یک نوع اندازه‌گیری است که ذرات را برحسب سرعت آن‌ها از یک‌دیگر «جدا» می‌کند.

از مثال بالا دو نتیجه می‌توان گرفت. اول آنکه هر نوع اندازه‌گیری درواقع یک فرآیند است که طی آن یک دستگاه ماکروسکوپی ذرات را برحسب یک خاصیت معین از یک‌دیگر جدا می‌کند. ثانیاً هر نوع اندازه‌گیری و تفسیر نتایج آن متکی بر یک نظریه است که بدون آن نظریه نمی‌توان به نتایج آن اندازه‌گیری معنا و مفهومی نسبت داد.

در دنیای ماکروسکوپی بعضی از خواص اشیاء هرنوع مقداری می‌توانند اتخاذ کنند؛ مثل جرم اندازه و تکانه و نظایرآن. بعضی از خواص دیگر تنها مقادیر گسسته‌ای را به خود می‌گیرند مثل تعداد یا امتداد قطبش نور. بنابراین گسسته بودن یا پیوسته بودن به خودی خود یک خاصیت منحصر بفرد میکروسکوپی نیست. آنچه که ویژگی منحصر به فرد دنیای میکروسکوپی است چیست؟

۶ـ۲ معنای حالت

برای تعیین کامل حالت ذرات می‌بایست تمام خاصیت‌های سازگار باهم آنهارا تعیین کرد ولی برای سادگی روابط بعدی، فرض می‌کنیم که ذرات فقط با یک خاصیت معین می‌شوند. بنابراین می‌توانیم تصور کنیم که ذرات در یکی از حالت‌های $\{|a_1\rangle, |a_2\rangle, ..., |a_N\rangle\}$ (اگر بلافاصله از دستگاه اندازه‌گیری A بیرون آمده‌اند) قرار دارند و یا دریکی از حالت‌های $\{|b_1\rangle, |b_2\rangle, ..., |b_N\rangle\}$ قرار دارند (اگربلافاصله از دستگاه اندازه‌گیری B بیرون آمده‌اند) و نظایر آن. آزمایش‌گر می‌تواند ذرات را که در حالت $|\Psi\rangle$ قرار دارند را از دستگاه اندازه‌گیری A عبور دهد. دراین‌جا، اولین وجه افتراق دنیای کوانتومی خود را آشکار می‌سازد و آن این است که با وجودی که تمامی شرایط آزمایش یکسان است و تمام دقت‌های لازم اعمال شده است، نتیجه این اندازه‌گیری هربار یک چیز است. یعنی ذره درحالت $|\Psi\rangle$ به طور تصادفی خود را درحالت‌های $|a_1\rangle$ تا $|a_N\rangle$ نشان خواهد داد.

مرحله دوم آن است که می‌توان جداولی از همه احتمالات گذار برای خصوصیات مختلف تعین کرد . ازاین به بعد احتمال گذار حالت $|a\rangle$ به $|b\rangle$ را به صورت زیر نشان می‌دهیم:

$$P(b,a) \qquad (۱ـ۶)$$

خواص زیر برای این تابع احتمال برقرار است:

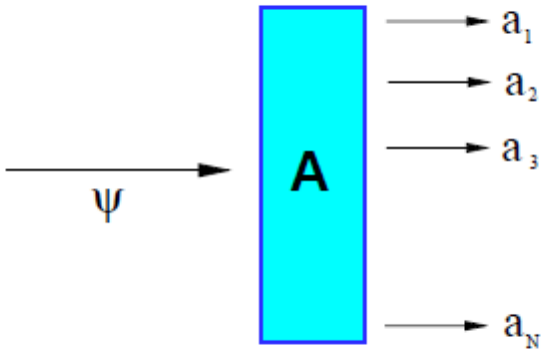
۱. $\sum_{j=1}^{N} P(b_j,a) = 1$

۲. $P(a_i,b_j) = P(b_j,a_i)$

۳. $P(a_i, a_j) = \delta_{ij}$

این رابطه به این معناست که ذره ای که در یک آزمایش A درحالت a_i جدا شده‌است، اگر دوباره تحت همان آزمایش قرار گیرد (البته بدون اینکه زمان برآن اثر بگذرد) باز هم همان خصلت a_i را از خود نشان خواهد داد.

شکل ۶ـ۱: دستگاه اندازه‌گیری A ذرات را به حالت‌های مختلف $|a_1\rangle$ تا $|a_N\rangle$ تجزیه می‌کند. حالت $|\Psi\rangle$ یک حالت ناشناخته است.



۶ـ۳ تداخل

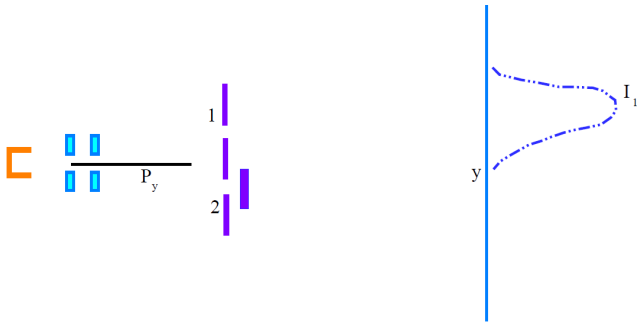
حال به مهم‌ترین خصلت دنیای میکروسکوپی می‌رسیم. در شکل درسمت چپ یک فیلامان حرارتی وجود دارد که بخاری از ذرات بار یونیزه را از خود متصاعد می‌کند. میدان‌های الکتریکی به همراه مجموعه‌ای از یکسوکننده ها ذرات در حالت $|P_y\rangle$ را جدا می‌کنند. شکاف پایینی مسدود شده است. هر ذره که از شکاف بالایی بگذرد درحالت $|1\rangle$ قرار می‌گیرد و سپس روی پرده در حالت $|y\rangle$ که نقطه نشستن آن روی پرده را (توسط یک آشکارساز) نشان می‌دهد، ثبت می‌شود. هرگاه این آزمایش را برای مدت طولانی انجام دهیم، در اثر نشستن ذرات روی یک پرده ـ مثلا یک پرده فلورسانس ـ طرح I_1 بوجود خواهد آمد. $I_1(y)$ درواقع متناسب با تعداد ذرات نشسته شده روی نقطه y است. درحقیقت داریم

$$I_1(y) = P(y,1)P(1,P_y) \qquad (۶ـ۲)$$

حال آزمایش را در حالتی که تنها شکاف پایینی باز باشد تکرار می‌کنیم. به همان معنا رابطه پیشین داریم:

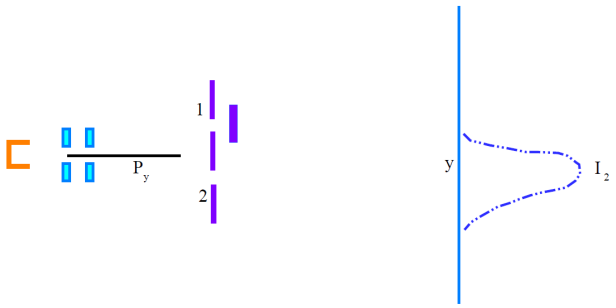
$$I_2 = P(y,2)P(2,P_y) \qquad (۶ـ۳)$$

شکل ۶ـ۲: آزمایش دو شکاف: تنها شکاف بالایی باز است و طرح I_1 روی پرده مشاهده می‌شود.



سپس آزمایش را در حالتی تکرار می‌کنیم که هر دو شکاف باز هستند. انتظار داریم این بار رابطه زیر برقرار

شکل ۶ـ۳: آزمایش دو شکاف: تنها شکاف پایینی باز است و طرح I_2 روی پرده مشاهده می‌شود.



باشد:

$$I_{1+2} = P(y,1)P(1,P_y) + P(y,2)P(2,P_y) = I_1 + I_2 \qquad (۴ـ۶)$$

و شکل ۶ـ۴ مشاهده شود.

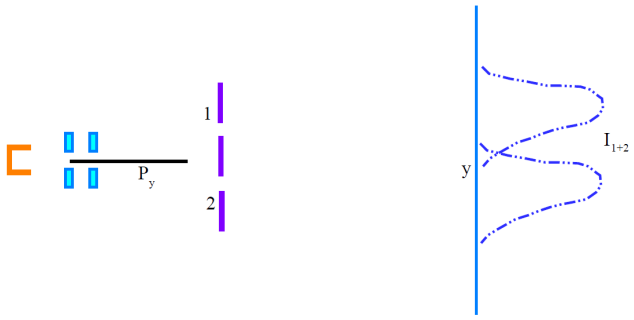
اما آنچه که در آزمایش می بینیم آن است که ذرات مطابق با طرح I_{12} که یک طرح تداخلی است روی پرده می‌نشینند. (شکل ۶ـ۵)

دراین طرح چندین نکته جالب و شگفت انگیز وجود دارد:

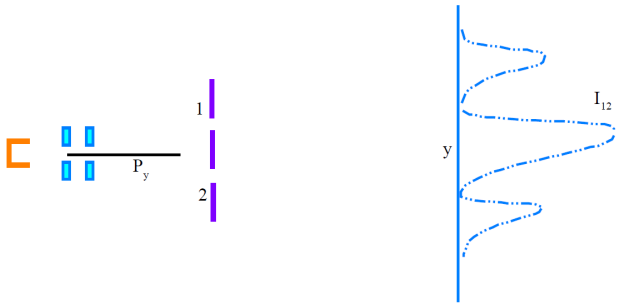
الف : در جاهایی از پرده، بازکردن هر دو شکاف با هم، باعث شده است که تعداد حتی کم‌تری ذرات نسبت به وقتی که تنها یک شکاف بازبود به آن نقطه برسد. در جاهایی نیز مثل وسط پرده تعداد ذرات دو برابر آن مجموع تعداد ذراتی است که درصورت باز بودن هرکدام از شکاف‌ها به تنهایی به پرده می‌رسید.

ب : برعکس درجاهای دیگری از ذرات باز کردن هر دو شکاف باعث شده است که تعداد ذراتی که به آن

شکل ۶ـ۴: آزمایش دو شکاف: هر دو شکاف باز هستند و طرح I_{1+2} روی پرده مورد انتظار است.



شکل ۶ـ۵: آزمایش دو شکاف: هر دو شکاف باز هستند و طرح I_{1+2} روی پرده رخ می‌دهد.



نقطه می‌رسد، بیشتر از مجموع ذراتی شود که درصورتی که هر دو شکاف باز می‌بود به آن نقطه می‌رسید.

ج : شکل این طرح تداخلی با رقیق کردن چشمه ذرات بطوری که درهر آن فقط و فقط یکی از ذرات از شکاف ها عبور کند، تغییر نمی‌کند. بنابراین نمی‌توان گفت که ذرات هنگام باز بودن هر دو شکاف با یکدیگر طوری برهم‌کنش می‌کنند که اثرات بالا دیده شود.

د : هرکدام از ذرات را روی پرده نهایی به طور کامل توسط آشکارساز ثبت می‌کنیم و آشکارساز ما ماهیت ذره‌ای آن را به‌خوبی تایید می‌کند. بنابراین نمی‌توان گفت که ذره در این آزمایش مثل یک موجود پیوستار عمل کرده است و بخشی از آن از یک شکاف و بخشی دیگراز یک شکاف دیگر عبور کرده است.

ه: ممکن است که ذره در حین عبور از دو شکاف به صورت یک پیوستار (چیزی شبیه یک ابر) رفتار می‌کند و سپس در انتها موقع نشستن روی پرده تمامی این ابر دوباره به صورت یک ذره کوچک متمرکز می‌شود. برای پی بردن به راز رفتار ذره می توان درست پشت شکاف ها آشکارسازهایی گذاشت تا بفهمیم که ذره درست موقع عبور از شکاف‌ها چگونه رفتار می‌کند. متوجه می‌شویم که درآنجا هم ذره به صورت یک ابر رفتار نمی‌کند بلکه به تمامی (با تمام جرم و بار و دیگر خصوصیات خود) درآشکار ساز ثبت می‌شود. تلاش ما برای پی بردن به راز رفتار ذره باعث شده است که طرح تداخلی I_{12} از بین برود و جای خود را به طرح معمولی داده است.

و : منطق ساده به ما حکم می‌کند که هر ذره‌ای که روی پرده می‌نشیند یا از شکاف ۱ آمده است یا از شکاف ۲. تعداد ذراتی که روی پرده نشسته‌اند برابرند با تعداد ذراتی که از شکاف ۱ آمده اند + تعداد ذراتی که از شکاف ۲ آمده اند. اما تعداد ذراتی که از شکاف ۱ عبور کرده وروی پرده نشسته‌اند برابراست با I_1 و تعداد ذراتی که از شکاف ۲ عبور کرده وروی پرده نشسته اند برابر است با I_2. پس حتی بدون مشاهده نزدیکی شکاف‌ها می توانیم حکم کنیم که طرحی که سرانجام روی پرده ثبت می‌شود، می‌بایست برابر با $I_1 + I_2$ باشد. درصورتی که اتم ها مثل توپ فوتبال عمل کرده باشند استدلال بالا صحیح است. درمقابل ایراداتی ازاین نوع که « بالاخره الکترون یا ازاین شکاف عبور می‌کند ویا از آن شکاف و دراین صورت نمی‌بایست طرح تداخلی داشته باشیم» تنها می‌توانیم به این بسنده کنیم که بگوییم وقتی سوال عبور الکترون از شکاف ها را به صورت عملی و تجربی بپرسیم می‌بنیم که طرح تداخلی واقعا از بین می‌رود و ما به تناقضی برنمی‌خوریم. بنابراین می‌گوییم که وقتی الکترون را مشاهده نمی‌کنیم، نمی‌توانیم مسیری برای آن تعریف کنیم.

نخستین کار ما آن است که ببینیم آیا نظمی در طرح تداخلی شکل وجود دارد یا نه. به نظر می‌رسد که طرح I_{12}، یک طرح ناشی از تداخل امواج باشد. بنابراین، برای پیداکردن نظمی که درجستجوی آن هستیم به تجربیات خود درمورد امواج بازمی‌گردیم . اگر I_1 را مربع یک عدد مختلط ϕ_1 موسوم به دامنه احتمال و I_2 را نیز مربع یک عدد مختلط ϕ_2 بگیریم چه بسا که I_{12} مربع $\phi_1 + \phi_2$ باشد، چنان که درمورد امواج چنین است:

$$I_1 := |\phi_1|^2 \quad I_2 := |\phi_2|^2 \quad I_{12} =: |\phi_{12}|^2 \qquad (۵-۶)$$

به طوری که

$$\phi_{12} = \phi_1 + \phi_2 \qquad (۶-۶)$$

و در معادله موج زیر، جملات سوم و چهارم که به جملات تداخلی موسوم هستند می‌توانند رفتار موجی ذرات را توجیه کنند:

$$I_{12} = I_1 + I_2 + \phi_1\phi_2^* + \phi_2\phi_1^* \qquad (۷-۶)$$

ولی باید توضیح دهیم این اعداد مختلط چه هستند. فرایند تغییر حالت در این وضعیت، نباید به حالاتی که یک الکترون در میانه را طی می‌کند توجهی کند، پس متغیر ϕ_{12} دامنه احتمالی است که یک حالت اولیه را به یک حالت نهایی می‌برد:

$$\phi_{12} = \langle y|P_y\rangle \qquad (۸-۶)$$

$$\phi_1 = \langle y|1\rangle \langle 1|P_y\rangle \qquad (۹\text{-}۶)$$

$$\phi_2 = \langle y|2\rangle \langle 2|P_y\rangle \qquad (۱۰\text{-}۶)$$

توجه کنید که از نمادگذاری فوق منظوری از ضرب داخلی نداریم. در نتیجه:

$$\langle y|P_y\rangle = \langle y|1\rangle \langle 1|P_y\rangle + \langle y|2\rangle \langle 2|P_y\rangle \qquad (۱۱\text{-}۶)$$

این رابطه، اصل رابطه‌ای است که ساختمان نظری مکانیک کوانتومی بر اساس آن بیان می‌شود.

$$\langle c_k|a_i\rangle = \sum_j \langle c_k|b_j\rangle \langle b_j|a_i\rangle \qquad (۱۲\text{-}۶)$$

پس برای شکل مشخص است که می‌توانیم با آزمایش‌های مکرر، مقدار احتمال‌های زیر را حساب کنیم و داخل یک بردار به شکل زیر نشان دهیم:

$$|\Psi\rangle_A = \begin{pmatrix} \langle a_1|\Psi\rangle \\ \langle a_2|\Psi\rangle \\ \vdots \\ \langle a_N|\Psi\rangle \end{pmatrix} \qquad (۱۳\text{-}۶)$$

شاخص A برای یادآوری آن است که اعداد داخل این بردار از اندازه‌گیری‌های A به دست آمده است.

با توجه به قانون برابری احتمال

$$P(a,b) = P(b,a) \longleftrightarrow \langle a|b\rangle = \langle b|a\rangle^* \qquad (۱۴\text{-}۶)$$

پس طبق رابطی کلی زیر

$$\langle b_j|\Psi\rangle = \sum_i \langle b_j|a_i\rangle \langle a_i|\Psi\rangle \qquad (۱۵\text{-}۶)$$

می‌توان شاخص‌های اندازه‌گیری را حذف کرد و اطمینان دهیم که حالت ذره توسط بردار Ψ توصیف شده است. با توجه به این که مقادیر بردار اندازه‌گیری احتمال هستند، ضرب‌کردن همه مقادیر در یک فاز، احتمالات را در یک شاخص اندازه‌گیری عوض نخواهد کرد.

۶ـ۴ معادله شرودینگر

$$i\hbar\frac{\partial\psi}{\partial t} = H\psi \qquad (۱۶ـ۶)$$

معادله شرودینگر[1] نقش قوانین نیوتن در فیزیک کوانتوم را دارد. برای فهمیدن این معادله با فرمول بندی همیلتونی مکانیک کلاسیک[2] شروع می‌کنیم.

۶ـ۴ـ۱ مکانیک همیلتونی

ذره‌ای با جرم m را در نظر بگیرید که در یک فضای یک بعدی در حرکت است. مکان این ذره را با q و تکانه[3] آن را با p نمایش می‌دهیم و فرض می‌کنیم که ذره در پتانسیل $V = V(q,t)$ قرار دارد. در این صورت انرژی کل ذره برابر است با

$$H = T + V \qquad (۱۷ـ۶)$$

که $T = \frac{p^2}{2m}$ انرژی جنبشی آن است. دو معادله زیر را در نظر بگیرید.

$$\begin{cases} \dot{q} = \frac{\partial H}{\partial p} \\ \dot{p} = -\frac{\partial H}{\partial q} \end{cases} \qquad (۱۸ـ۶)$$

از آنجا که V مستقل از p است، داریم

$$\frac{\partial H}{\partial p} = \frac{\partial T}{\partial p} = \frac{p}{m} \qquad (۱۹ـ۶)$$

و لذا معادله اول چیزی جز تعریف تکانه $p = m\dot{q}$ نیست. به طور مشابه از آنجا که T مستقل از q است از معادله دوم به دست می‌آوریم

$$\dot{p} = -\frac{\partial V}{\partial q}. \qquad (۲۰ـ۶)$$

در نتیجه از ترکیب این دو داریم

$$m\ddot{q} = -\frac{\partial V}{\partial q} \qquad (۲۱ـ۶)$$

که همان قانون دوم نیوتن است. در واقع معادله شرودینگر، فرمول بندی معادلی با $F = ma$ است که به آن فرمول بندی همیلتونی گفته می‌شود و کل مکانیک کلاسیک را می‌توان براساس آن پایه ریزی کرد.

---
[1] Schrodinger Equation
[2] Hamiltonian Mechanics
[3] momentum

۶ـ۵ اصول مکانیک کوانتومی

۶ـ۵ـ۱ اصل اول ـ فضای حالات

به هر سیستم فیزیکی یک فضای هیلبرت متناظر است. حالت سیستم (در هر لحظه از زمان) با یک بردار ناصفر در فضای هیلبرت مشخص می‌شود. دو بردار که ضریبی از یکدیگر باشند یک حالت فیزیکی را بیان می‌کنند. بنابراین حالت سیستم را می‌توان با یک بردار به طول یک (بردار واحد) مشخص کرد.

فضای هیلبرت فضای برداری است که دارای ضرب داخلی باشد و نسبت به نرمی که ضرب داخلی آن القاء می‌کند، کامل باشد. توجه کنید که فضاهای ضرب داخلی با بعد متناهی همواره کامل هستند.

مثال ۵. کیوبیت یک سیستم کوانتومی است که فضای هیلبرت H متناضر با آن دوبعدی باشد. اگر پایه تعامد یکه $\{|0\rangle, |1\rangle\}$ را برای این فضا در نظر بگیریم، آنگاه داریم:

$$\forall |\Psi\rangle \in H, \quad |\Psi\rangle = a|0\rangle + b|1\rangle, \quad a, b \in \mathbb{C} \qquad (۲۲ـ۶)$$

$$\| |\Psi\rangle \| = 1 \Rightarrow |a|^2 + |b|^2 = 1 \qquad (۲۳ـ۶)$$

بردار یکه $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ مثالی از یک حالت است که یک کیوبیت می‌تواند داشته باشد. از آنجا که این بردار ضریبی از بردار یکه $-\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ است، این دو بردار یک حالت سیستم را نشان می‌دهند. تفاوت این دو بردار یکه ضریب کلی با نرم یک است و لذا به عنوان حالات کوانتومی، یکسان هستند. توجه کنید که این دو، با حالت $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ متفاوت هستند چون ضریبی از یکدیگر نیستند.

یک سیستم فیزیکی که بعد فضای هیلبرت متناظر آن d باشد، $dim(H) = d$ یک کیودیت[1] نامیده می‌شود. فضای برداری متناظر با یک کیودیت با پایه متعامد یکه زیر نمایش داده می‌شود:

$$\{|0\rangle, |1\rangle, ..., |d-1\rangle\} \qquad (۲۴ـ۶)$$

۶ـ۵ـ۲ اصل دوم ـ تحول زمانی

تحول زمانی یک سیستم بسته با یک عملگر یکانی که روی فضای هیلبرت عمل می‌کند، بیان می‌شود. یعنی اگر حالت سیستم در زمان t_0، $|\Psi\rangle$ باشد و در زمان t_1، $|\Psi'\rangle$ باشد، آنگاه $U\mathcal{H} \to \mathcal{H}$ یکانی وجود دارد که $U|\Psi\rangle = |\Psi'\rangle$. U تنها وابسته به زمان است.

[1] Qudit

این اصل در واقع فرمول بندی دیگری از اصل شرودینگر است. این معادله تحول زمانی یک سیستم کوانتومی را به صورت زیر بیان می‌کند:

$$i\hbar\frac{d}{dt}|\Psi(t)\rangle = H|\Psi(t)\rangle \qquad (۲۵\text{ـ}۶)$$

که در آن $H : \mathcal{H} \to \mathcal{H}$ یک عملگر هرمیتی است. اگر H مستقل از زمان باشد،حل معادله دیفرانسیل فوق به صورت زیر است:

$$|\Psi(t)\rangle = \exp\left\{-\frac{it}{\hbar}H\right\}|\Psi(0)\rangle \qquad (۲۶\text{ـ}۶)$$

حال اگر قرار دهیم

$$U = \exp\left\{-\frac{it}{\hbar}H\right\} \qquad (۲۷\text{ـ}۶)$$

آنگاه معادله زمان اولیه برقرار می‌شود. می‌توان نشان داد U یکانی است و این شرایط برای حالتی که H مستقل از زمان هم نیست برقرار است.

مثال ۶. تحول زمانی یک کیوبیت با ماتریس‌های یکانی 2×2 مانند ماتریس‌های یکانی و هرمیتی زیر که آن‌ها را ماتریس پاولی[1] می‌نامیم، بیان می‌شود:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (۲۸\text{ـ}۶)$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad (۲۹\text{ـ}۶)$$

این عملگرها به صورت زیر عمل می‌کنند:

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle \qquad (۳۰\text{ـ}۶)$$

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle \qquad (۳۱\text{ـ}۶)$$

یک مثال دیگر، عملگر یکانی هادامارد[2] است:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad (۳۲\text{ـ}۶)$$

[1] Pauli Matrices
[2] Hadamard Matrix

توجه کنید که H هرمیتی هم است و داریم $H^\dagger X H = Z$ که نتیجه می‌دهد ویژه‌مقادیر X و Z یکسان است. ویژه‌بردارهای Z به علت آن که در پایه استاندارد قطری است برابر با $\{|0\rangle , |1\rangle\}$ است و ویژه‌بردارهای X برابرند با

$$\{|+\rangle := \frac{1}{2}(|0\rangle + |1\rangle), |-\rangle := \frac{1}{2}(|0\rangle - |1\rangle) \qquad (۳۳\text{-}۶)$$

و خواهیم داشت $H|0\rangle = |+\rangle$ و $H|1\rangle = |-\rangle$.

۶-۵-۳ اصل سوم - اندازه‌گیری

اندازه گیری بر روی یک سیستم با فضای هیلبرت $\mathcal{H}$ با مجموعه‌ای به صورت

$$\{M_i : M_i : \mathcal{H} \to \mathcal{H}, i \in S\} \qquad (۳۴\text{-}۶)$$

مشخص می شود که :

$$\sum_{i \in S} M_i^\dagger M_i = I \qquad (۳۵\text{-}۶)$$

در این صورت به M_iها عملگرهای اندازه‌گیری می‌گویند. با انجام این اندازه‌گیری، اگر حالت سیستم $|\Psi\rangle \in \mathcal{H}$ باشد، حاصل اندازه‌گیری با احتمال $p(i) = \left\langle M_i^\dagger M_i \Psi \right\rangle$ برابر می‌شود. اگر هم حاصل اندازه گیری i باشد، حالت سیستم به

$$\left|\Psi'\right\rangle = \frac{M_i |\Psi\rangle}{\sqrt{p(i)}} \qquad (۳۶\text{-}۶)$$

تغییر[1] می‌کند.

مثال ۷. اندازه‌گیری یک کیوبیت، اگر $M_i = |v_i v_i\rangle\langle v_i v_i|$ باشد، آنگاه می‌توان نشان داد که $\{M_0, M_1, ..., M_{d-1}\}$ یک اندازه‌گیری است. پس اگر حالت سیستم به صورت $|\Psi\rangle = \sum_i a_i |v_i\rangle$ باشد، آنگاه

$$p(i) = \langle\Psi|M_i^\dagger M_i|\Psi\rangle = |a_i|^2 \qquad (۳۷\text{-}۶)$$

مثال ۸. اندازه‌گیری تصویری: عملگرهای تصویر را در نظر بگیرید. می‌توان نشان داد که $\{P_i : i \in S\}$ یک اندازه‌گیری است. به چنین اندازه‌گیری تصویری می‌گویند. توجه کنید که در اندازه‌گیری تصویری، برای هر $i \neq j$ می‌توان نشان داد $P_i P_j = 0$. در واقع اگر تصویر P_i را با W_i نشان دهیم، آنگاه $\mathcal{H} = \bigoplus_{i \in S} W_i$ افراز فضا به زیرفضاهای عمود بر هم است.

[1] collapse

مثال ۹. یک مشاهده‌پذیر[1] فیزیکی با یک عملگر هرمیتی روی فضای هیلبرت مشخص می‌شود:

$$A : \mathcal{H} \to \mathcal{H} \qquad (۳۸\text{ـ}۶)$$

مثلا، عملگر همیلتونی متناظر با مشاهده‌پذیر انرژی است. از آن‌جایی که A هرمیتی است، در پایه‌های متعامد یکه، قطری می‌شود. در واقع، اگر $\lambda_i \in \mathbb{R}$ ویژه‌مقادیر A باشند و W_iها زیرفضاهای تولید شده توسط ویژه‌بردارهای متناظر با λ_i باشند، و P_i را عملگر تصویر عمود بر روی این زیرفضا بگیریم، آنگاه

$$A = \sum_i \lambda_i P_i \qquad (۳۹\text{ـ}۶)$$

و از آنجا که بردارهای ویژه A کل $\mathcal{H}$ را می‌پوشانند، داریم $\sum_i P_i$. پس اندازه گیری $\{P_i\}$ را داریم.

اگر حالت $|\Psi\rangle$ را با $\{P_i\}$ اندازه‌گیری کنیم و حاصل اندازه‌گیری i باشد، آنگاه می‌گوییم مقدار مشاهده‌پذیر A برابر با λ_i است. در این صورت، امید ریاضی این مشاهده پذیر که با $\langle A\rangle$ نشان داده می‌شود برابر است با

$$\langle A\rangle = \sum_i \lambda_i p(i) = \sum_i \lambda_i \langle\Psi|P_i|\Psi\rangle = \langle\Psi|\sum_i \lambda_i P_i|\Psi\rangle = \langle\Psi|A|\Psi\rangle \qquad (۴۰\text{ـ}۶)$$

۶ـ۵ـ۴ اصل چهارم ـ سیستم های ترکیبی

فضای هیلبرت متناظر با یک سیستم فیزیکی که متشکل از n سیستم کوچک‌تر است از ضرب تانسوری فضاهای کوچک‌تر بدست می‌آید.

به عبارت دیگر، اگر فضای هیلبرت متناظر با سیستمiـم $\mathcal{H}_i$ باشد، فضای هیلبرت متناظر با کل n سیستم برابر است با

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_n. \qquad (۴۱\text{ـ}۶)$$

اگر سیستم iـم در حالت $|\Psi_i\rangle \in \mathcal{H}_i$ باشد، کل سیستم در حالت

$$\Psi_1 \otimes \Psi_2 \otimes ... \otimes \Psi_n. \qquad (۴۲\text{ـ}۶)$$

است.

۶ـ۶ درهم‌تنیدگی[2]

دو کیوبیت A و B را در نظر بگیرید. $\mathcal{H}_A$ و $\mathcal{H}_B$ فضای هیلبرت معادل هر کدام از این کیوبیت‌ها با پایه‌های $\{|0\rangle_A, |1\rangle_A\}$ و $\{|0\rangle_B, |1\rangle_B\}$ نمایش داده می‌شود. طبق اصل چهارم، فضای هیلبرت متناظر با سیستم ترکیبی

[1] Observable
[2] Entanglement

این دو کیوبیت برابر است با

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{B} \qquad (۴۳\text{ـ}۶)$$

که با پایه متعامد یکه

$$\{|0\rangle_A \otimes |0\rangle_B , |0\rangle_A \otimes |1\rangle_B , |1\rangle_A \otimes |0\rangle_B , |1\rangle_A \otimes |1\rangle_B\} \qquad (۴۴\text{ـ}۶)$$

مشخص می‌شود که برابر است با:

$$\{|00\rangle_{AB} , |01\rangle_{AB} , |10\rangle_{AB} , |11\rangle_{AB}\}. \qquad (۴۵\text{ـ}۶)$$

هر $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ به صورت ترکیب خطی از چهار عضو مجموعه بالاست. اگر $|\psi\rangle_{AB}$ را $= |v\rangle_A \otimes |w\rangle_B$ نمایش داد به این حالت، حالت ضربی[1] و یا حالت جداپذیر[2] گفته می‌شود. اگر چنین نمایشی برای $|\psi\rangle_{AB}$ وجود نداشته باشد، به آن حالت درهم‌تنیده[3] می‌گویند. مثال:

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = \frac{1}{\sqrt{2}} |0\rangle_A \otimes (|0\rangle_B + |1\rangle_B) \qquad (۴۶\text{ـ}۶)$$

یک حالت ضربی است و

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (۴۷\text{ـ}۶)$$

یک حالت درهم‌تنیده‌است.

۶ـ۷ اختتامیه‌ای بر عجایب مکانیک کوانتومی

کنترل اتم‌های منفرد و به همراه آن گسترش رایانش و اطلاعات کوانتومی منجر به پیدایش سوال‌های جدید در ساختمان نظری مکانیک کوانتومی شده‌است. تلاش برای پاسخ‌گویی به این سوال‌ها به نوبه خود منجر به غنی شدن نظریه مکانیک کوانتومی از جهات متعدد شده است. به عنوان مثال، چگونه می‌توان درهم‌تنیدگی دو حالت مثل

$$|\phi\rangle = \sqrt{0.9}|0,0\rangle + \sqrt{0.1}|1,1\rangle \qquad (۴۸\text{ـ}۶)$$

و

$$|\phi\rangle = \sqrt{0.8}|0,0\rangle + \sqrt{0.2}|1,1\rangle \qquad (۴۹\text{ـ}۶)$$

[1] Product State
[2] Seperable State
[3] Entangled State

را با هم مقایسه کرد؟ مثل هر ویژگی دیگری در فیزیک باید بتوانیم به صورت کمی مقدار درهم‌تنیدگی این دو حالت را با هم مقایسه کنیم.

چگونه می‌توان بیشتر از دو ذره را در هم تنیده کرد؟ اکنون می‌توانیم جفت فوتون هایی را که بیش از یکصد و پنجاه کیلومتر از یکدیگر دور هستند، درهم‌تنیده کنیم. سوال این است که چگونه می‌توانیم با انجام آزمایش در هرکدام از آزمایشگاه‌ها مقدار این درهم‌تنیدگی را کم و زیاد کنیم. چگونه می‌توانیم این کار را برای جفت فوتون‌هایی که بین زمین و ماهواره ها درهم تنیده هستند انجام دهیم؟ چگونه می توانیم اتم‌های ساکن دور از هم را درهم تنیده کنیم؟ آیا می‌توانیم شبکه‌ای از حالت های درهم تنیده بین نقاط مختلف و دور از هم درست کنیم و از آن برای مبادله اطلاعات کوانتومی و فرابرد کوانتومی استفاده کنیم؟

سوالات در مورد درهم تنیدگی نه تنها از نظر عملی مهم هستند بلکه از نظر ریاضی نیز اهمیت دارند. ما شناخت نسبتا کاملی از فضای هیلبرت دو کیوبیت داریم. مثلا می‌دانیم که حالتی مثل

$$|\phi\rangle = \sqrt{0.5}|0,0\rangle + \sqrt{0.5}|1,1\rangle \qquad (۵۰\text{-}۶)$$

بیشترین میزان درهم تنیدگی را دارد و تمام حالت های دیگر را با اعمال موضعی می توان از این حالت درست کرد. در واقع می توانیم با سنجش درهم‌تنیدگی تمام بردارهای فضای هیلبرت، دو ذره را مرتب کنیم. ولی به محض اینکه به فضای هیلبرت سه کیوبیت می رسیم با انواع سوال‌های جدید و بی پاسخ مواجه می‌شویم و این وضعیت ساده از بین می رود. هیچ ملاک مقایسه‌ای نداریم که بر مبنای آن بگوییم کدام یک از دو حالت

$$|GHZ\rangle = \sqrt{0.5}|0,0,0\rangle + \sqrt{0.5}|1,1,1\rangle \qquad (۵۱\text{-}۶)$$

یا

$$|W\rangle = \sqrt{1/3}(|1,0,0\rangle + |0,1,0\rangle + |0,0,1\rangle) \qquad (۵۲\text{-}۶)$$

در هم تنیدگی بیشتری دارند. این گونه مطالعات به ما کمک می‌کنند که ملاک‌های معینی برای دسته بندی حالت‌های فضای هیلبرت دو و چند ذره‌ای ابداع کنیم و بتوانیم فضای بسیار بزرگ هیلبرت را برای یک سیستم چند ذره‌ای بر اساس این خاصیت‌ها شناسایی کنیم. سوال‌ها و کشفیات جدید البته منحصر به در هم تنیدگی نیستند و حوزه‌های خیلی وسیعی را در بر می‌گیرند. در ادامه به یک نوع دیگر از این سوال‌ها می‌پردازیم.

۶ـ۸ قضایای عدم امکان در مکانیک کوانتومی

در سال‌های اخیر و بعد از توجه دوباره به مبانی مکانیک کوانتومی، معلوم شده است که بعضی اعمال را در دنیای میکروسکوپی هرگز نمی‌توان انجام داد. این قضایای عدم امکان[1] اهمیت نظری و عملی بسیار زیادی دارند. به عنوان مثال قضیه عدم تکثیر[2] که یک قضیه بسیار ساده ولی مهم و بنیادی در مکانیک کوانتومی است ، تنها در سال ۱۹۸۲ یعنی هشتاد سال بعد از پیدایش مکانیک کوانتومی کشف شد . در زیر، یکی از این قضایای عدم امکان را، که همگی به تازگی کشف شده‌اند، بیان می‌کنیم.

۶ـ۸ـ۱ تکثیر حالت‌های کوانتومی

نخست ساده ترین حالت رادر نظر می‌گیریم. حالتی که می‌خواهیم آن راتکثیر کنیم با $|\phi\rangle$ نشان می‌دهیم. حالتی را که می خواهیم یک نسخه از $|\phi\rangle$ روی آن نوشته شود را با $|b\rangle$ نشان می‌دهیم. این حالت حکم کاغذ سفید را دارد و به همین دلیل آن را حالت سفید یا حالت خالی می‌نامیم. حالت دستگاه را نیز با $|m\rangle$ نشان می دهیم. فرض کنید که یک عمل یکانی وجود دارد که برای هرحالت ورودی کار زیر را انجام می‌دهد:

$$U(|\phi\rangle \otimes |b\rangle \otimes |m\rangle) = |\phi\rangle \otimes |\phi\rangle \otimes |m_\phi\rangle) \qquad (۵۳ـ۶)$$

دراین صورت این دستگاه حالت یک نسخه از حالت ورودی را روی حالت سفید می‌نویسد و حالت خود دستگاه نیز بسته به حالت ورودی تغییر می‌کند. درخروجی دو نسخه از حالت $|\phi\rangle$ داریم. حال دو حالت متعامد $|0\rangle$ و $|1\rangle$ را در نظر می‌گیریم. حالت زیر را هم در نظر بگیرید:

$$|+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \qquad (۵۴ـ۶)$$

حال، سه حالت $|0\rangle$ و $|1\rangle$ و $|+\rangle$ را به داخل ماشین تکثیر می‌فرستیم. دقت کنید که این دوحالت لزوماً دو حالت از یک سیستم دوبعدی نیستند. دراین صورت خواهیم داشت:

$$U(|0\rangle \otimes |b\rangle \otimes |m\rangle) = |0\rangle \otimes |0\rangle \otimes |m_0\rangle \qquad (۵۵ـ۶)$$

و

$$U(|1\rangle \otimes |b\rangle \otimes |m\rangle) = |1\rangle \otimes |1\rangle \otimes |m_1\rangle \qquad (۵۶ـ۶)$$

و

$$U(|+\rangle \otimes |b\rangle \otimes |m\rangle) = |+\rangle \otimes |+\rangle \otimes |m_+\rangle \qquad (۵۷ـ۶)$$

[1] No go theorems
[2] No Cloning Theorem

اماهرگاه تساوی سوم را بسط دهیم و ازدو رابطه اول و خطی بودن مکانیک کوانتومی استفاده کنیم به رابطه زیر می‌رسیم:

$$|0\rangle|0\rangle|m_0\rangle + |1\rangle|1\rangle|m_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)|m_+\rangle \qquad (۵۸\text{ـ}۶)$$

هرگاه طرفین این رابطه را یک‌بار در $\langle 0|\langle 0|$ و یک‌بار در $\langle 1|\langle 1|$ ضرب کنیم، با استفاده از خاصیت متعامد بودن $\langle 0|$ و $\langle 1|$ به نتیجه زیر می‌رسیم:

$$|m_+\rangle = \sqrt{2}|m_0\rangle = \sqrt{2}m_1\rangle \qquad (۵۹\text{ـ}۶)$$

با جایگذاری این رابطه در رابطه قبلی و مقایسه دوطرف می‌رسیم به

$$|0\rangle|1\rangle + |1\rangle|0\rangle = 0 \qquad (۶۰\text{ـ}۶)$$

هرگاه طرفین این رابطه را در $\langle 1|\langle 0|$ ضرب کنیم به رابطه $0 = 1$ می‌رسیم که تناقض است.

فصل هفتم

محاسبات و الگوریتم‌های کوانتومی

مطالب این فصل با اقتباس از [۵، ۸، ۱۲] تهیه شده است.

۷ـ۰ـ۱ محدودیت‌های رایانش کلاسیک

در کنگره ریاضیدانان در سال ۱۹۰۰ دیوید هیلبرت ۲۳ مسئله مهم را بیان کرد که در واقع نقشه راهی بود برای ریاضیدانان در قرن بیستم. در این میان، مسئله دهم هیلبرت جایگاه ویژه ای دارد چرا که تلاش برای حل آن توسط آلن تورینگ ریاضیدان انگلیسی منجر به ابداع نظریه رایانش کلاسیک شد. نظریه‌ای که یک دهه قبل از ظهور اولین رایانه‌ها و ماشین‌های محاسبه پدید آمد و اهمیت آن در این است که خیلی پیش از ساخت اولین کامپیوترها نشان داد که کامپیوترها چه نوع مسائلی را هرگز نخواهند توانست حل کنند. معادلات چندجمله‌ای با ضرایب صحیح مثل $x^3 + y^4 + z^2 + w = 0$ معادلات دیوفانتی[1] خوانده می‌شوند و مسئله دهم هیلبرت طرح این سوال بود که آیا الگوریتمی برای یافتن پاسخ به این سوال‌ها وجود دارد یا خیر. برای پاسخ به این سوال بود که آلن تورینگ مفهوم ماشین تورینگ را به عنوان ماشینی انتزاعی برای محاسبه الگوریتمی ابداع کرد. به این ترتیب وی نه تنها مبانی نظری علم رایانش را بنا نهاد بلکه نشان داد که این ماشین می‌تواند هر نوع ماشین

[1] Diophantine

محاسبه دیگری را نیز شبیه‌سازی کند. به بیان دیگر، هر نوع مسئله‌ای که بر روی هر نوع ماشین محاسبه‌ای قابل حل باشد، توسط ماشین تورینگ نیز قابل حل است. ماحصل کار وی اثبات این بود که پاسخ سوال هیلبرت منفی است و مسئله معادلات دیوفانتی را نمی‌توان به صورت الگوریتمی حل کرد.

در طول بیش از ۸۰ سال که از ابداع نظریه محاسبه می‌گذرد، این اعتقاد عمومی تقویت شده‌است که هر ماشین محاسبه‌ای مستقل از این که از چه نوع سازوکاری فیزیکی پیروی کند، توسط ماشین تورینگ قابل شبیه‌سازی است. این نظریه یا تز که به نام تز چرچ ـ تورینگ شناخته می‌شود در واقع محدوده قوانین فیزیک را به نظریه محاسبه پیوند می‌دهد.

ماشین تورینگ البته یک مدل نظری محاسبه است . در عمل، مدل‌های گوناگونی می‌توانند محاسبه و رایانش را انجام دهند. رایج‌ترین مدل محاسبه مدل مداری است که در آن داده‌ها در رشته‌ای از بیت‌های کلاسیک 0 و 1 ذخیره می‌شوند و مدارهای منطقی کلاسیکی که از گیت‌های کلاسیک ساخته شده‌اند این داده‌ها را پردازش می‌کنند. این مدارهای منطقی می‌توانند توابع قابل محاسبه را با ترکیبی از گیت‌های منطقی AND و NOT و OR محاسبه کند. یک بیت کلاسیک می‌تواند تنها در یکی از دو حالت 0 و 1 قرار بگیرد. حال آنکه بیت کوانتومی یا کیوبیت[1] می تواند در ترکیبی از این دو حالت نیز قرار گیرد. یک حافظه کوانتومی شامل n کیوبیت می‌تواند در ترکیبی خطی از 2^n حالت مختلف قرار بگیرد. به عنوان مثال، فرض کنید که بتوانیم از اسپین یک هسته به عنوان یک کیوبیت استفاده کنیم و بتوانیم یک کامپیوتر کوانتومی بسازیم که تنها ۱۰۰۰ تا اسپین را به عنوان کیوبیت استفاده می‌کند. در این صورت یک حالت کلی از این ۱۰۰۰ اسپین حالتی است که در یک فضای بسیار بسیار بزرگ 2^{1000} قرار دارد. حالت این کامپیوتر در هر زمان ترکیبی خطی از این تعداد حالت محاسباتی است. این ویژگی که از آن به خاصیت توازی کوانتومی[2] یاد می‌شود کامپیوتر کوانتومی را قادر می‌کند که همزمان یک تابع را برای تعداد نمایی از متغیرها محاسبه کند. این قابلیت کامپیوترهای کوانتومی، آنها را قادر می‌کند که توانایی حل مسائلی را داشته باشند که حل آن‌ها برای کامپیوترهای کلاسیک زمان بسیار زیادی خواهد برد. مشهورترین این مسائل، مسئله تجزیه یک عدد به عامل‌های اول آن است. امروزه، می‌دانیم که با بهترین الگوریتم‌های کلاسیک، اگر بخواهیم اعداد ۵۰۰ رقمی را با قوی‌ترین کامپیوترهای موجود حل کنیم، به زمانی از مرتبه میلیون‌ها سال نیاز داریم. اما نشان داده شده که الگوریتم‌های کوانتومی که روی کامپیوترهای کوانتومی پیاده سازی می شوند، می توانند این مسئله را در زمان خیلی کوتاه‌تری حل کنند.

[1] Qubit
[2] Quantum Parallelism

۷ـ۱ مبادله کوانتومی اطلاعات

برهم‌نهی حالت‌ها اگرچه یکی از ویژگی‌های سیستم‌های کوانتومی است ولی ویژگی‌ای نیست که تنها مختص سیستم‌های کوانتومی باشد. مثلا نور و امواج الکترومغناطیسی نیز از این ویژگی برخوردارند. یک باریکه نور می‌تواند دارای قطبش خطی در راستای افقی یا عمودی و یا ترکیبی از هر دو راستا باشد. بنابراین باریکه نور کلاسیک از خود خاصیت برهم‌نهی نشان می‌دهد. اما آنچه که واقعا ویژگی منحصر بفرد و یکتای مکانیک کوانتومی است، خصلت ناموضعی[۱] آن است. این خصلت ارتباط نزدیکی با درهم تنیدگی[۲] دارد و نشان می‌دهد که اندازه‌گیری یک ذره در یک نقطه می‌تواند خصلت‌های بالقوه‌ای را که در یک ذره در دوردست وجود دارد، به طور آنی تغییر دهد و آن‌ها را به فعلیت درآورد، بدون این‌که هیچ‌گونه ارتباط علی با آن ذره داشته باشد. اندازه‌گیری شما از میان تمام حالت‌های احتمالی‌ای که یک ذره در کیلومترها آن طرف‌تر می‌توانست اختیار کند، یکی را به صورت قطعی انتخاب می‌کند، بدون اینکه نور و یا هیچ علامت دیگری فرصت کرده باشد که در بین این دو اندازه گیری این فاصله را طی کرده باشد. امروزه، با آزمایش‌های دقیق اپتیکی می‌توانیم فوتون هایی را تولید کنیم که در فاصله‌های بیش از ۱۵۰ کیلومتر از یکدیگر درهم‌تنیده باشند. بر خلاف چهره تناقض‌گونه این خاصیت، که گمان می‌رفت ناقض نسبیت خاص است، عمیق‌ترین و رازآلودترین ویژگی کوانتومی است. ویژگی‌ای که به کرات در ادامه این گزارش از آن استفاده خواهیم کرد. تا قبل از سال‌های آغازین دهه آخر قرن بیستم، فیزیکدانان توجه خود را معطوف به تلاش برای درک این خصلت کرده بودند.

تنها پس از شصت سال که توجه عموم فیزیکدانان معطوف به بررسی جنبه های معنایی درهم تنیدگی شده بود نخستین کاربردهای مهم و تکان دهنده درهم تنیدگی پدیدار شدند. نخست در سال ۱۹۹۱ معلوم شد که از حالت های درهم‌تنیده می توان برای توزیع کوانتومی کلید[۳] برای رمزنگاری[۴] استفاده کرد و سپس در ۱۹۹۵ معلوم شد که می‌توان حالت کوانتومی ذرات را با سرعت نور از یک نقطه به نقطه دیگر انتقال داد. اگر قبول کنیم که یک شئ چیزی نیست جز حالت کوانتومی آن، این پدیده که به آن فرابرد کوانتومی[۵] می‌گوییم، در واقع نخستین نمونه از جابجایی اشیا با سرعت نور خواهد بود. اینکه یک شی ماکروسکوپی را نیز بتوان با استفاده از این پدیده با سرعت نور جابجا کرد در حال حاضر به طور کامل دور از دسترس علم و فناوری است. اخیرا نشان داده شده است که با طراحی یک آزمایش دو شکاف می‌توان طرح‌های تداخلی را حتی برای مولکول‌هایی به بزرگی فولرین یا C^{60} مشاهده کرد. اما این برهم‌نهی و خصلت کوانتومی تا به کجا ادامه پیدا می‌کند؟ آیا یک پروتئین ، یا

[1] Non-locality
[2] Entanglement
[3] Quantum Key Distribution
[4] Quantum Cryptography
[5] Quantum Teleportation

سلول، یک گربه یا یک انسان نیز می تواند در یک برهم‌نهی از حالت‌هایش قرار بگیرد؟ در حال حاضر می‌دانیم که یک انسان می‌تواند در مکان A یا در مکان B قرار بگیرد، ولی در یک برهم‌نهی از این دو حالت نه. حتی اگر در چنین حالتی قرار داده شود برهم کنش‌هایی که با محیط خود دارد بلافاصله حالت او را به یکی از دو حالت تقلیل می دهد. این پدیده که به آن وادوسی[1] می‌گوییم، برای اشیای ماکروسکوپی با سرعت سرسام آوری رخ می‌دهد به نحوی که این اشیا هرگز در چنین حالت‌هایی دیده نمی‌شوند و حال آنکه اشیای میکروسکوپی مثل الکترون و اتم می‌توانند درچنین حالت‌هایی قرار بگیرند. به اصطلاح زمان وادوسی برای الکترون و اتم طولانی و برای موجودات ماکروسکوپی بسیار کوتاه است. البته این وضعیت امروزین است. این که آیا می‌توان در آینده یک شی ماکروسکوپی مثل یک گربه را آنقدر از محیط اطرافش جدا کرد و آنقدر تاثیرات محیطی را روی آن کاهش داد که زمان وادوسی‌اش طولانی شود، موضوعی است که هنوز چیزی درباره آن نمی‌دانیم. حتی ممکن است که این وادوسی تنها ناشی از برهم‌کنش با محیط نباشد بلکه ناشی از خصلت ماکروسکوپی خود شی و تعداد زیاد اتم‌های موجود در آن باشد که در این صورت انجام فرابرد کوانتومی برای این گونه اشیا به کلی منتفی خواهد بود. به هرحال این موضوع که دقیقا مرز دنیای ماکروسکوپی و میکروسکوپی یا به اصطلاح مرز بین دنیای کلاسیک و کوانتومی کجاست، سوالی است که پاسخ آن تا به امروز مشخص نیست. ممکن است که هیچ مرز مشخصی بین این دو دنیا وجود نداشته باشد که در این صورت با پیشرفت تکنولوژی ممکن است صدها سال بعد بتوان یک گربه را نیز در برهم‌نهی از دو حالت یا چند حالت‌اش نگاه داشت و ممکن است که یک ثابت بنیادی جدید در طبیعت کشف شود که مرز بین این دو دنیا را مشخص کند.

۲ـ۷ شبیه‌سازی کوانتومی

یک دستگاه ساده کلاسیکی مثل منظومه شمسی را در نظر بگیرید. این دستگاه دارای N ذره (اعم از خورشید، سیارات، قمرها و سیارک‌ها و ستارگان دنباله‌دار) است که همگی تحت نیروی گرانش حرکت می‌کنند. هر کدام از این ذرات با سه مختصه برای مکان و سه مختصه برای سرعت یا تکانه مشخص می‌شوند. هم چنین از انجا که سیارات را نمی‌توان به صورت نقاط بدون بعد در نظر گرفت می‌توان برای هر کدام سه مختصه که نشان‌دهنده وضعیت دورانی آن‌ها باشد نیز در نظر گرفت. بنابراین تعداد کل متغیرهایی که برای توصیف این سیستم به کار می‌رود برابر است با $9N$.

می‌توان مقدار هرکدام از این متغیرها را در یک آرایه از کامپیوتر ذخیره کرد و سپس مطابق با قوانین نیوتن مقدار هر کدام از این متغیرها را لحظه به لحظه پیدا کرد. به این ترتیب می‌توان رفتار این دستگاه کلاسیکی را

[1] Decoherence

در یک کامپیوتر شبیه‌سازی کرد و توسط این برنامه شبیه‌سازی می‌توان کسوف ها و خسوف‌ها و برخوردهای احتمالی و ده‌ها پدیده دیگر را در منظومه شمسی پیش بینی کرد. نکته مهم در اینجا این است که تعداد متغیرهایی که می‌بایست در حافظه کامپیوتر ذخیره کرد نسبت به تعداد اشیای موجود در منظومه شمسی به صورت خطی رشد می‌کند. هرگاه که تعداد ذرات را به عنوان مثال دو برابر کنیم کافی است که مقدار حافظه کامپیوتر را دو برابر کنیم. این خصلت بسیاری از سیستم های کلاسیک است که با افزایش تعداد ذرات ، تعداد متغیرهای توصیف کننده وضعیت این سیستم‌ها به صورت چندجمله‌ای رشد می‌کند. به همین ترتیب است که می‌توان نه تنها منظومه شمسی بلکه رفتار خوشه های ستاره‌ای، کهکشان‌ها و خوشه‌های کهکشانی و یا رفتار دستگاه‌های فناوری را در کامپیوترها شبیه سازی کرد.

حال به یک سیستم کوانتومی ساده توجه می‌کنیم. ماده بس‌ذره‌ای که از همه درجات آزادی اتم‌های آن صرف نظر کرده و فقط اسپین اتم‌های آن را در نظر گرفته‌ایم. اگر N تا اتم داشته باشیم و هر اتم یک ذره اسپین $1/2$ باشد، تعداد حالت‌های اسپینی این اتم‌ها برابر است با 2^N. بنابراین، هر حالت بردار سیستم یک بردار 2^N مولفه‌ای است و اگر بخواهیم دینامیک چنین سیستم ساده‌ای را با کامپیوترهای کلاسیک شبیه‌سازی کنیم، می‌بایست 2^N عدد را که نشان دهنده این بردار حالت در هر لحظه است در حافظه کامپیوتر ذخیره کنیم. بدلیل نمایی بودن این بعد احتیاج به یک حافظه خیلی خیلی بزرگ داریم. کافی است که برای سادگی یک سیستم ۱۰۰۰ اتمی را تصور کنید. حالت کوانتومی چنین سیستمی، یک بردار با $2^{1000} = 10^{300}$ مولفه است . واضح است که ذخیره کردن چنین اعدادی در توان هیچ کامپیوتر کلاسیکی نیست. با این مثال ساده می‌بینیم که برخلاف سیستم‌های کلاسیک، سیستم‌های کوانتومی را هرگز نمی‌توان در کامپیوترهای کلاسیک شبیه سازی کرد.

این در حالی است که در ابعاد میکروسکوپی و در سطح بنیادین ماده تمامی سیستم‌ها رفتار کوانتومی دارند و ما برای درک رفتار ماده در مقیاس میکروسکوپی احتیاج به شبیه‌سازی رفتار ذرات و میدان‌های کوانتومی داریم. چگونه می‌توانیم از این بن‌بست راهی به بیرون بیابیم؟ نخستین بار ریچارد فاینمن راه برون رفت را نشان داد. برای شبیه‌سازی سیستم‌های کوانتومی می‌بایست از خود سیستم‌های کوانتومی استفاده کرد. به زبان امروزی، این راه چنین است. گروهی از اتم‌ها را تصور کنید که در شرایط خاص و تحت کنترل شما قرار گرفته‌اند. تعداد این اتم‌ها از مرتبه ۱۰۰۰ تا بیشتر است. این اتم‌ها می‌توانند در یک شبکه نوری[1] قرار گرفته باشند. یک شبکه نوری، شبکه‌ای متشکل از امواج ایستاده است که اتم‌ها مثل تخم‌مرغ‌های درون یک شانه تخم‌مرغ در درون فرورفتگی‌های آن قرار می گیرند. می توان روی این اتم‌ها انواع گیت‌های کوانتومی را اعمال کرد که مثل این

[1] Optical Lattice

است که بتوانیم دینامیک متناظر با هر نوع هامیلتونی را در مورد این اتم‌ها اعمال کنیم. می‌توانیم کاری کنیم که درجات آزادی این سیستم و نوع هامیلتونی آن خیلی نزدیک به درجات آزادی و نوع هامیلتونی یک سیستم دیگر باشد که می‌خواهیم شبیه‌سازی‌اش کنیم. حتی می‌توانیم برهم‌کنش‌ها را طوری تنظیم کنیم که این سیستم دوبعدی یک سیستم سه‌بعدی را شبیه‌سازی کند.

در این صورت، حالت اولیه این مجموعه اتم‌ها را مطابق با حالت اولیه سیستم مورد نظر خود به صورت فیزیکی تهیه می‌کنیم و اجازه می دهیم که این سیستم با هامیلتونی خاصی که برایش تدارک دیده‌ایم تحول پیدا کند. بعد از گذشت زمان دلخواه می‌توانیم هر نوع مشاهده‌پذیری از این سیستم را اندازه گیری کنیم. این اندازه گیری را می‌توانیم بارها و بارها تکرار کنیم تا متوسط مشاهده‌پذیر را محاسبه کنیم. به این ترتیب می‌توانیم کمیت‌های مورد نظر خود را از سیستم واقعی بدست بیاوریم. شبیه‌ساز ما به این ترتیب و به صورت واقعی یک سیستم کوانتومی دیگر را شبیه‌سازی می‌کند. این شبیه‌ساز حتی قادر است که میدان‌های کوانتومی را نیز با تقریب خوبی شبیه سازی‌کند. از نظر فناوری دیر نخواهد بود که ما بتوانیم در شبیه‌ساز کوانتومی خود میدان‌های کوانتومی ای نظیر میدان الکترو ضعیف و یا میدان کرومودینامیک را شبیه سازی کنیم و بتوانیم به سوال های بنیادی در مورد ساختار ماده پاسخ گوییم.

۳ـ۷ فرابرد کوانتومی

درفرابرد کوانتومی، هدف ما آن است که بامخابره اطلاعات کلاسیک حالت کوانتومی یک شی را به نقطه‌ای دوردست انتقال دهیم. درساده ترین حالت فرض کنید که آلیس یک کیوبیت S در اختیار دارد و می‌خواهد آن را به باب منتقل کند. فرض کنید کیوبیت S در حالت $|v\rangle_S = \alpha|0\rangle + \beta|1\rangle$ قرار دارد و آلیس و باب از آن مطلع نیستند. اگر بین آلیس و باب یک کانال وجود داشت که به وسیله آن می‌توانستند کیوبیت (اطلاعات کوانتومی) انتقال دهند، مسأله انتقال S ساده بود (کافی بود آلیس کیوبیت خود را در ورودی کانال قرار دهد). ولی فرض کنید که بین آنها فقط یک کانال برای انتقال اطلاعات کلاسیک (مانند تلفن معمولی) وجود دارد. سؤال این است که آیا در این صورت نیز انتقال S امکان‌پذیر است یا خیر. نکته‌ای که باید به آن توجه کنیم آن است که چرا اصولا نیاز است که کانالی با خواص کوانتومی برای انتقال یک حالت یا یک کیوبیت وجود داشته باشد؟ برای انتقال کامل یک کیوبیت از طریق کانال ارتباطی کلاسیک، لازم است که مقادیر مختلط α و β مخابره بشوند که برای مخابره دقیق این مقادیر نیاز به بی‌نهایت مخابره داریم، حتی تخمین آن‌ها هم مخابره زیادی از نظر تعداد بیت ارسالی می‌طلبد.

فرض کنید که آلیس و باب هر کدام یک کیوبیت دیگر دارند که مستقل از S در حالت درهم‌تنیده

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (۱\text{ـ}۷)$$

آماده سازی شده‌اند. پس در کل سه کیوبیت داریم. کیوبیت‌های A و S در دست آلیس هستند و کیوبیت B در دست باب.

حال، پایه متعامد یکه بل[1] را برای فضای دو کیوبیت در نظر بگیرید:

$$\mathcal{B} = \{\left|\Phi^+\right\rangle, \left|\Phi^-\right\rangle, \left|\Psi^+\right\rangle, \left|\Psi^-\right\rangle\} \qquad (۲\text{ـ}۷)$$

که در آن

$$\left|\Phi^\pm\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad \left|\Psi^\pm\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \qquad (۳\text{ـ}۷)$$

توجه کنید که داریم:

$$\begin{aligned} |00\rangle &= \frac{1}{\sqrt{2}}(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle) \quad |01\rangle = \frac{1}{\sqrt{2}}(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle), \\ |10\rangle &= \frac{1}{\sqrt{2}}(\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle) \quad |11\rangle = \frac{1}{\sqrt{2}}(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle). \end{aligned} \qquad (۴\text{ـ}۷)$$

حال، سیستم ترکیبی هر سه کیوبیت در حالت $|v\rangle_S \otimes |\Phi^+\rangle$ است که اگر SA را در پایه بل بنویسیم داریم:

$$\begin{aligned} &|v\rangle_S \otimes \left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}[\alpha\,|00\rangle_{SA}\,|0\rangle_B + \alpha\,|01\rangle_{SA}\,|1\rangle_B + \alpha\,|10\rangle_{SA}\,|0\rangle_B + \alpha\,|11\rangle_{SA}\,|1\rangle_B \\ &= \frac{1}{2}[\alpha(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle)_{SA}\,|0\rangle_B + \alpha(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle)_{SA}\,|1\rangle_B \\ &+ \beta(\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle)_{SA}\,|0\rangle_B + \beta(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle)_{SA}\,|1\rangle_B] \\ &= \frac{1}{2}[\left|\Phi^+_{SA}\right\rangle(\alpha\,|0\rangle + \beta\,|1\rangle)_B + \left|\Phi^-_{SA}\right\rangle(\alpha\,|0\rangle - \beta\,|1\rangle)_B \\ &+ \left|\Psi^+_{SA}\right\rangle(\alpha\,|0\rangle + \beta\,|1\rangle)_B + \left|\Psi^-_{SA}\right\rangle(\alpha\,|0\rangle - \beta\,|1\rangle)_B] \end{aligned} \qquad (۵\text{ـ}۷)$$

اگر ماتریس‌های پاولی را به خاط بیاوریم:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad (۶\text{ـ}۷)$$

خواهیم داشت

$$|v\rangle_S \otimes \left|\Phi^+\right\rangle_{AB} = \frac{1}{2}[\left|\Phi^+\right\rangle_{SA}|v\rangle_B + \left|\Phi^-\right\rangle_{SA} \otimes Z\,|v\rangle_B + \left|\Psi^+\right\rangle_{SA} \otimes X\,|v\rangle_B \left|\Psi^-\right\rangle_{SA} \otimes XZ\,|v\rangle_B]$$

[1] Bell basis

(۷ـ۷)

فرض کنیم آلیس دو کیوبیتی که در اختیار دارد، یعنی SA را در پایه بل اندازه‌گیری کند. در این صورت عملگرهای اندازه‌گیری آلیس برابرند با

$$M_1 = \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|, \quad M_2 = \left|\Phi^-\right\rangle\!\left\langle\Phi^-\right| \; M_3 = \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right|, \quad M_4 = \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| \qquad (۸ـ۷)$$

اگر برای مثال حاصل اندازه‌گیری آلیس M_1 باشد، با توجه به محاسبات فوق سیستم به حالت زیر تغییر می‌کند:

$$(M_{1,SA}\otimes I_B)\left|v\right\rangle_S\otimes\left|\Phi^+\right\rangle_{AB} = (\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|\otimes I_B)\left|v\right\rangle_S\otimes\left|\Phi^+\right\rangle_{AB} = \frac{1}{2}\left|\Phi^+\right\rangle_{SA}\left|v\right\rangle_B \qquad (۹ـ۷)$$

یعنی کیوبیت باب به حالت $|v\rangle$ تغییر پیدا می‌کند.در واقع بسته به حاصل اندازه‌گیری آلیس، تغییر کیوبیت باب به صورت زیر خواهد بود:

$$\begin{aligned} &M_1 \Rightarrow \left|V\right\rangle, \quad M_2 \Rightarrow Z\left|V\right\rangle, \\ &M_3 \Rightarrow X\left|V\right\rangle, \quad M_4 \Rightarrow XZ\left|V\right\rangle. \end{aligned} \qquad (۱۰ـ۷)$$

حال فرض کنید که آلیس بعد از انجام اندازه‌گیری، نتیجه را با استفاده از ۲ بیت کلاسیک فوق برای باب ارسال کند. در این صورت باب با توجه تناظر فوق می‌تواند وارون ماتریس پائولی مناسب را بر کیوبیت خود اعمال و حالت $|v\rangle$ به دست می‌آورد.

توجه کنید که در این پروتکل، اندازه‌گیری آلیس چهار حالت دارد. پس آلیس ۲ بیت اطلاعات کلاسیک برای باب می‌فرستد. همچنین حالت $|\Phi^+\rangle_{AB}$ که آلیس و باب از قبل با هم قسمت کرده بودند، یک واحد درهم‌تنیدگی یا ای‌ـبیت[1] نامیده می‌شود. به طور خلاصه

$$1\,ebit + 2\,bit \rightarrow 1\,qubit \qquad (۱۱ـ۷)$$

۴ـ۷ کدگذاری چگال

مساله کدگذاری چگال[2] دقیقا برعکس فرابرد است. یعنی، با در اختیار داشتن یک کانال کوانتومی، چگونه اطلاعات کلاسیک مخابره کنیم. در این آلیس و باب دو کیوبیت را مانند حالت قبل در حالت درهم‌تنیده

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (۱۲ـ۷)$$

[1] Entanglement bit or ebit
[2] Superdense Coding

تقسیم کرده‌اند. آلیس ۲ بیت کلاسیک دارد که می‌خواهد به باب منتقل کند. ولی کانال بین آنها یک کانال کوانتومی است. در اینجا نشان می‌دهیم که این کار با انتقال تنها ۱ کیوبیت امکان‌پذیر است. در واقع

$$1ebit + 1qubit \rightarrow 2bit \qquad (۱۳\text{ـ}۷)$$

نمادگذاری زیر را در نظر بگیرید:

$$\sigma_{00} = I, \quad \sigma_{01} = X, \qquad \sigma_{10} = Z, \quad \sigma_{11} = ZX. \qquad (۱۴\text{ـ}۷)$$

توجه کنید که این چهار عملگر یکانی هستند. پس آلیس می‌تواند هر یک از آن‌ها را بر کیوبیت خود A اثر دهد. داریم

$$\sigma_{00}^A \otimes I^B \left|\Phi^+\right\rangle = \left|\Phi^+\right\rangle, \quad \sigma_{01}^A \otimes I^B \left|\Phi^+\right\rangle = \left|\Phi^-\right\rangle, \qquad \sigma_{10}^A \otimes I^B \left|\Phi^+\right\rangle = \left|\Psi^+\right\rangle, \quad \sigma_{11}^A \otimes I^B \left|\Phi^+\right\rangle = \left|\Psi^-\right\rangle, \qquad (۱۵\text{ـ}۷)$$

پس نتیجه یکی از بردارهای پایه بل می‌شود و از آنجا که این حالت‌ها بر هم عمود هستند، اگر آلیس بعد از اثر دادن عملگر σ_{ij} کیوبیت خود را برای باب بفرستد، باب می‌تواند به طور دقیق تشخیص دهد که این دو کیوبیت در چه حالتی هستند و از آنجا می‌فهمد که آلیس کدام σ_{ij} را اثر داده است.

به طور دقیق‌تر، فرض کنید دو بیت آلیس $i, j \in 0, 1$ پروتکل این طور شروع می‌شود که آلیس σ_{ij} را روی کیوبیت A اعمال می‌کند و بعد این کیوبیت را از طریق کانال کوانتومی برای باب می‌فرستد. حال، باب دو کیوبیت A و B را در اختیار دارد و آنها را در پایه بل اندازه می‌گیرد (پس عملگرهای متناظر این اندازه‌گیری از رابطه به دست می‌آیند). از آنجا که چهار حالت $\sigma_{ij} \otimes I \left|\Phi^+\right\rangle$ بر هم عمودند، این اندازه‌گیری آن‌ها را از هم بدون خطا تشخیص می‌دهد. پس باب از روی حاصل اندازه‌گیری، می‌تواند i, j را بیابد.

۵ـ۷ الگوریتم‌های کوانتومی

۱ـ۵ـ۷ کیوبیت

مفهوم مرکزی در کامپیوتر کوانتومی بیت کوانتومی یا کیوبیت است. یک حافظه کوانتومی nـ کیوبیتی[1] عبارت است از مجموعه‌ای متشکل از n کیوبیت. فضای هیلبرت این حافظه عبارت است از:

$$(\mathcal{C}^2)^{\otimes n} = \{ \sum_{s_0, s_1, ..., s_{n-1} \in 0,1} \alpha_{s_0, s_1, ..., s_{n-1}} \left|s_0, s_1, ..., s_{n-1}\right\rangle \} \qquad (۱۶\text{ـ}۷)$$

و بعدِ آن برابر است با 2^n. دقت کنید که این حافظه می بایست چنان باشد که تمام بردارهای فضای هیلبرت آن قابل دسترسی باشند. بنابراین اگر دو کیوبیت را تنها کنارهم بگذاریم به این معنی نیست که یک حافظه دو

[1] n-qubit Quantum Register

کیوبیتی ساخته‌ایم. زیرا بردارهای فضای هیلبرت دو کیوبیت جداگانه به صورت زیر هستند:

$$|\phi\rangle \otimes |\phi\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes (\alpha' |0\rangle + \beta' |1\rangle) \qquad (۱۷\text{ـ}۷)$$

یعنی به صورت ضرب تنسوری دو بردار از فضاهای هرکدام از کیوبیت‌ها نوشته می‌شوند و حال آنکه در فضای هیلبرت دِو کیوبیت یعنی $(\mathcal{C}^2)^{\otimes 2}$بردارهایی وجود دارند که به صورت فوق قابل نوشتن نیستند، مثل بردار درهم‌تنیده $|\Phi^+\rangle$. برای آنکه یک بردار کلی به صورت

$$a |00\rangle + b |01\rangle + c |10\rangle + d |11\rangle \qquad (۱۸\text{ـ}۷)$$

به صورت حاصل ضرب تانسوری دو بردار نوشته شود، می‌بایست شرط $ad - bc = 0$ برقرار شود. بنابراین بردارهایی که به صورت ضرب تنسوری هستند، مجموعه‌ای با اندازه صفر را در فضای هیلبرت دو کیوبیت تشکیل می‌دهند.

۷ـ۵ـ۲ توازی کوانتومی

اولین تفاوت مهم کامپیوتر کوانتومی با کامپیوتر کلاسیک این است که یک حافظه کوانتومی می‌تواند در آن واحد در تمام حالت های بالقوه خود قرار بگیرد. این خصلت ناشی از برهم‌نهی حالت‌های کوانتومی است و اصطلاحاً توازی کوانتومی خوانده می‌شود. هرگاه هر حالت $|s_0, s_1, ..., s_{n-1}\rangle$ را برای کد کردن عددِ دودویی $s = (s_0, s_1, ..., s_{n-1})$ به کار ببریم، حالتی مثل

$$|\phi\rangle = \sum_{s=0}^{2^n-1} \phi_s |s\rangle , \qquad (۱۹\text{ـ}۷)$$

حالت کلی یک حافظه n کیوبیتی است. بنابراین هرگاه حافظه را در حالت $|\phi\rangle$ با ضرایب ناصفر قرار دهیم، مثل این است که همزمان آن را در تمام حالت‌های $|s\rangle$ قرار داده‌ایم. البته واضح است که هرگاه حافظه را در پایه محاسباتی اندازه‌گیری کنیم، تنها یکی از مقادیر s با احتمال $|\phi_s|^2$ بدست خواهند آمد. بنابراین توازی کوانتومی اگر چه یک خاصیت مهم حافظه است ولی این خاصیت را می‌بایست با ظرافت مورد بهره برداری قرار داد.

۷ـ۵ـ۳ گیت کوانتومی

اگر اطلاعات را در کیوبیت‌ها ذخیره کنیم، به ناچار پردازش اطلاعات می‌بایست یا با عملگرهای یکانی که تحول‌ها یا اندازه‌گیری‌ها را نشان می‌دهند انجام بگیرند. معمولا اصطلاح گیت کوانتومی برای یک عملگر یکانی به کار برده می‌شود. گیت کوانتومی هرگاه روی یک کیوبیت اثر کند آن را گیت تک کیوبیتی و هرگاه روی nتا کیوبیت اثر کند، گیت n کیوبیتی خوانده می‌شود. گیت‌های مهم همان عملگرهای یکانی مهم مانند

ماتریس‌های پاولی و عملگر هادامارد هستند. نکته مهم برای گیت‌های کوانتومی در مقابل گیت‌های کلاسیک، برگشت‌پذیر بودن آن‌هاست.

۷ـ۵ـ۴ روند یک الگوریتم کوانتومی

الگوریتم کوانتومی در ساده ترین شکل آن به مجموعه‌ای از گیت های کوانتومی متوالی گفته می‌شود که روی یک حالت معین اولیه اثر می‌کنند و چنان تنظیم شده‌اند که حالت نهایی چنان باشد که پس از اندازه‌گیری‌های سنجیده‌ای روی آن جواب یک مسئله معین را با احتمال بسیار خوب در بر داشته باشد. در ادامه چند الگوریتم مطرح کوانتومی را خواهیم دید.

۷ـ۶ الگوریتم دوچ‌ـجوزا

الگوریتم دوچ‌ـجوزا[1] که در سال ۱۹۸۲ مطرح شد به حل مسأله زیر می‌پردازد.

ورودی: تابع $F : \{0,1\}^n \to \{0,1\}$

شرط: یا F به ازای تمامی ورودی‌ها 0 می‌دهد و یا دقیقاً به ازای نصف ورودی‌ها صفر و به ازای نصف دیگر یک است.

خروجی: F کدام یک از دو حالت گفته شده است؟

یک الگوریتم احتمالاتی کلاسیک برای حل این مسأله این است که به ازای یک ورودی دلخواه خروجی تابع را چک کنیم. اگر یک بود حتماً تابع در حالت دوم است و اگر صفر بود، یا در حالت اول و یا در حالت دوم است که انتخاب تصادفی یکی از این دو حالت منجر به یک الگوریتم احتمالاتی می‌شود. حال اگر به دنبال یک الگوریتم کلاسیک باشیم که بتواند به صورت قطعی پاسخ درست دهد، باید حداقل $2^{n-1}+1$ تا از ورودی‌ها را چک کنیم. در اینجا نشان می‌دهیم که الگوریتمی کوانتومی وجود دارد که با فقط یک بار سوال پرسیدن کوانتومی[2] از تابع، می‌تواند به جواب قطعی برسد.

۷ـ۶ـ۱ سوال پرسیدن کوانتومی

قبل از پرداختن به الگوریتم کوانتومی توجه کنید که ابتدا باید سوال پرسیدن کوانتومی از تابع F را مدل کنیم. به طور کلاسیک ما، به سادگی فرض می‌کنیم که با ورودی x می‌توان خروجی $F(x)$ را بدست آورد. به طور کوانتومی ممکن این عمل را به صورت $|x\rangle \to |F(x)\rangle$ مدل کنیم، ولی توجه کنید که سوال پرسیدن در دنیای کوانتومی باید یکانی باشد. حال آنکه $|x\rangle \to |F(x)\rangle$ یکانی نیست چون بعد فضای ورودی و خروجی یکسان

[1] Deutsch–Jozsa
[2] Quantum Query

نیست. حتی اگر عملگر $|x\rangle \to |F(x)\rangle \left|\underbrace{000...0}^{n-1}\right\rangle$ در نظر بگیریم، باز هم یکانی نیست چون ضرب داخلی را حفظ نمی‌کند.

سؤال پرسیدن کوانتومی از یک تابع معمولاً به یکی از دو صورت زیر مدل می‌شود.

$$T_F |x\rangle = (-1)^{F(x)} |x\rangle \qquad (۲۰\text{ـ}۷)$$

و یا

$$O_F |x\rangle |y\rangle = |x\rangle |F(x) \oplus y\rangle \qquad (۲۱\text{ـ}۷)$$

در $T_{F(x)}$ با توجه به پاسخ تابع، فاز حالت را عوض می‌کنیم و در مدل $O_{F(x)}$ با استفاده از تغییر حالت $|y\rangle$ مقدار $F(x)$ برای ما روشن می‌شود. توجه شود که هردوی این عملگرها یکانی هستند و برای $|\psi\rangle = \sum_x \alpha_x |x\rangle$ داریم:

$$T_{F(x)} |\psi\rangle = \sum_x \alpha_x (-1)^{F(x)} |x\rangle \qquad (۲۲\text{ـ}۷)$$

و

$$O_{F(x)} |\psi\rangle |0\rangle = \sum_x \alpha_x |x\rangle |F(x)\rangle . \qquad (۲۳\text{ـ}۷)$$

۷ـ۶ـ۲ تبدیل فوریه روی گروه $\mathcal{Z}_2^n$

عملکرد گیت یک کیوبیتی هادامارد روی ورودی‌های $|0\rangle$ و $|1\rangle$ به صورت زیر است:

$$\begin{aligned} |0\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \qquad (۲۴\text{ـ}۷)$$

پس اگر ورودی $|b_i\rangle$ به صورت صفر یا یک باشد، خروجی عملگر هادامارد به صورت $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{b_i} |1\rangle)$ است. حال با در نظر گرفتن ورودی $|x\rangle = |b_1\rangle , |b_2\rangle , |b_3\rangle , ..., |b_n\rangle$ خروجی به صورت زیر خواهد بود:

$$\begin{aligned} H^{\otimes n} |x\rangle &= H |b_1\rangle \otimes H |b_2\rangle \otimes ... \otimes H |b_n\rangle \\ &= (\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{b_1} |1\rangle)) \otimes ... \otimes (\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{b_n} |1\rangle)) \\ &= \frac{1}{\sqrt{2^n}} \sum_{a_1,...,a_n \in 0,1} (-1)^{a_1 b_1 + ... + a_n b_n} |a_1 ... a_n\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{y \in 0,1^n} (-1)^{x.y} |y\rangle \end{aligned} \qquad (۲۵\text{ـ}۷)$$

که در آن $y = a_1 ... a_n$، آنگاه $x.y := a_1 b_1 + ... + a_n b_n$.

۷ـ۶ـ۳ الگوریتم اصلی

روند الگوریتم را به این صورت شروع می‌کنیم:

۱. حالت n کیوبیتی $|0...0\rangle$ را در نظر بگیرید.

۲. برای استفاده از توازی کوانتومی، همه بردارهای n کیوبیتی را در یک برهم‌نهی قرار می‌دهیم. باید عملگر هادامارد را روی همه کیوبیت‌ها اعمال کنیم.

۳. سپس یک بار از مدل تابع F یعنی T_F سوال می‌پرسیم.

۴. سپس با اعمال دوباره H تبدیل فوریه می‌گیریم.

۵. در نهایت حالت به دست آمده را اندازه‌گیری می‌کنیم.

$$
\begin{aligned}
\left|\underbrace{0...0}_{n}\right\rangle &\rightarrow^{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in 0,1^n} |x\rangle \\
&\rightarrow^{T_F} \frac{1}{\sqrt{2^n}} \sum_{x\in 0,1^n} (-1)^{F(x)} |x\rangle \\
&\rightarrow^{H^{\otimes n}} \frac{1}{2^n} \sum_{x\in 0,1^n} (-1)^{F(x)} \sum_{y\in 0,1^n} (-1)^{x.y} |y\rangle \\
&= \frac{1}{2^n} \sum_{y\in 0,1^n} \Big(\sum_{x\in 0,1^n} (-1)^{F(x)+x.y} \Big) |y\rangle
\end{aligned}
\qquad (۲۶ـ۷)
$$

اگر در حالت اول باشیم، یعنی تابع F متحد با صفر باشد، T_F عملگر همانی است، و از آنجا که $H^2 = I$، حالت نهایی با حالت اولیه برابر است و اندازه‌گیری نهایی به ما حالت $\left|\underbrace{0...0}_{n}\right\rangle$ می‌دهد.

فرض کنید که در حالت دوم باشیم. با توجه به جمله آخر، ضریب حالت $\left|\underbrace{0...0}_{n}\right\rangle$ در برهم‌نهی نهایی حساب می‌کنیم. چون $x.y = 0$ است، ضریب این جمله برابر است با $\sum_{x\in\{0,1\}^n}(-1)^{F(x)}$. اما، می‌دانیم که خروجی تابع F در نیمی از ورودی‌های 0 و در نیمی دیگر برابر با 1 است. در نتیجه، عبارت $\sum_{x\in\{0,1\}^n}(-1)^{F(x)}$ برابر با 0 است و کل حالت نهایی برهم‌نهی شده بر حالت $\left|\underbrace{0...0}_{n}\right\rangle$ عمود است و و حاصل حداقل یکی از n اندازه‌گیری برابر با 1 است.

به طور خلاصه، اگر حاصل همه اندازه‌گیری‌ها 0 شد، در حالت اول هستیم و اگر حداقل یکی از آن‌ها 1 شد، در حالت دوم هستیم.

۷ـ۷ الگوریتم جست‌وجوی گرور

مدل الگوریتم قبلی، از ساختار و ماهیت تابع به ما اطلاعی نمی‌دهند و صرفا با سوال پرسیدن از مدل، مقدار تابع را در ورودی مورد نظر به ما می‌دهند. گویی این مدل یک جعبه سیاه[1] است که ورودی را می‌گیرد و خروجی را با توجه به آنچه تابع روی آن اثر می‌کند، به ما می‌دهد. به این نوع مدل کردن، مدل جعبه‌ـسیاه یا مدل جستاری می‌گویند. قابل توجه است که پیچیدگی مسائل در این مدل بر حسب تعداد سوال‌کردن‌ها محاسبه می‌شود.

۱ـ۷ـ۷ مساله

ورودی: $f : \{0,1\}^n \to \{0,1\}$ شرط: دقیقاً یک $t \in \{0,1\}^n$ وجود دارد که $f(t) = 1$.

خروجی: t.

تعداد ورودی‌ها برابر با $N = 2^n$ می باشد. و به طور کلاسیک نمی‌توان این مساله را با پیچیدگی بهتر از $O(N)$ حل کرد. الگوریتم کوانتومی گرور[2] توانایی حل این مساله را با $O(\sqrt{N})$ سوال را دارد.

۸ـ۷ مقدمه

برای حل مساله فوق، سوال کوانتومی از تابع f را به صورت عملگر یکانی زیر مدل می‌کنیم:

$$T_f \left|x\right\rangle = (-1)^{f(x)} \left|x\right\rangle \qquad (۲۷ـ۷)$$

تعریف کنید

$$\left|s\right\rangle := \frac{1}{\sqrt{N-1}} \sum_{y\in\{0,1\}^n, y\neq t} \left|y\right\rangle . \qquad (۲۸ـ۷)$$

در نتیجه، $\langle s|t\rangle$ و

$$\left|\phi\right\rangle = \alpha \left|t\right\rangle + \beta \left|s\right\rangle \Rightarrow T_f \left|\phi\right\rangle = -\alpha \left|t\right\rangle + \beta \left|s\right\rangle \qquad (۲۹ـ۷)$$

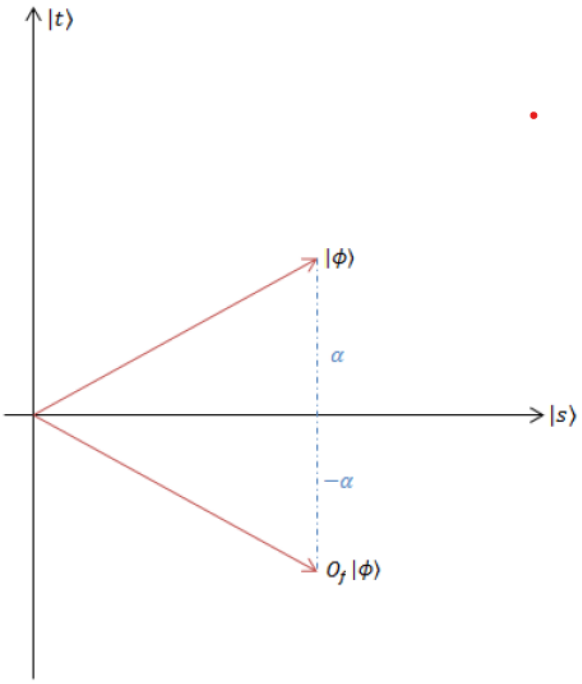
در واقع با توجه به شکل ۷ـ۱ ،اعمال T_f متناظر با قرینه کردن نسبت به بردار $\left|s\right\rangle$ است.

بردارهای $\langle v|$ و $|w\rangle$ را به صورت زیر تعریف کنید

$$\begin{aligned} \left|v\right\rangle &:= \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} \left|x\right\rangle \Rightarrow \left|v\right\rangle = \sqrt{\frac{N-1}{N}} \left|s\right\rangle + \frac{1}{\sqrt{N}} \left|t\right\rangle \\ \left|w\right\rangle &:= \frac{1}{\sqrt{N}} \left|s\right\rangle - \sqrt{\frac{N-1}{N}} \left|t\right\rangle \Rightarrow \langle v|w\rangle = 0 \end{aligned} \qquad (۳۰ـ۷)$$

[1] Black Box
[2] Grover

شکل ۷ـ۱: اعمال T_f که در واقع عمل قرینه‌کردن نسبت به $|s\rangle$ است.



تبدیل یکانی U را در نظر بگیرید:

$$U := H^{\otimes n}(2\,|0...0\rangle\langle 0...0| - I)H^{\otimes n} = 2H^{\otimes n}\,|0...0\rangle\langle 0...0|\,H^{\otimes n} - I \qquad (۳۱\text{ـ}۷)$$

می‌دانیم

$$H^{\otimes n}\,|0...0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle \quad = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle = |v\rangle \qquad (۳۲\text{ـ}۷)$$

در نتیجه،

$$U = 2\,|v\rangle\langle v| - I \qquad (۳۳\text{ـ}۷)$$

و برای $|\psi\rangle = \gamma\,|v\rangle + \lambda\,|w\rangle$ داریم:

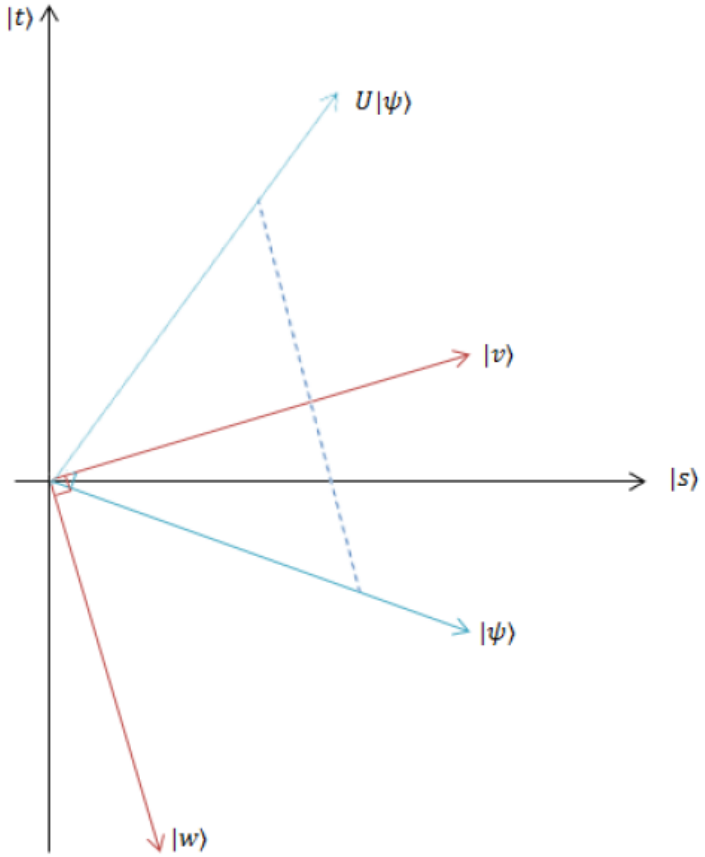
$$U\,|psi\rangle = \gamma U\,|v\rangle + \lambda U\,|w\rangle = \gamma\,|v\rangle - \lambda\,|w\rangle \qquad (۳۴\text{ـ}۷)$$

نتیجه می‌شود که U نسبت به $|v\rangle$ عمل قرینه انجام می‌دهد. (شکل ۷ـ۲)

همانطور که می‌دانیم، ترکیب دو عمل قرینه، یک عمل دوران بدست می‌دهد. (شکل ۷ـ۳)

$$f = R_{2\theta} \qquad (۳۵\text{ـ}۷)$$

شکل ۷ـ۲: اعمال U که در واقع عمل قرینه‌کردن نسبت به $|v\rangle$ است.



که در آن

$$cos\theta = \langle v|s\rangle = \sqrt{\frac{N-1}{N}} \Rightarrow \theta \approx \frac{1}{\sqrt{N}} \qquad (۳۶ـ۷)$$

۷ـ۹ الگوریتم اصلی

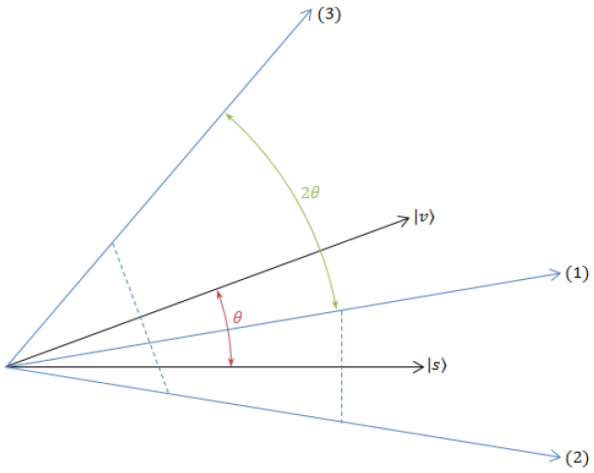
با n کیوبیت که همگی در حالت $|0\rangle$ آماده‌سازی شده‌اند شروع می‌کنیم. ابتدا، روی هر یک از n کیوبیت عملگرد هامارد را اعمال می‌کنیم و بعد $R_{2\theta}$ را q بار و در آخر همه n کیوبیت را اندازه‌گیری می‌کنیم:

$$|0...0\rangle \rightarrow^{H^{\otimes n}} |v\rangle \rightarrow^{(UT_f)^q} |\tau\rangle \rightarrow measurement \qquad (۳۷ـ۷)$$

$|\tau\rangle$ یک بردار با زاویه $\theta + 2q\theta$ از $|s\rangle$ می‌باشد. اگر $q \approx \frac{\sqrt{N}}{4}\pi$ بگیریم، این زاویه تقریبا برابر با $\pi/2$ خواهد بود. در این صورت $|\tau\rangle$ تقریبا با $|t\rangle$ برابر است. حال با اندازه‌گیری τ، حاصل اندازه‌گیری با احتمال

$$p(t) = \| \langle t|(UT_f)^q|v\rangle \|^2 = \| \langle t|\tau\rangle \qquad (۳۸ـ۷)$$

$(2) = T_f(1), (3) = U(2)$ شکل ۷ـ۳:



برابر t خواهد شد، و از آنجا که $|t\rangle$ و $|\tau\rangle$ به هم نزدیک است، این عدد نزدیک به 1 است.

فصل هشتم

پیچیدگی ارتباطی کوانتومی

در فضای پیچیدگی ارتباطی، آیا می‌توان از مکانیک کوانتومی به نحوی بهره برد که پیچیدگی مخابره نیز کاهش یابد؟ قضیه هولف[1] نشان می‌دهد که اگر بنا باشد که فقط n کیوبیت بین دو نفر جابه‌جا کنیم، امکان ندارد که بین آن دو بتوانیم چیزی فراتر از n بیت کلاسیک جابه‌جا کنیم؛ مگر این که کیوبیت‌های دو طرف درهم‌تنیده باشند. [۹] لبته در این صورت هم فقط می‌توان دوبرابر تعداد کیوبیتی که می‌فرستیم، بیت ارسال کنیم. در یک تناقض آشکار، مسائلی وجود دارد که الگوریتم‌های توزیع شده کوانتومی، به صورت بهینه توسط سیستم کلاسیک شبیه‌سازی نمی‌شوند. در این بخش، تفاوت اطلاعات و محاسبات توزیع شده برای یک سیستم با تنظیمات کوانتومی، چه به صورت کانال کوانتومی و چه به صورت استفاده از کیوبیت‌های درهم‌تنیده را نشان می‌دهیم و پروتکل‌های کوانتومی را برای چند مساله مطرح معرفی می‌کنیم. مطالب این بخش از [۳، ۸] اقتباس شده است.

[1] Holevo's Theorem

۸ـ۱ یک سوال کوانتومی

تصور کنید که آلیس و باب مسائل پیچیدگی ارتباطی، این اجازه را داشته باشند که در یک کانال کوانتومی و با ارسال کیوبیت‌ها با هم ارتباط برقرار کنند و یا این که قبل از شروع مخابره، با هم یک حالت کوانتومی درهم‌تنیده را تقسیم کنند.

برای مدل اول، فرض کنید که حالت بین دو طرف از سه قسمت تشکیل شده است، فضای مخفی آلیس، کانال و فضای مخفی باب. حالت شروع اولیه را برای یک تابع مانند $f : X \times Y \to \{0,1\}$ به صورت $|x\rangle |0\rangle |y\rangle$ فرض کنید که در آن $x \in X$ ورودی آلیس است و $y \in Y$ ورودی باب و کانال در حالت اولیه $|0\rangle$ قرار دارد. حال آلیس می‌تواند محاسبات و انتقال پیام روی کانال را با استفاده از عملگرهای یکانی بر روی حالت خودش و حالت کانال انجام دهد و باب به همین ترتیب. در انتهای پروتکل، آلیس یا باب با انجام یک اندازه‌گیری، نتیجه پروتکل را اعلام می‌کند. [۱۸]

در مدل دوم، آلیس و باب تعداد نامحدودی کیوبیت درهم‌تنیده با هم به اشتراک می‌گذارند، ولی در ادامه پروتکل از یک کانال کلاسیک با قابلیت ارسال بیت معمولی استفاده می‌کنند. برای محاسبه پیچیدگی، تنها بیت‌های ارسال شده را می‌شمریم و نه تعداد ای‌ـبیت‌ها را. پروتکلی با این سیستم را می‌توان با استفاده از پروتکل مدل اول با سربار 2 برابر شبیه‌سازی کرد، مانند کاری که در فرابرد کوانتومی کردیم. توجه کنید که یک بیت درهم‌تنیده می‌تواند حکم یک بیت تصادفی مشترک بین آلیس و باب را داشته باشد. [۶]

مدل سوم، از قدرت هر دو مدل استفاده می‌کند: آلیس و باب تعداد بی‌نهایتی کوبیت در هم تنیده در اشتراک دارند و از یک کانال کوانتومی برای انتقال اطلاعات استفاده می‌کنند. توجه کنید که این مدل هم با یک سربار با ضریب ۲ معادل حالت دوم است، با استفاده از فرابرد کوانتومی.

حال سوالی که مطرح می‌شود این است: آیا به بهبودی دست می‌یابیم؟ طبق مقدمه، قضیه هولف نشان می‌دهد اطلاعات کوانتومی مخابره شده فراتر از اطلاعات کلاسیک مخابره شده نخواهد بود مگر آنکه یک حالت درهم‌تنیده داشته باشیم. ولی مساله‌ای که با آن روبرو هستیم، مساله مخابره اطلاعات کامل نیست. در واقع آلیس یا باب علاقه‌مند به ورودی طرف دیگر نیستند، بلکه هدف این کار محاسبه یک تابع $f(x,y)$ با خروجی 1 بیت است. مفهومی که مرز مخابره و محاسبه توزیع شده را جدا می‌کند، در مثال‌های زیر به خوبی نمایش داده شده است.

۸ـ۲ الگوریتم دوچ‌ـجوزا: توزیع شده

اولین فاصله پیچیدگی ارتباطی کوانتومی و کلاسیک، در همتای ارتباطی و توزیع شده الگوریتم پرس‌وجوی دوچ‌ـجوزا مطرح شد. [۷] در این مساله، آلیس و باب هر کدام یک رشته n بیتی دارند که برای این ورودی وعده‌ای به ما داده شده است. توجه کنید که این مساله، نوع وعده‌داده‌شده[1] از مساله برابری است. وعده مذکور به شرح زیر است:

مساله دوچ‌ـجوزا توزیع شده: یا $x = y$ و یا x و y دقیقا در $n/2$ بیت‌ها با هم اختلاف دارند (n سایز ورودی‌های x و y است).

حال پروتکلی را مطرح می‌کنیم که با استفاده از $\log(n)$ کیوبیت مساله را حل می‌کند:

۱. آلیس برای باب حالت $\log n$ـ کیوبیتی $\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(-1)^{x_i}|i\rangle$ را ارسال می‌کند. این حالت با استفاده از عملگر یکانی H و حالت اولیه $|0...0\rangle$ و عملگر یکانی T_f به دست می‌آید.

۲. باب هم عملگر $|i\rangle \to (-1)^{y_i}|i\rangle$ را اعمال می‌کند و سپس عملگر هادامارد را. سپس اندازه‌گیری انجام می‌دهد.

۳. اگر خروجی اندازه‌گیری برابر با $\left|0^{\log n}\right\rangle$ بود، خروجی 1 می‌دهد و در غیر این صورت خروجی 1.

توجه کنید که تنها $\log n$ کیوبیت مخابره شده است. همچنین، برای فهم درستی قضیه به این توجه کنید که حالتی که در نهایت باب اندازه‌گیری می‌کند، در حالت برهم‌نهی شده زیر است:

$$H^{\otimes logn}(\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(-1)^{x_i+y_i}|i\rangle) = \frac{1}{n}\sum_{i=1}^{n}(-1)^{x_i+y_i} + \sum_{j\in\{0,1\}^{logn}}(-1)^{i.j}|j\rangle \qquad (۱ـ۸)$$

تنها مساله‌ای که در مورد عبارت فوق باید به آن توجه کنیم آن است که ضریب پایه $\left|0^{logn}\right\rangle$ در هر حالت برابر با چند می‌شود. با کمی بررسی متوجه می‌شویم که این ضریب برابر با $\frac{1}{n}\sum_{i=1}^{n}(-1)^{x_i+y_i}$ که برابر با یک خواهد بود اگر و تنها اگر $x = y$. ادامه درستی مساله مانند فصل پیشین است.

این پیشرفت در مخابره درحالی است که اگر می‌خواستیم این عملیات را با مخابرات کلاسیک و قطعی انجام دهیم، پیچیدگی معادل با $O(n)$ می‌داشتیم.

۸ـ۲ـ۱ مساله اشتراک

اگر آلیس و باب هر کدام یک ورودی به اندازه n بیت داشته باشند، که x ورودی آلیس و y ورودی باب باشد، هدف از مخابره یافتن i است که $x_i = y_i$. تلاش می‌کنیم بر اساس الگوریتم جست‌وجوی گروور، یک پروتکل

[1] Promise Problem

بهینه برای این مساله ارائه دهیم. [۷] لازم است ابتدا بدانیم ورودی مساله جست‌وجوی ما چیست.

قرار دهید که

$$z_i = x_i \wedge y_i. \qquad (۲\text{ـ}۸)$$

در نتیجه مساله جست‌وجو برابر با یافتن iی خواهد بود که در آن $z_i = 1$. ایده اصلی آن است که آلیس و باب با کمک به هم الگوریتم گروور را اجرا کنند. نکته‌ای که نیاز به همکاری در آن حس می‌شود، عملگر یکانی T_z است. آلیس برای این که بدون آن که اطلاعاتی به صورت بیتی به باب در مورد ورودی خودش بدهد، بتواند عملگر T_z را روی یک حالت مانند $|\phi\rangle$ اجرا کند، که

$$|\phi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle \qquad (۳\text{ـ}۸)$$

لازم است از یک کیوبیت کمکی استفاده کند و توجه کنید که حالت $|\phi\rangle$ یک حالت $\log n$ کیوبیتی است. آلیس یک کیوبیت با مقدار اولیه 0 در کنار $\log n$ کیوبیت دیگر قرار می‌دهد و سپس عملگر O_x را روی آن اجرا می‌کند:

$$|\phi\rangle \rightarrow^{\otimes|0\rangle} |\phi\rangle |0\rangle \rightarrow^{O_x} T_x |\phi\rangle |0\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle |x_i\rangle \qquad (۴\text{ـ}۸)$$

سپس آلیس این $\log n + 1$ کیوبیت را برای باب می‌فرستد.

باب عملگر یکانی زیر را اعمال می‌کند و سپس نتیجه را برای آلیس می‌فرستد.

$$|i\rangle |x_i\rangle \rightarrow (-1)^{x_i \wedge y_i} |i\rangle |x_i\rangle \qquad (۵\text{ـ}۸)$$

آلیس آخرین کیوبیت را برابر با $|0\rangle$ می‌گذارد (چون x را دارد این عمل یکانی است). پس در نتیجه، آلیس $T_z |\phi\rangle$ را دارد. در نتیجه، آلیس و باب می‌توانند با $O(\log n)$ کیوبیت مخابره، یک بار اعمال T_z را شبیه‌سازی کنند. برای اجرای کامل الگوریتم جست‌وجو، نیاز به $\sqrt{n}$ مرحله مخابره داریم که در نهایت پیچیدگی کوانتومی $O(\log n\sqrt{n})$ برای این مساله نشان داده می‌شود. درحالی است که این مساله حتی در حالت احتمالاتی پیچیدگی کلاسیک $O(n)$ را دارد.

فصل نهم

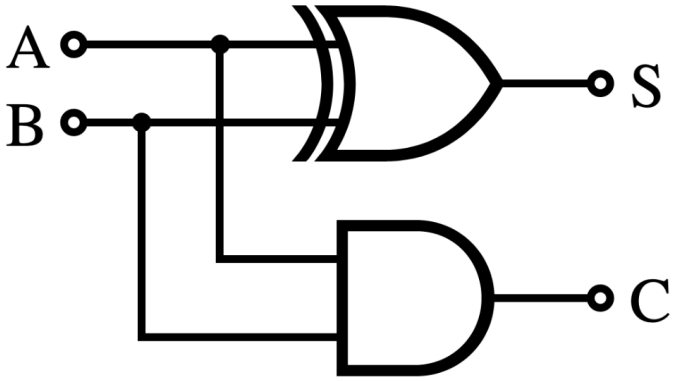
شبیه‌سازی الگوریتم‌ها و پروتکل‌های کوانتومی

در مورد این مساله که ذات مکانیک کوانتومی پیچیده است شکی نداریم. مساله‌ای که از آن پیچیده‌تر به نظر می‌رسد، الگوریتم‌های کوانتومی هستند. شهود بشریت با مسائلی مانند توپ و اهرم سازگارتر از مفاهیمی مانند الکترون و فوتون است و به نظر می‌رسد اتفاقاتی که در دنیای کوانتومی رخ می‌دهد چیزی شبیه جادو باشد. اما با کمی درنگ متوجه می‌شویم که همانند فیزیک کلاسیک، فیزیک کوانتومی از یک سری قائده و اصول مشخص پیروی می‌کند. اصولی که با بهره‌برداری هوشمندانه به بشریت در محاسبات، شبیه‌سازی و ... قدرتی بیش از پیش می‌دهد. برای ما، اولین قدم برای درک این قدرت محاسبات کوانتومی است.

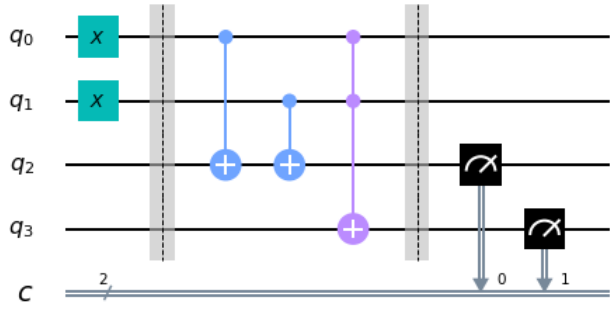
۹ـ۱ مدار کوانتومی

در دنیای کلاسیک، هر اطلاعاتی را می‌توان به صورت بیت‌های 0 و 1 نشان داد. همچنین، محاسبات را می‌توان از طریق مدارهای دیجیتالی پیش برد. مداری مانند شکل ۹ـ۱ را به یاد بیاورید. در مورد دنیای محاسبات کوانتومی نیز همین مساله صادق است. مثلا مدار کوانتومی شکل ۹ـ۲ کار مدار دیجیتالی شکل۹ـ۱ را انجام می‌دهد. که همان جمع دو بیت و یا دو کیوبیت است. ابزاری که در ادامه برای شبیه‌سازی مفاهیم و الگوریتم‌های کوانتومی استفاده می‌کنیم کتابخانه پایتون $qisikit$ [۱] محصول شرکت IBM از پیشروهای علم محاسبات

شکل ۹ـ۱: مدار دیجیتالی ساده



شکل ۹ـ۲: مدار کوانتومی ساده



کوانتومی است.

۹ـ۱ـ۱ اندازه‌گیری

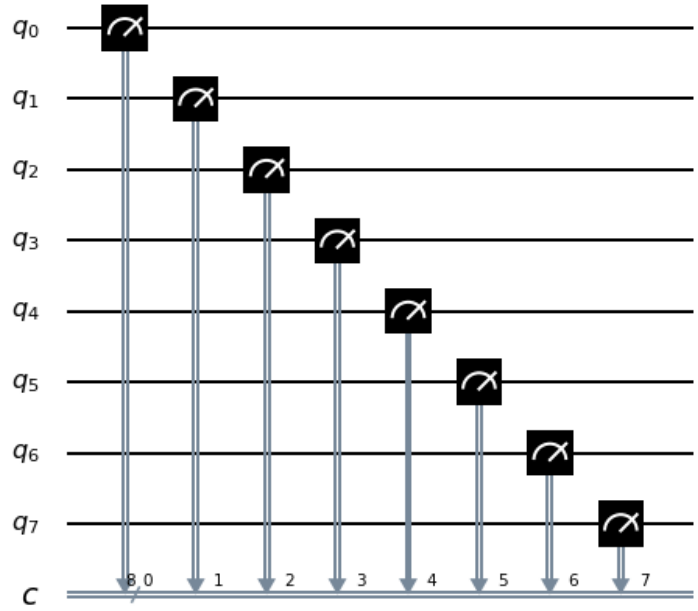
در شکل کد ۹ـ۳ تلاش می‌کنیم یک مدار کوانتومی ساده با اندازه اولیه 8 کیوبیت که همه در حالت $|0\rangle$ بسازیم و سپس آن‌ها را اندازه بگیریم. شکل مدار به صورت ۹ـ۴ خواهد بود. به نمادی که برای اندازه‌گیری مشخص

شکل ۹ـ۳: ساخت مدار کوانتومی با 8 کیوبیت و سپس اندازه‌گیری

```
from qiskit import QuantumCircuit, execute, Aer
from qiskit.visualization import plot_histogram
n = 8
n_q = n
n_b = n
qc_output = QuantumCircuit(n_q,n_b)
for j in range(n):
    qc_output.measure(j,j)
qc_output.draw()
```

می‌کنیم توجه کنید. توجه کنید که کامپیوترهای کوانتومی و محاسبات کوانتومی شامل مقداری رفتار تصادفی هستند. به همین منظور، گاها نتایج چندین بار تکرار می‌شود تا به صورت آماری‌ـاحتمالی نتایج بررسی شود.

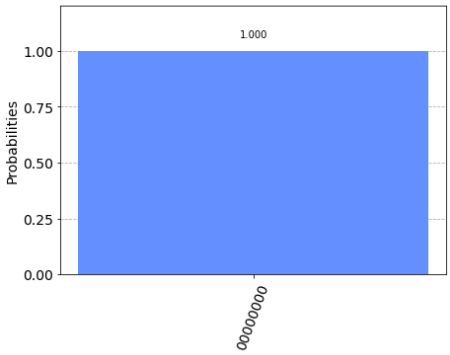
شکل ۹ـ۴: مدار کوانتومی اندازه‌گیری



مانند شکل ۹ـ۵. همچنین خوب است بدانیم که چون این ماشین‌های کلاسیک هستند که عملکرد ماشین

شکل ۹ـ۵: بردار نتایج بعد از چندبار اجرا

```
In [8]: counts = execute(qc_output,Aer.get_backend('qasm_simulator')).result().get_counts()
        plot_histogram(counts)
```



کوانتومی را شبیه‌سازی می‌کنند، توانایی بیشتر از 30 کیوبیت محاسبه را ندارند.

۹ـ۱ـ۲ مدار جمع‌کننده

برای طراحی مدارهای بیشتر، لازم است که با گیت‌های بیشتری آشنا شویم. به یاد داریم که گفته بودیم هر گیت کوانتومی یک عملگر یکانی است. پس عملگرهای یکانی مانند

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (۱ـ۹)$$

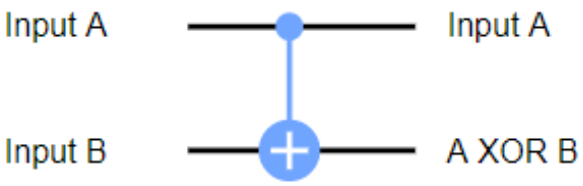
$$Z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{۲-۹}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{۳-۹}$$

$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{۴-۹}$$

همه گیت‌های منطقی کوانتومی برگشت‌پذیر هستند. توجه کنید که عملگر دو کیوبیتی CX یا نات‌ـکنترل‌شده[1] عملگری است که برای هر دو کیوبیت ورودی، اگر کیوبیت اولیه برابر با 1 باشد، خروجی دوم را NOT ورودی دوم قرار می‌دهد و بالعکس. همچنین خروجی اول با ورودی اول برابر است. به شکل ۹ـ۶ توجه کنید. همانطور که می‌بینید، این عملگر همان XOR است، اما برگشت‌پذیر هم هست! نکته‌ای که در دنیای دیجیتال

شکل ۹ـ۶: گیت CX



نداریم.

حال لازم است که یک گیت AND هم داشته باشیم که برگشت‌پذیر هم باشد. گیت کوانتومی معادلی آن، گیت $Toffoli$ است که روی فضای 3 کیوبیت اعمال می‌شود.

$$CCX = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{۵-۹}$$

[1] Controlled-Not

این گیت، اگر دو کیوبیت ورودی اول 1 باشند، خروجی 1 می‌دهند.

حال لازم است مدار را بسازیم:

۱. لازم است که دو بیت اول با هم XOR بشوند تا بیت کم ارزش مشخص شود.

۲. برای مشخص کردن بیت پر ارزش هم لازم است که دو کیوبیت با هم AND بشوند.

۳. برای این‌کارها، ۴ کیوبیت تعریف می‌کنیم. دو ورودی، دو خروجی و دو بیت کلاسیک برای اندازه گیری.

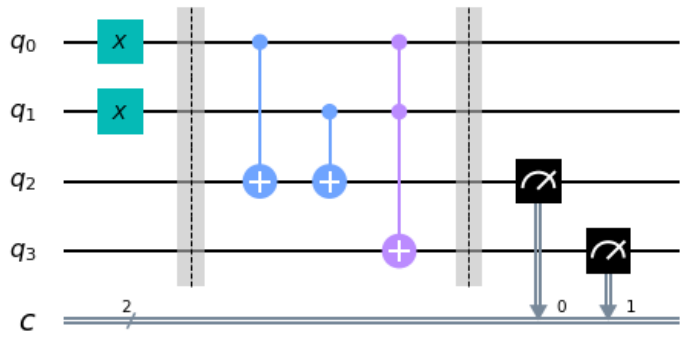
کد شکل ۹ـ۷ قرار است دو کیوبیت در حالت $|1\rangle$ و $|1\rangle$ را جمع کند. مدار نهایی در شکل ۹ـ۸ نشان داده

شکل ۹ـ۷: کد مدار جمع‌کننده

```
In [8]:
qc_ha = QuantumCircuit(4,2)
# encode inputs in qubits 0 and 1
qc_ha.x(0)
qc_ha.x(1)
qc_ha.barrier()
# use cnots to write the XOR of the inputs on qubit 2
qc_ha.cx(0,2)
qc_ha.cx(1,2)
# use ccx to write the AND of the inputs on qubit 3
qc_ha.ccx(0,1,3)
qc_ha.barrier()
# extract outputs
qc_ha.measure(2,0) # extract XOR value
qc_ha.measure(3,1) # extract AND value

qc_ha.draw()
```

شده است. مانند حالت پیشین تعدادی بار این کار را تکرار می‌کنیم تا نتیجه را ببینیم. (شکل ۹ـ۹)

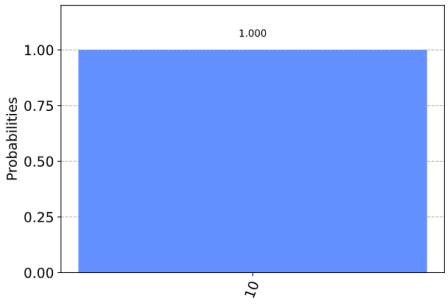
شکل ۹ـ۸: مدار جمع‌کننده



۹ـ۲ فرابرد کوانتومی

در این مرحله، یک کد ساده برای اجرای فرابرد کوانتومی اجرا می‌کنیم. مراحل کار را به یاد می‌آوریم:

شکل ۹ـ۹: تکرار مدار



۱. ابتدا آلیس و باب می‌بایست دو کیوبیت درهم‌تنیده در اشتراک بگذارند.

۲. آلیس عملگر هادامارد را روی کیوبیتی که می‌خواهد ارسال کند، اجرا می‌کند.

۳. آلیس مقدار کیوبیت خود و کیوبیت ارسالی را اندازه می‌گیرد.

۴. مقدارهای به دست آمده را در اختیار باب می‌گذارد.

۵. باب با توجه به مقادیر به دست آمده، عملگرهای مختلف را روی کیوبیت خودش اعمال می‌کند.

در شکل ۹ـ۱۰ کد مربوط به این کار را می‌بینید. در شکل ۹ـ۱۱ که مدار نهایی را نشان می‌دهد، کیوبیت اول بنا است که ارسال شود. کیوبیت دوم و سوم درهم‌تنیده شده‌اند و کیوبیت دوم در اختیار آلیس و کیوبیت سوم در اختیار باب است. در نهایت، نتیجه اندازه‌گیری آلیس بر روی دو ثبات کلاسیک می‌نشیند که در اختیار باب است و با توجه به نتیجه آن‌ها، عملگرهای X و Z را روی کیوبیت خود اجرا می‌کند. شکل مدار به صورت ۹ـ۱۱ است.

در نهایت با اندازه‌گیری حالت باب در یک ثبات دیگر می‌توانیم ببینم چگونه آخرین کیوبیت اندازه‌گیری شده همواره 0 است.

۹ـ۳ الگوریتم دوچ‌ـجوزا

برای یادآوری، مراحل زیر یک اجرای الگوریتم دوچ‌ـجوزا برای تشخیص ثابت یا مجموع صفر بودن تابع f است.

۱. دو ثبات کوانتومی آماده می‌کنیم. یکی با n بیت و دیگری با 1 بیت. اولی را با 0 مقداردهی اولیه می‌کنیم و دومی را با 1.

$$|\psi_0\rangle = |0\rangle^{\otimes 0} |1\rangle \qquad (۶ـ۹)$$

شکل ۹ـ۱۰: کد مدار فرابرد کوانتومی

In [11]:
```
# Protocol uses 3 qubits and 2 classical bits in 2 different registers
qr = QuantumRegister(3)
crz, crx = ClassicalRegister(1), ClassicalRegister(1)
teleportation_circuit = QuantumCircuit(qr, crz, crx)

## STEP 1
def create_bell_pair(qc, a, b):
    qc.h(a) # Put qubit a into state |+>
    qc.cx(a,b) # CNOT with a as control and b as target
create_bell_pair(teleportation_circuit, 1, 2)

## STEP 2
teleportation_circuit.barrier()
def alice_gates(qc, psi, a):
    qc.cx(psi, a)
    qc.h(psi)
alice_gates(teleportation_circuit, 0, 1)

## STEP 3
def measure_and_send(qc, a, b):
    qc.barrier()
    qc.measure(a,0)
    qc.measure(b,1)
measure_and_send(teleportation_circuit, 0 ,1)

## STEP 4
teleportation_circuit.barrier() # Use barrier to separate steps
def bob_gates(qc, qubit, crz, crx):
    qc.x(qubit).c_if(crx, 1) # Apply gates if the registers
    qc.z(qubit).c_if(crz, 1) # are in the state '1'
bob_gates(teleportation_circuit, 2, crz, crx)
teleportation_circuit.draw()
```

۲. سپس عملگرد هادامارد را روی هر کیوبیت اجرا می‌کنیم.

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle \left(|0\rangle - |1\rangle\right) \qquad (۹ـ۷)$$

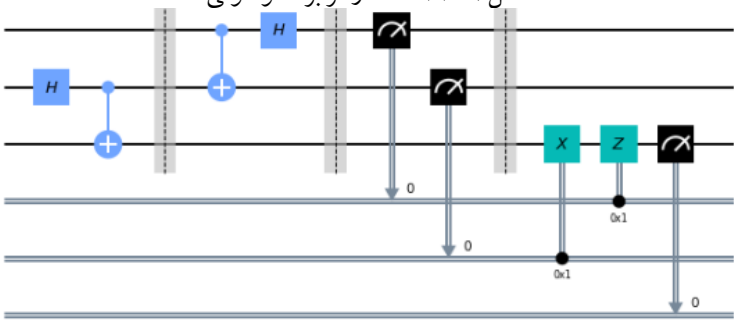
۳. جعبه سیاه تابع f را به این صورت اعمال می‌کنیم که در شکل۹ـ۱۳ نشان داده شده است.

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle \left(|f(x)\rangle - |f(x)\oplus 1\rangle\right) \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle\right) \end{aligned} \qquad (۹ـ۸)$$

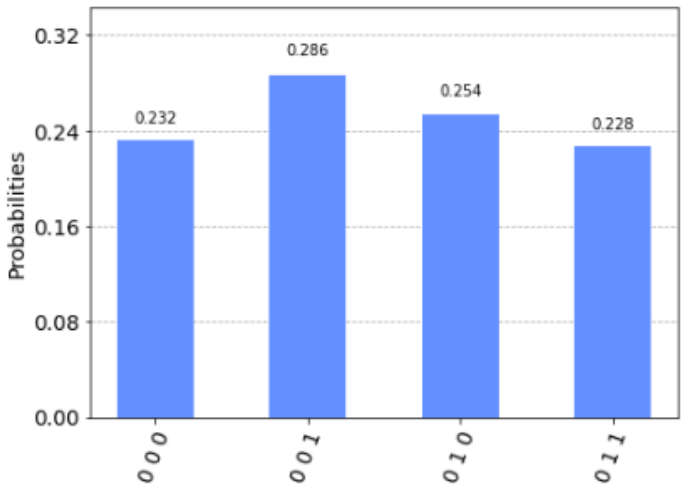
۴. در این مرحله، کیوبیت دوم را حذف می‌کنیم و یک بار دیگر هادامارد را اعمال می‌کنیم.

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} [\sum_{y=0}^{2^n-1} (-1)^{x.y} |y\rangle] \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} [\sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x.y}] |y\rangle \end{aligned} \qquad (۹ـ۹)$$

شکل ۹ـ۱۱: مدار فرابرد کوانتومی



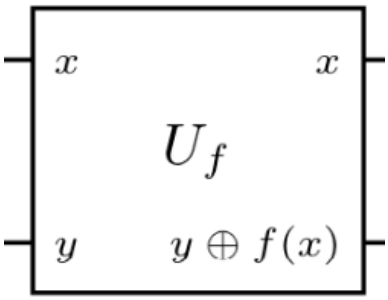
شکل ۹ـ۱۲: نتیجه اجرای کد به تعداد زیاد



۵. در نهایت با اندازه‌گیری کلیه کیوبیت‌ها، نتیجه‌گیری می‌کنیم.

در مرحله اول، تلاش می‌کنیم که یک جعبه‌سیاه برای این تابع بسازیم. بدین منظور، لازم است که شکل تابع را مشخص کنیم. فرض کنید عملیات را روی 4 کیوبیت انجام می‌دهیم. در شکل ۹ـ۱۴، دقیقا عملیاتی که در مرحله سوم الگوریتم بالا رخ داد انجام شده است. در این تابع، یک تابع مجموع صفر را برنامه نویسی می‌کنیم. که شکل ۹ـ۱۵ این مدار را نشان می‌دهد. در ادامه، لازم است ورودی‌ها را بچینیم و مرحله 1 و 2 را انجام دهیم. سپس جعبه سیاه را وصله کنیم و مرحله 4 و 5 را اعمال کنیم. برای اینکار به شکل ۹ـ۱۶ توجه کنید. که مدار آن را در شکل ۹ـ۱۷ می‌بینیم. در نهایت، اجرای چندباره این الگوریتم با این تابع نشان می‌دهد احتمال گرفتن 0000 در خروجی 0 است. (شکل ۹ـ۱۸)

شکل ۹ـ۱۳: جعبه‌سیاه تابع f



شکل ۹ـ۱۴: کد دوچ‌ـجوزا ـ جعبه سیاه

```
balanced_oracle = QuantumCircuit(4+1)
b_str = "1010"

# Place X-gates
for qubit in range(len(b_str)):
    if b_str[qubit] == '1':
        balanced_oracle.x(qubit)
balanced_oracle.barrier()

# Controlled-NOT gates
for qubit in range(4):
    balanced_oracle.cx(qubit, 4)

balanced_oracle.barrier()

# Place X-gates
for qubit in range(len(b_str)):
    if b_str[qubit] == '1':
        balanced_oracle.x(qubit)

# Show oracle
balanced_oracle.draw()
```

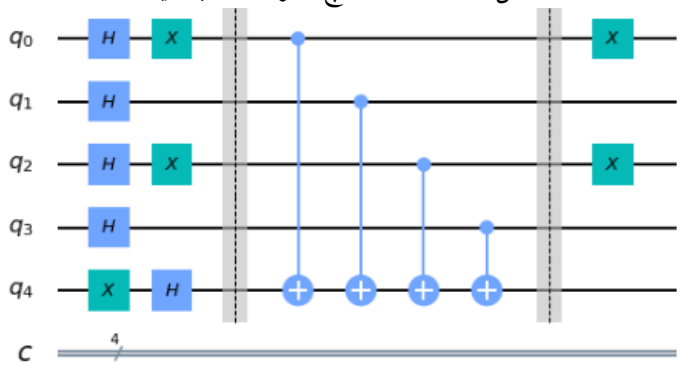
۹ـ۴ الگوریتم دوچ‌ـجوزا توزیع‌شده

در ادامه قسمت قبل، الگوریتم ارائه شده در قسمت ۸ـ۲ را پیاده‌سازی می‌کنیم.

کد مربوط به این قسمت نسبت به کدهای قبلی طویل‌تر است و ارائه قسمت به قسمت آن در این مجال ممکن نیست. در پیوست دوم (قسمت ـ۲)، کل کد تکه به تکه به همراه مدار مربوط به هر قسمت به تفضیل بررسی خواهد شد.

مدار نهایی و نتیجه اجرای کد، در شکل‌های ۹ـ۲۰ و ۹ـ۱۹ آورده‌شده است.

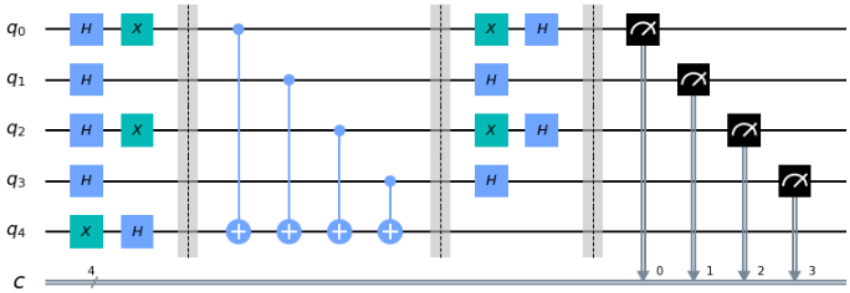
شکل ۹ـ۱۵: مدار دوچ‌ـجوزا ـ جعبه سیاه

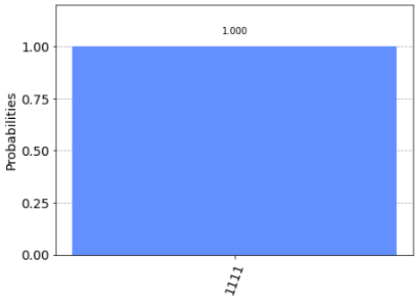


شکل ۹ـ۱۶: کد دوچ‌ـجوزا

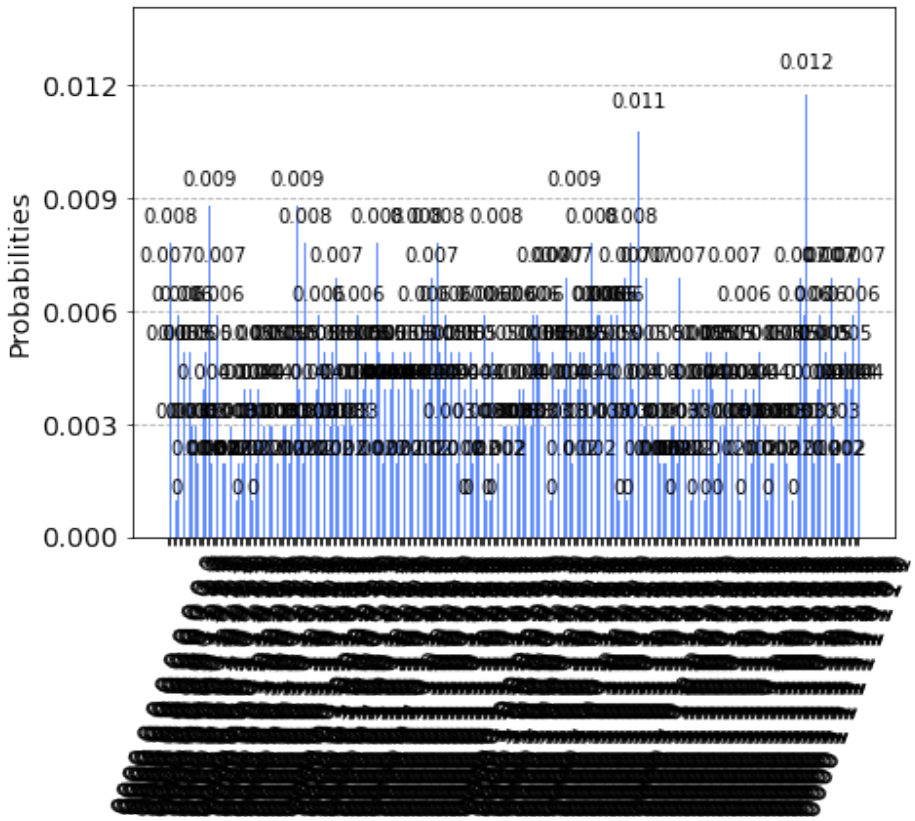
```
dj_circuit = QuantumCircuit(4+1, 4)

# Apply H-gates
for qubit in range(4):
    dj_circuit.h(qubit)

# Put qubit in state |->
dj_circuit.x(4)
dj_circuit.h(4)

# Add oracle
dj_circuit += balanced_oracle

# Repeat H-gates
for qubit in range(4):
    dj_circuit.h(qubit)
dj_circuit.barrier()

# Measure
for i in range(4):
    dj_circuit.measure(i, i)

# Display circuit
dj_circuit.draw()
```

شکل ۹ـ۱۷: مدار دوچ‌ـجوزا

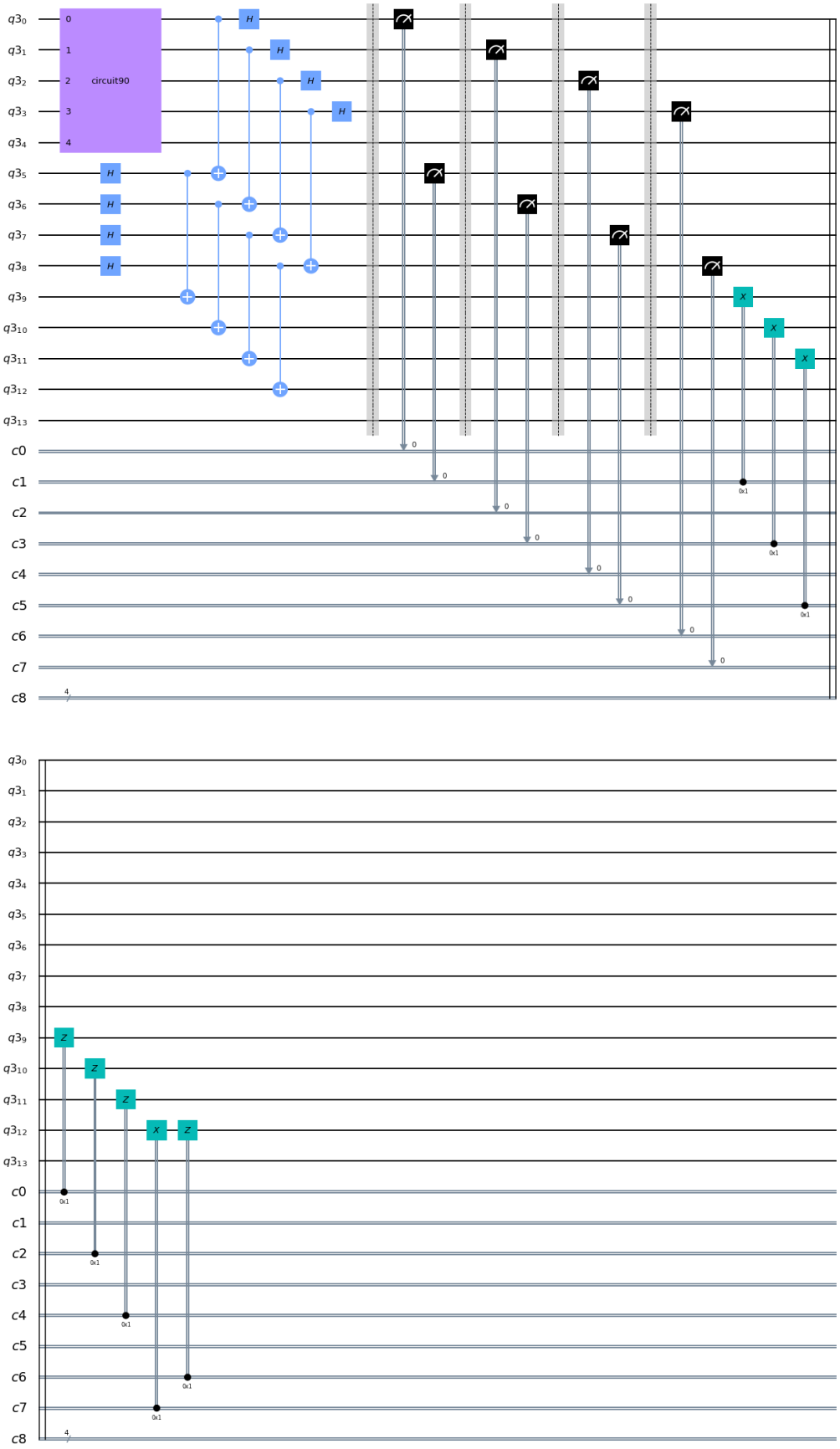




شکل ۹ـ۱۸: نتیجه اجرای چند باره الگوریتم دوچ جوزا. احتمال خروجی ۱۱۱۱ برابر با ۱۰۰% به‌دست آمده است.



شکل ۹ـ۱۹: نتیجه اجرای چندباره الگوریتم دوچ جوزا توزیع شده و ارتباط بین آلیس و باب با ورودی‌های متفاوت.



شکل ۹ـ۲۰: مدار نهایی استفاده شده توسط آلیس (بالا) و باب (پایین) در الگوریتم دوچ جوزا توزیع‌شده.

۱ـ پیوست: مبانی ریاضی مکانیک کوانتومی

دراین بخش با ریاضیات مورد نیاز برای فهم چارچوب نظری مکانیک کوانتومی آشنا می‌شویم. مطالب این بخش از [۵، ۸، ۱۲، ۱۷] اقتباس شده است.

۱ـ۱ فضای برداری

مجموعه V را یک فضای برداری روی میدان F می‌گوییم هرگاه دو عمل زیر تعریف شده

$$+ : V \times V \to V \quad , \quad . : F \times V \to V \tag{۱۰}$$

و دارای خواص زیر باشند:

$$\begin{aligned}
A_1 :&\quad x + y = y + x \\
A_2 :&\quad (x + y) + z = x + (y + z) \\
A_3 :&\quad \exists 0 \in V | 0 + x = x \\
A_4 :&\quad \forall x \in V | - x + x = 0 \\
M_1 :&\quad \alpha(x + y) = \alpha x + \alpha y \\
M_2 :&\quad (\alpha + \beta)x = \alpha x + \beta x \\
M_3 :&\quad \alpha(\beta x) = (\alpha\beta)x \\
M_4 :&\quad 1x = x
\end{aligned} \tag{۱۱}$$

بسته به این که F میدان اعداد حقیقی یا میدان اعداد مختلط باشد، فضای برداری V را فضای برداری مختلط یا حقیقی گوییم. ازاین به بعد منحصراً با فضاهای برداری مختلط کار می‌کنیم.

مثال ۱۰. مجموعه‌های زیر هرکدام یک فضای برداری هستند.

۱. R^n یا مجموعه nـتایی‌های مرتب حقیقی

۲. C^n یا مجموعه nـتایی‌های مرتب مختلط

۳. $M_{m\times n}(F)$ یا مجموعه ماتریس‌های $m \times n$ که درایه‌های آن عناصر یک میدان F هستند.

۴. $P_n([a, b])$ یا مجموعه چندجمله‌ای‌های حقیقی مرتبه n از متغیر x که در فاصله $[a, b]$ تعریف شده‌اند.

۵. $C^k[a, b]$ یا مجموعه توابع حقیقی یا مختلط k بار مشتق‌پذیر در بازه $[a, b]$.

تعریف ۹. هرگاه V یک فضای برداری و $W \subset V$ یک زیر مجموعه از آن باشد، آنگاه W را یک زیرفضای V گوییم اگر W نسبت به جمع بردارها و ضرب اعداد در بردارها بسته باشد.

۲ـ۱ـ ضرب داخلی و اندازه

تعریف: در یک فضای برداری V یک عمل دوتایی $\langle , \rangle : V \times V \to C$ را یک ضرب داخلی می‌نامیم هرگاه در شرایط زیر صدق کند:

$$\langle x, y + \alpha z \rangle = \langle x, y \rangle + \alpha \langle x, z \rangle \qquad (۱۲)$$

$$\langle x, y \rangle = \langle y, x \rangle^* \qquad (۱۳)$$

$$\langle x, x \rangle \geq 0 \qquad (۱۴)$$

$$\langle x, x \rangle = 0 \to x = 0 \qquad (۱۵)$$

فضایی را که به ضرب داخلی مجهز شده باشد یک فضای برداری ضرب داخلی می‌گوییم.

قضیه ۹. کوشی‌ـشوارتز: در فضای ضرب داخلی داریم:

$$|\langle x, y \rangle| = \langle x, x \rangle \langle y, y \rangle. \qquad (۱۶)$$

تعریف ۱۰. اندازه یک بردار: در هر فضای ضرب داخلی، می‌توان اندازه یک بردار را به شکل زیر تعریف کرد:

$$|x| := \sqrt{\langle x, x \rangle} \qquad (۱۷)$$

با توجه به نامساوی کوشی‌ـشوارتز می‌توان نوشت:

$$|\langle x, y \rangle| = |x||y| \qquad (۱۸)$$

تعریف ۱۱. فضای نرم یا اندازه‌دار: یک فضای برداری V که در آن نگاشت $\| \quad \| : V \to R$ تعریف شده باشد را فضای برداری اندازه‌دار[1] می‌گوییم هرگاه شرایط زیر برقرار باشد:

$$\|v\| \geq 0 \quad \forall v \tag{۱۹}$$

$$\|v\| = 0 \to v = 0 \tag{۲۰}$$

$$\|\alpha v\| = |a|\|v\| \tag{۲۱}$$

$$\|v + w\| \leq \|v\| + \|w\| \tag{۲۲}$$

هرفضای ضرب داخلی باهمان اندازه‌ای که از روی ضرب داخلی تعریف می‌شود یک فضای اندازه‌دار است، ولی یک فضای اندازه‌دار الزاماً یک فضای ضرب داخلی نیست. به عبارت دیگر، اندازه لزوما از روی ضرب داخلی تعریف نشده است. برای مثال، برای فضای توابع $C[a,b]$ نگاشت $\|f\| = sup_{x\in[a,b]}|f(x)|$ یک اندازه است که از روی ضرایب داخلی تعریف نشده است.

۱ـ۳ـ۱ پایه

پایه به‌هنجار[2] $\{e_i, i = 1, ..., N\}$ را برای فضای برداری V در نظر می‌گیریم. به‌هنجار بودن به معنای آن است که $\langle e_i, e_j\rangle = \delta_{ij}$. هر بردار $x \in V$ را می‌توان بر حسب این بردارهای پایه بسط داد و نوشت:

$$x = \sum_{i=1}^{N} x_i e_i \tag{۲۳}$$

بدیهی است که

$$x_i = \langle e_i, x\rangle \tag{۲۴}$$

پایه‌ها را می‌توان با یک ماتریس تبدیل پایه دو بعدی مانند S به یک دیگر تبدیل کرد. برای مثال، فرض کنید که بردار x را که در پایه e_i است را می‌خواهیم در پایه e_i' بنویسیم. لازم است درایه‌های ماتریسی آن را

[1] Normed Vector Space
[2] Normal

استخراج کنیم. در نظر بگیرید $e_i^{'} = S_{li}e_l$:

$$x_i^{'} = \langle e_i^{'}, x\rangle = \langle S_{li}e_l, x\rangle = S_{li}x_l \qquad (۲۵)$$

و یا به صورت فشرده‌تر:

$$x^{'} = xS. \qquad (۲۶)$$

از آنجا که پایه‌های $\{e_i\}$ و $\{e_i^{'}\}$ هر دو بهنجار هستند به راحتی نتیجه می‌گیریم که ماتریس تبدیل پایه S در شرط زیر صدق می‌کند:

$$S^{\dagger}S = I \qquad (۲۷)$$

چنین ماتریسی را ماتریس‌های یکانی[1] می‌گوییم.

که در آن $S^{\dagger}$ ماتریس الحاقی[2] S است و چنین تعریف می‌شود:

$$S^{\dagger} = (S^*)^T \quad or \quad S^{\dagger}_{ij} = (S^*)_{ji} \qquad (۲۸)$$

همچنین هرگاه ماتریس با الحاقی خود برابر باشد، آن را ماتریس هرمیتی می‌گوییم:

$$S^{\dagger} = S. \qquad (۲۹)$$

۴ـ۱ـ فضای کامل و هیلبرت

تعریف ۱۲. دنباله کوشی: در یک فضای برداری، دنباله‌ای از بردارها مانند $\{x_1, x_2, ..., x_n, ...\}$ درنظر می‌گیریم. این دنباله، یک دنباله کوشی نامیده می‌شود هر گاه فاصله بین بردارها به تدریج کم شود؛ به عبارت دقیق‌تر، هرگاه به ازای هر $\epsilon > 0$ عددی مانند N یافت شود که

$$\forall m, n > N \rightarrow |x_n - x_m| \leq \epsilon \qquad (۳۰)$$

در یک فضای برداری، لزوما حد کوشی در خود فضا قرار ندارد. مثلا، هرگاه میدان اعداد گویا را به عنوان یک فضای برداری روی خودش درنظر بگیریم، دنباله $\{(1 + \frac{1}{n})^n\}$ اگرچه یک دنباله کوشی است، ولی حد آن در میان اعداد گویا قرار ندارد. با افزودن اعداد گنگ به میدان، یک فضای برداری میدان حقیقی به دست می‌آید که کامل است.

[1] Unitary
[2] Conjugate Transpose

تعریف ۱۳. یک فضای برداری را فضای برداری کامل گوییم هرگاه حد دنباله کوشی را در خود داشته باشد.

تعریف ۱۴. یک فضای برداری با ضرب داخلی کامل را فضای هیلبرت[1] می‌نامیم. از آنجایی که میدان اعداد حقیقی و مختلط کامل است، می‌توان ثابت کرد هر فضا با بعد محدود روی این میدان‌ها هیلبرت است.

۵ـ۱ـ تبدیلات خطی

در یک فضای برداری V، نگاشت $\hat{T} : V \to V$ را یک تبدیل خطی یا یک عملگر خطی[2] می‌گوییم هرگاه داری خاصیت زیر باشد:

$$\hat{T}(x + \alpha y) = \hat{T}(x) + \alpha\hat{T}(y) \quad \forall \alpha \in F, x, y \in V \tag{۳۱}$$

ماتریس T با درایه‌های T_{mn} را ماتریس مربوط به تبدیل خطی $\hat{T}$ در پایه $\{e_i\}$ می‌گوییم. هرگاه پایه فوق به‌هنجار باشد، می‌توانیم بنویسیم

$$\langle e_j, \hat{T}e_i\rangle = T_{ji} \tag{۳۲}$$

تاثیر تابع $\hat{T}$ روی بردار x عبارت است از:

$$\hat{T}x = \hat{T}x_i e_i = x_i(\hat{T}e_i) = x_i T_{ji} e_j = (T_{ji}x_i)e_j = (Tx)_j e_j \tag{۳۳}$$

که برابر با ضرب از سمت چپ ماتریس T روی x است.

همچنین، با تعویض پایه، ماتریس تغییر می‌یابد:

$$T'_{ij} = \langle e'_i, \hat{T}e'_j\rangle = \langle S_{li}e_l, \hat{T}S_{mj}e_m\rangle = S^*_{li}T_{lm}S_{mj} \tag{۳۴}$$

که به صورت زیر قابل بازنویسی است:

$$T' = S^\dagger TS \tag{۳۵}$$

هرگاه A و B دو تبدیل خطی دلخواه روی V و α عددی دلخواه متعلق به میدان F باشد، آنگاه $\alpha A + B$ نیز یک تبدیل خطی روی V است. درنتیجه، مجموعه تبدیلات خطی روی V تشکیل یک فضای برداری می‌دهند که آن را با $End(V)$ نشان می‌دهیم. همچنین، ضرب دو تبدیل خطی با تعریف

$$(AB)x := A(Bx) \tag{۳۶}$$

[1] Hilbert Space
[2] Linear Operator

نیز یک تبدیل خطی است. پس می‌توان گفت که $End(V)$ نه تنها یک فضای برداری است بلکه یک جبر است که خاصیت شرکت پذیری دارد ($(AB)C = A(BC)S$) ولی جبر جابه‌جایی ندارد ($AB \neq BA$) اما یکه‌دار[1] است که یعنی عنصری دارد مانند I که $AI = IA = A$.

دیدیم که به یک عملگر خطی می‌توان یک ماتریس نسبت داد. وقتی که پایه فضا را معین می‌کنیم، بین فضای تبدیلات خطی یعنی $End(V)$ و فضای ماتریس‌های $M_{n\times n}(C)$ یک نگاشت یک به یک خواهیم داشت. بنابراین یک تبدیل خطی و ماتریس آن به جای هم قابل استفاده هستند. همچنین، با تبدیل زیر می‌توان فضای تبدیل خطی روی V را به یک فضای ضرب داخلی تبدیل کرد:

$$\langle A, B\rangle = tr(AB^{\dagger}) \qquad (۳۷)$$

که در آن رد[2] ماتریس $tr(A)$ برای ماتریس مربعی A برابر با مجموعه درایه‌های قطر اصلی است.

۱ـ۶ جمع نیمه‌مستقیم دو زیرفضا

تعریف ۱۵. هرگاه V یک فضای برداری و U و W دو زیرفضای آن باشند، $U + W$ را به عنوان مجموعه زیر تعریف می‌کنیم:

$$U + W := \{v|v = u + w, u \in U, w \in W\} \qquad (۳۸)$$

واضح است که $U + W$ نیز یک زیرفضا برای V است.

تعریف ۱۶. فرض کنید که V یک فضای برداری و W و U دو زیرفضای آن باشند به طوری که:

۱. $V = W + U$

۲. تنها بردار مشترک U و W بردار صفر باشد.

در این صورت V جمع نیمه‌مستقیم[3] U و W می‌گوییم و می‌نویسیم

$$V = U \oplus W \qquad (۳۹)$$

قضیه ۱۰. $V = W \oplus U$ اگر و تنها اگر هر بردار $v \in V$ را بتوان به صورت $u + w$ یکتایی نوشت که در آن $u \in U$ و $w \in W$.

قضیه ۱۱. اگر $V = U + W$ آنگاه $dim(V) = dim(U) + dim(W)$.

---

[1] Unital
[2] Trace
[3] Semi-direct Sum

تعریف ۱۷. فرض کنید که $V = V_1 \oplus V_2 \oplus ... \oplus V_r$. در این صورت، هر بردار $v \in V$ به صورت یکتای $v = v_1 + v_2 + ... + v_r$ تجزیه می‌شود. P_j را عملگری تعریف کنید که:

$$P_j v = v_j \tag{۴۰}$$

در این صورت، P_j را عملگر تصویر روی زیرفضای V_j می‌خوانیم.

قضیه ۱۲. عملگرهای تصویری[1] خواص زیر را دارند:

۱. $P_j P_k = \delta_{jk} P_j$

۲. $\sum_{j=1}^{r} P_j = I$

قضیه ۱۳. هرگاه V یک فضای ضرب داخلی باشد و $V = \bigoplus_{j=1}^{r} V_j$ که در آن V_jها بر هم عمود هستند، آنگاه عملگرهای P_j هرمیتی[2] هستند.

۱ـ۷ مساله ویژه‌مقدار

عملگر $T : V \to V$ را درنظر می‌گیریم. مساله ویژه‌مقدار[3] عبارت است از یافتن بردارهای غیرصفری که تحت اثر T به مضربی از خود تبدیل بشوند:

$$Tx = \lambda x \tag{۴۱}$$

بردار x غیرصفر خواهد بود هرگاه ماتریس $T - \lambda I$ وارون‌پذیر نباشد، یعنی این‌که

$$det(T - \lambda I) = 0 \tag{۴۲}$$

این معادله، یک معادله درجه N است که در حوزه اعداد مختلط حتما N جواب مانند $\{\lambda_i, i = 1, ..., N\}$ دارد که به آن‌ها ویژه‌مقدارهای تبدیل T گوییم. این جواب‌ها لزوما با هم متفاوت نیستند.

بردار مربوط به λ_i که در معادله $Tv_i = \lambda_i v_i$ صدق می‌کند را ویژه‌بردار[4] متناظر با آن ویژه‌مقدار می‌خوانیم. هرگاه x و y ویژه‌بردارهای مربوط به λ باشند، بدیهی است که هر ترکیب خطی از آن‌ها هم ویژه‌برداری از λ است. بنابراین، مجموعه بردارهای متعلق به یک ویژه‌مقدار تشکیل یک زیرفضا را می‌دهند که به آن ویژه‌فضای[5] آن ویژه‌مقدار می‌گویند.

---
[1] Image Operators
[2] Hermitian
[3] Eigenvalue
[4] Eigenvector
[5] Eigenspace

۸ـ۱ـ عملگرهای هرمیتی، یکانی و به‌هنجار

تعریف ۱۸. در یک فضای ضرب داخلی، الحاقی یک عملگر T عملگری مانند $T^\dagger$ است که در شرط زیر صدق کند:

$$\langle v, Tw\rangle = \langle T^\dagger v, w\rangle \qquad (۴۳)$$

با استفاده از این تعریف می‌توان به راحتی خواص زیر را ثابت کرد:

۱. الحاقی یک عملگر خطی خود نیز یک عملگر خطی است.

۲. $(cA+B)^\dagger = c^* A^\dagger + B^\dagger$

۳. $AB)^\dagger = B^\dagger A^\dagger$

۴. $(A^\dagger)^\dagger = A$

تعریف ۱۹. در یک فضای ضرب داخلی عملگر هرمیتی به عملگری گفته می‌شود که در شرط $T^\dagger = T$ صدق کند. عملگر پادهرمیتی به عملگری گفته می‌شود که در شرط $T^\dagger = -T$ صدق کند.

تعریف ۲۰. در یک فضای ضرب داخلی، عملگر یکانی U به عملگری گفته می‌شود که ضرب داخلی بردارها رو حفظ کند، یعنی

$$\langle Uv, Uw\rangle = \langle v, w\rangle \qquad (۴۴)$$

چنین عملگری در شرط $UU^\dagger = U^\dagger U$ صدق می‌کند.

تعریف ۲۱. عملگر نرمال یا به‌هنجار عملگری است که با الحاقی خود جابه‌حا شود. عملگرهای هرمیتی و یکانی نرمال هستند.

$$AA^\dagger = A^\dagger A \qquad (۴۵)$$

قضیه ۱۴. فرض کنید که A یک عملگر به‌هنجار است. در این صورت اگر $Ax = \lambda x$ آنگاه $A^\dagger x = \lambda^* x$.

نتیجه: ویژه‌مقادیر یک عملگر هرمیتی حقیقی هستند.

قضیه ۱۵. ویژه‌بردارهای متناظر با ویژه‌مقدارهای متمایز یک عملگر به‌هنجار بر هم عمودند.

تعریف ۲۲. عملگر مثبت نیمه معین[1] عملگری است که

$$\forall v \in V : \quad \langle x, Tx \rangle \geq 0 \tag{۴۶}$$

همچنین عملگر مثبت معین[2] عملگری است که

$$\forall v \in V : \quad \langle x, Tx \rangle > 0 \tag{۴۷}$$

اگر $f : \mathbb{R} \to \mathbb{R}$ یک تابع و $A : \mathcal{H} \to \mathcal{H}$ عملگری هرمیتی و به صورت زیر باشد:

$$A = \sum_{i=0}^{d-1} \lambda_i \, |v_i\rangle\langle v_i| \tag{۴۸}$$

آنگاه تعریف می‌کنیم:

$$f(A) := \sum_{i=0}^{d-1} f(\lambda_i) \, |v_i\rangle\langle v_i| \tag{۴۹}$$

توجه کنید که ویژه‌مقادیر $f(A)$ برابر با $f(\lambda_i)$ها هستند که λ_iها ویژه‌مقادیر A هستند.

۹ـ۱ـ نمادگذاری دیراک

یک فضای برداری V با بعد N با پایه‌های به‌هنجار $\{e_1, e_2, e_3, ..., e_N\}$ درنظر می‌گیریم. هر بردار $v \in V$ بسطی از بردارهای پایه به شکل زیر است:

$$v = \sum_{i=1}^{N} v_i e_i \tag{۵۰}$$

ضرب داخلی این بردار در خودش به صورت زیر نوشته می‌شود:

$$\langle v, v \rangle = \sum_{i=1}^{N} v_i^* v_i \tag{۵۱}$$

می‌توان به ازای چنین برداری، یک بردار ستونی با نماد $|v\rangle$ و یک بردار سطری با نماد $\langle v|$ به شکل زیر تعریف کرد:

$$|v\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_N \end{pmatrix} \tag{۵۲}$$

$$\langle v| = \begin{pmatrix} v_1^* & v_2^* & \cdots & v_N^* \end{pmatrix} \tag{۵۳}$$

[1] Positive Semidefinite
[2] Definite Positive

بردار $\langle v|$ را یک بردار bra و بردار $|v\rangle$ یک بردار ket می‌نامیم. توجه کنیم که می‌توانیم این دو بردار را در هم ضرب کنیم:

$$\langle v|v\rangle = \sum_{i=1}^{N} v_i^* v_i = \langle v, v\rangle \qquad (۵۴)$$

بردارهای پایه $e_1, ..., e_N$ نیز شکل زیر را پیدا می‌کنند:

$$|N\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \quad |2\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\langle 1| = (1 \quad 0 \quad \cdots \quad 0)$$

$$\langle 2| = (0 \quad 1 \quad \cdots \quad 0)$$

$$\langle N| = (0 \quad 0 \quad \cdots \quad 1)$$

بنابراین داریم

$$|v\rangle = \sum_{i=1}^{N} v_i |i\rangle \qquad (۵۵)$$

$$\langle v| = \sum_{i=1}^{N} v_i^* \langle i| \qquad (۵۶)$$

از این به بعد تمامی بردارها را با این نمادگذاری نشان می‌دهیم.

خواص زیر برای این نمادگذاری وجود دارد:

۱. $\langle v|w\rangle = \langle v, w\rangle$

۲. $\langle v|w + w'\rangle = \langle v|w\rangle + \langle v|w'\rangle$

۳. $\langle v|cw\rangle = c\langle v|w\rangle$

۴. $\langle cv|w\rangle = c^*\langle v|w\rangle$

۵. $\langle v|v\rangle \geq 0$

۶. $\langle v|v\rangle = 0 \rightarrow |v\rangle = \langle v| = 0$

۷. $|v\rangle = \sum_{i=1}^{N} v_i |i\rangle$

۸. $\langle i|v\rangle = v_i$

۹. $$|v\rangle \langle w| := \begin{pmatrix} v_1 w_1^* & v_1 w_2^* & v_1 w_3^* & \cdots & v_1 w_n^* \\ v_2 w_1^* & v_2 w_2^* & v_2 w_3^* & \cdots & v_2 w_n^* \\ v_3 w_1^* & v_3 w_2^* & v_3 w_3^* & \cdots & v_3 w_n^* \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_N w_1^* & v_N w_2^* & v_N w_3^* & \cdots & v_N w_n^* \end{pmatrix}$$

۱۰. $|v\rangle \left\langle w + w' \right| = |v\rangle \langle w| + |v\rangle \left\langle w' \right|$

۱۱. $|v\rangle \langle cw| = c^* |v\rangle \langle w|$

۱۲. $|cv\rangle \langle w| = c |v\rangle \langle w|$

۱۳. $\langle i|j\rangle = \delta_{ij}$

۱۴. $\sum_i |i\rangle \langle i| = I$

۱۵. $|v\rangle = I |v\rangle = \sum_{i=1}^{N} |i\rangle \langle i|v\rangle = \sum_{i=1}^{N} v_i |i\rangle$

۱۶. $T = \sum_j |j\rangle \langle i| T \sum_i |i\rangle \langle i| = \sum_{i,j} T_{ji} |j\rangle \langle i|$

۱۷. $\langle i|AB|j\rangle = \sum_k \langle i|AB|k\rangle \langle k|AB|j\rangle$

۱۰ـ۱ـ ضرب تنسوری

هرگاه $(A)_{m\times n}$ و $(B)_{p\times q}$ دو ماتریس با ابعاد داده شده باشند، می‌توان ضرب تنسوری[1] آن‌ها را که ماتریسی با ابعاد $mp \times nq$ است را به شکل زیر تعریف کرد

$$(A \otimes B)_{ij,kl} := A_{ik} B_{jl} \qquad (۵۷)$$

به لحاظ عملی ضرب این دو ماتریس به شکل زیر محاسبه می‌شود:

$$A \otimes B := \begin{pmatrix} a_{11}B & a_{12}B & a_{13}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & a_{23}B & \cdots & a_{2n}B \\ a_{31}B & a_{32}B & a_{33}B & \cdots & a_{3n}B \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & a_{m3}B & \cdots & a_{mn}B \end{pmatrix} \qquad (۵۸)$$

[1] Tensor Product

ضرب تنسوری خواص زیر را دارد:

۱. $A \otimes (B + C) = A \otimes B + A \otimes C$

۲. $A \otimes (\alpha B) = (\alpha A) \otimes B = \alpha(A \otimes B)$

۳. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$

۴. $(A \otimes B)(C \otimes D) = AC \otimes BD$

۵. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

حال اگر فضای برداری V با بردارهای پایه $\{|i\rangle, i = 1, ..., m\}$ و فضای برداری W با بردارهای پایه $\{|\mu\rangle, \mu = 1, ..., m\}$ را درنظر بگیریم، می‌توان ضرب تنسوری بردارهای پایه را مطابق با تعریف بالا به دست آوریم. به ترتیب بردار پایه به شکل $|i\rangle \otimes |\mu\rangle$ به دست می‌آوریم که آن‌ها را به اختصار با $|i, \mu\rangle$ نشان می‌دهیم. این بردارهای جدید یک فضای برداری جدید را جاروب[1] می‌کنند که با بعد mn است که آن را فضای برداری ضرب تنسوری W و V می‌خوانیم.

نکته آخر این است که یک بردار دلخواه در فضای $V \otimes W$ را نمی‌توان به صورت ضرب‌های $|v\rangle \otimes |w\rangle$ نوشت؛ مثل بردار زیر

$$|\psi\rangle := |0, 0\rangle + |1, 1\rangle \qquad (۵۹)$$

این نکته ما را دعوت می‌کند که در مورد خاصیت درهم‌تنیدگی در مکانیک کوانتومی بیشتر بررسی کنیم.

[1] Span

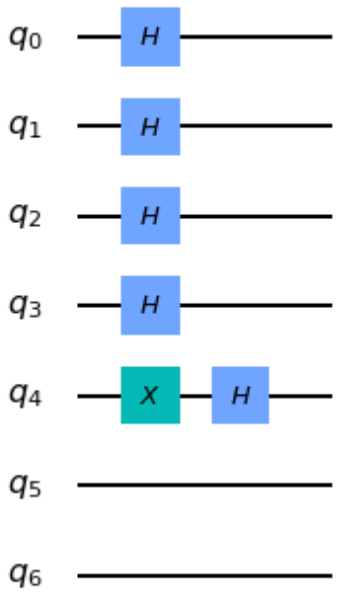
۲ـ پیوست دوم: بررسی دقیق کد دوچ جوزا توزیع‌شده

از آنجایی که نحوه عملکرد قطعه‌های این کد در الگوریتم‌های قبلی بیان‌شده اند، در این قسمت فقط با اضافه کردن مرحله به مرحله گیت‌ها، مدار حاصل را نمایش می‌دهیم.

[73]:
```
def dj_oracle(b_str):
    oracle_qc = QuantumCircuit(len(b_str)+1)
    for qubit in range(len(b_str)):
        if b_str[qubit] == '1':
            oracle_qc.x(qubit)

    for qubit in range(len(b_str)):
        oracle_qc.cx(qubit, len(b_str))

    for qubit in range(len(b_str)):
        if b_str[qubit] == '1':
            oracle_qc.x(qubit)

    return oracle_qc
```

[93]:
```
alice_start = QuantumCircuit(4+1+2, name="test")
alice_start.x(4)
alice_start.h(4)
for qubit in range(4):
    alice_start.h(qubit)
# oracle_alice = dj_oracle('0101')
# alice_start.append(tto.circuit, range(4+1+2))
alice_start.draw(output='mpl')
```

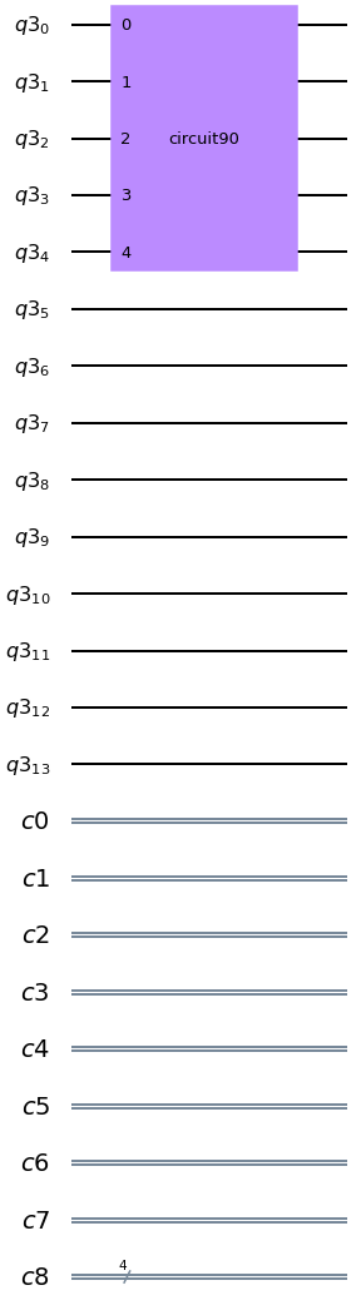
[93]:



[60]:
```
alice_bob_tele_qr = QuantumRegister(4+1+4+4+1)
c11,c12,c21,c22,c31,c32,c41,c42,c_m = ClassicalRegister(1),␣
 ↪ClassicalRegister(1), ClassicalRegister(1), ClassicalRegister(1),␣
 ↪ClassicalRegister(1), ClassicalRegister(1), ClassicalRegister(1),␣
 ↪ClassicalRegister(1), ClassicalRegister(4)
alice_bob_tele =␣
 ↪QuantumCircuit(alice_bob_tele_qr,c11,c12,c21,c22,c31,c32,c41,c42,c_m)
alice_bob_tele.draw()
```

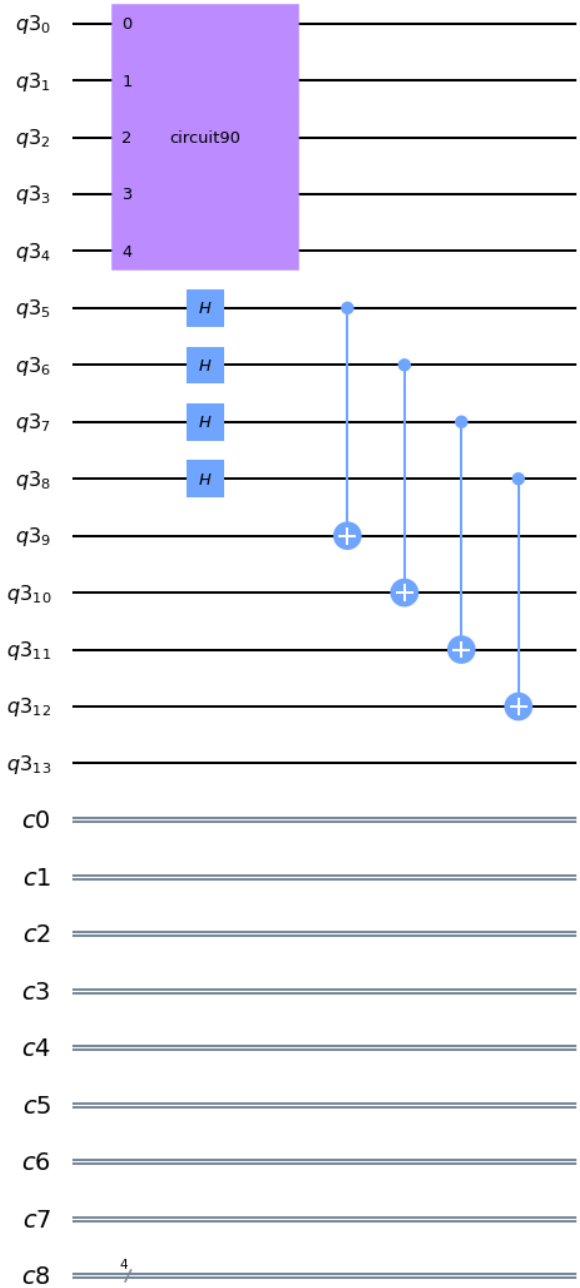
[61]:
```
alice_bob_tele.append(alice_start,range(4+1))
alice_bob_tele.draw()
```

[61]:



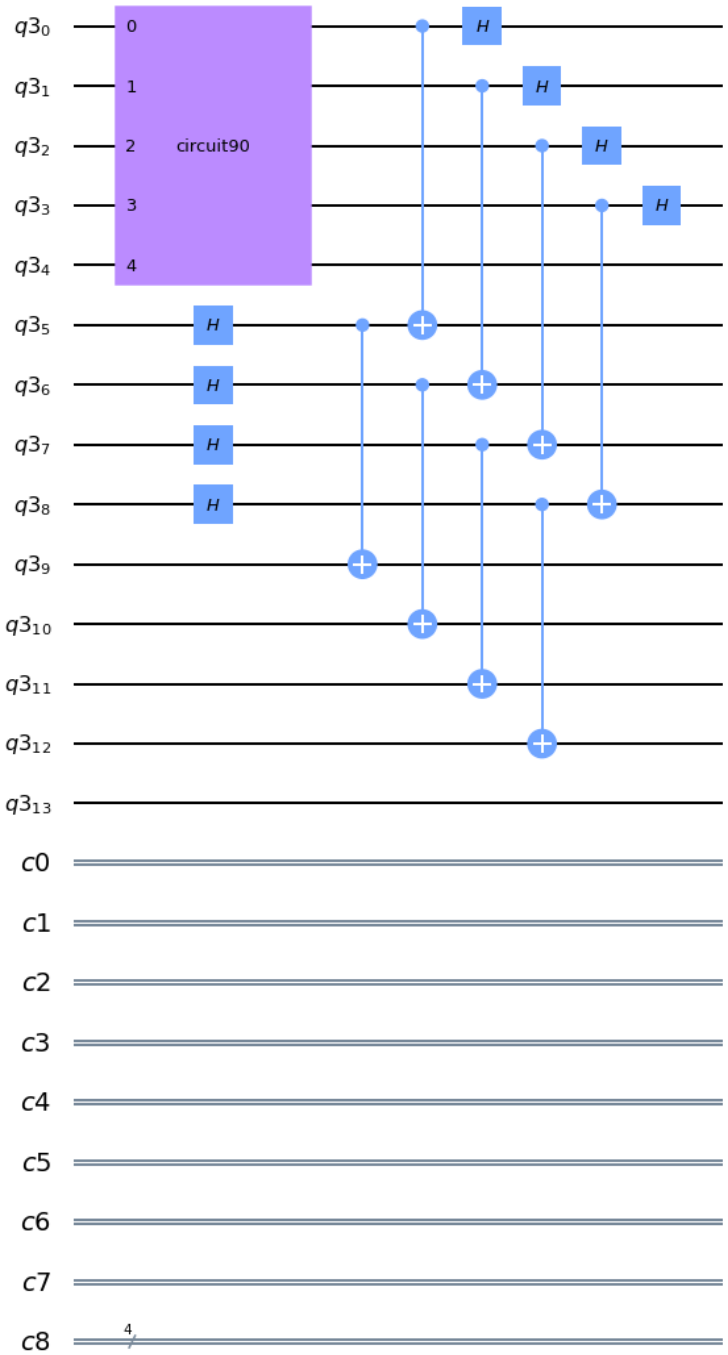
[62]:
```
def create_bell_pair(qc, a, b):
    qc.h(a) # Put qubit a into state |+>
    qc.cx(a,b) # CNOT with a as control and b as target
create_bell_pair(alice_bob_tele, 5, 9)
create_bell_pair(alice_bob_tele, 6, 10)
create_bell_pair(alice_bob_tele, 7, 11)
create_bell_pair(alice_bob_tele, 8, 12)
alice_bob_tele.draw()
```

[62]:



[63]:
```
def alice_gates(qc, psi, a):
    qc.cx(psi, a)
    qc.h(psi)
alice_gates(alice_bob_tele, 0, 5)
alice_gates(alice_bob_tele, 1, 6)
alice_gates(alice_bob_tele, 2, 7)
alice_gates(alice_bob_tele, 3, 8)
alice_bob_tele.draw()
```

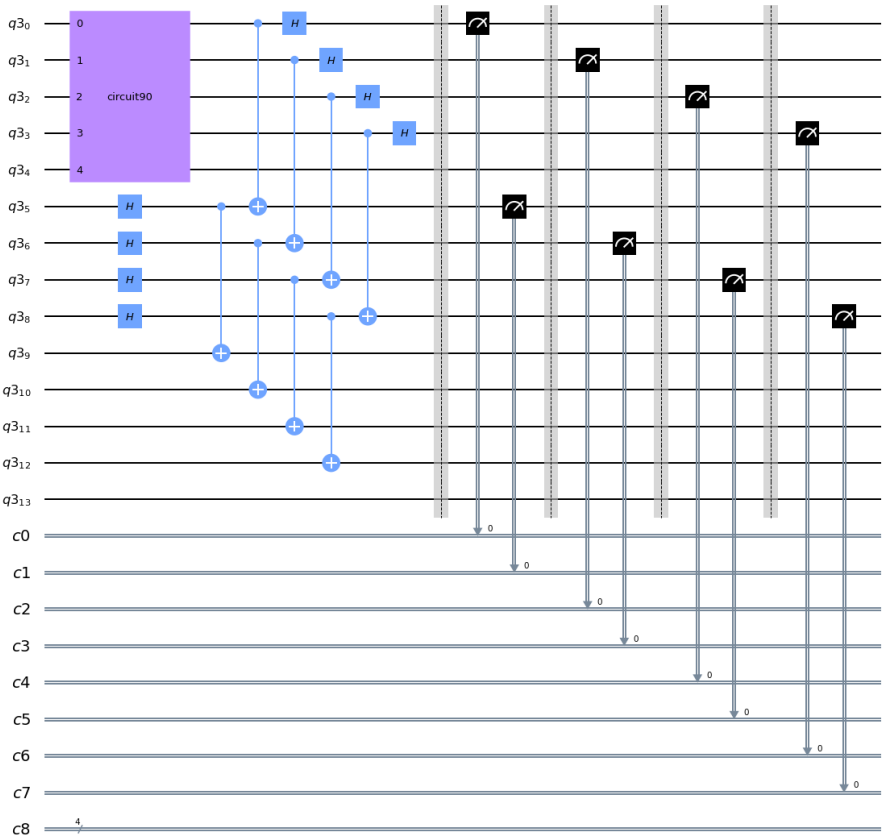
[63]:



[64]:
```
def measure_and_send(qc, psi, a, c1, c2):
    qc.barrier()
    qc.measure(psi,c1)
    qc.measure(a,c2)
measure_and_send(alice_bob_tele,0,5,0,1)
measure_and_send(alice_bob_tele,1,6,2,3)
measure_and_send(alice_bob_tele,2,7,4,5)
measure_and_send(alice_bob_tele,3,8,6,7)
```

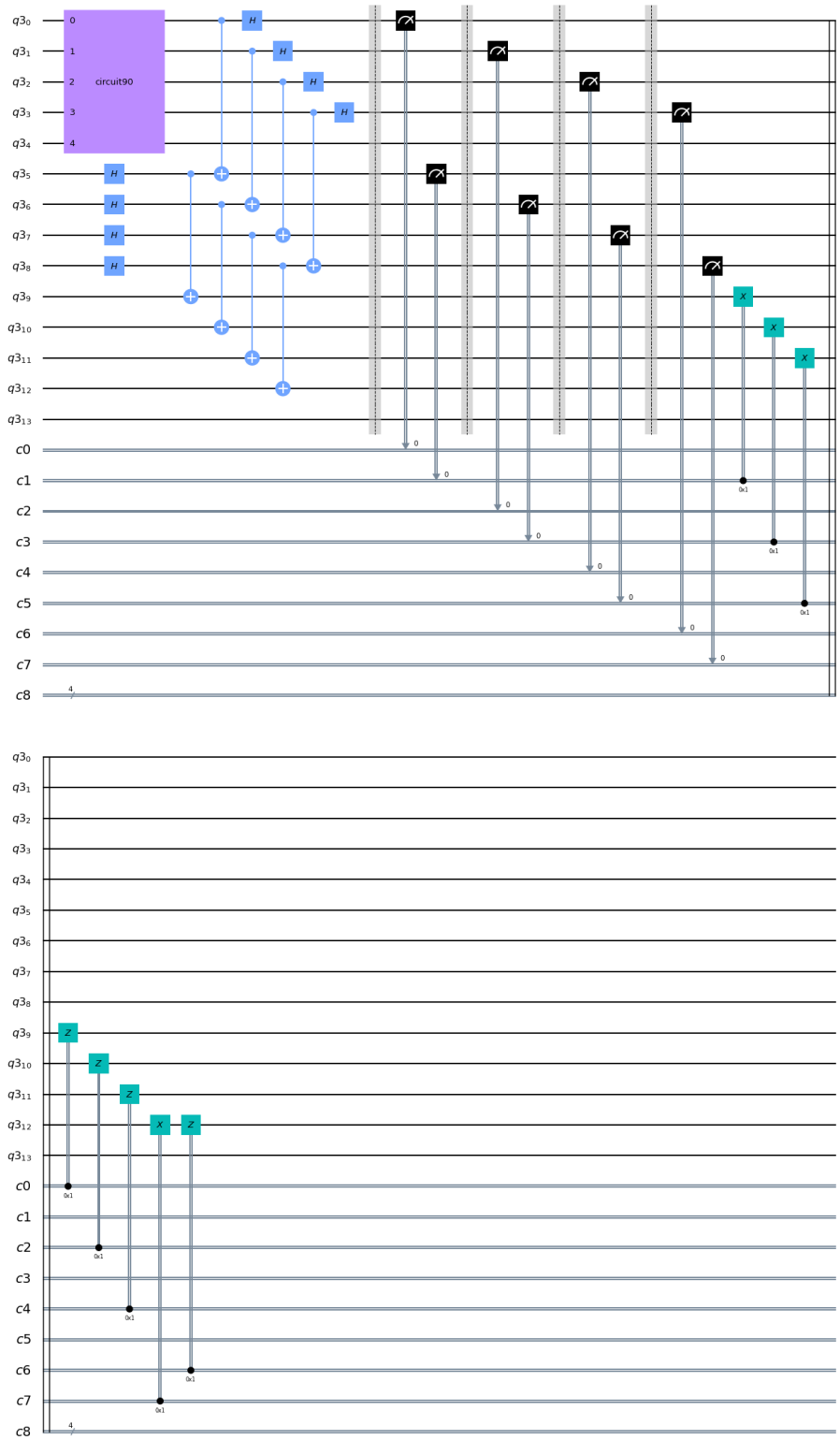
[65]:
```
alice_bob_tele.draw()
```

[65]:



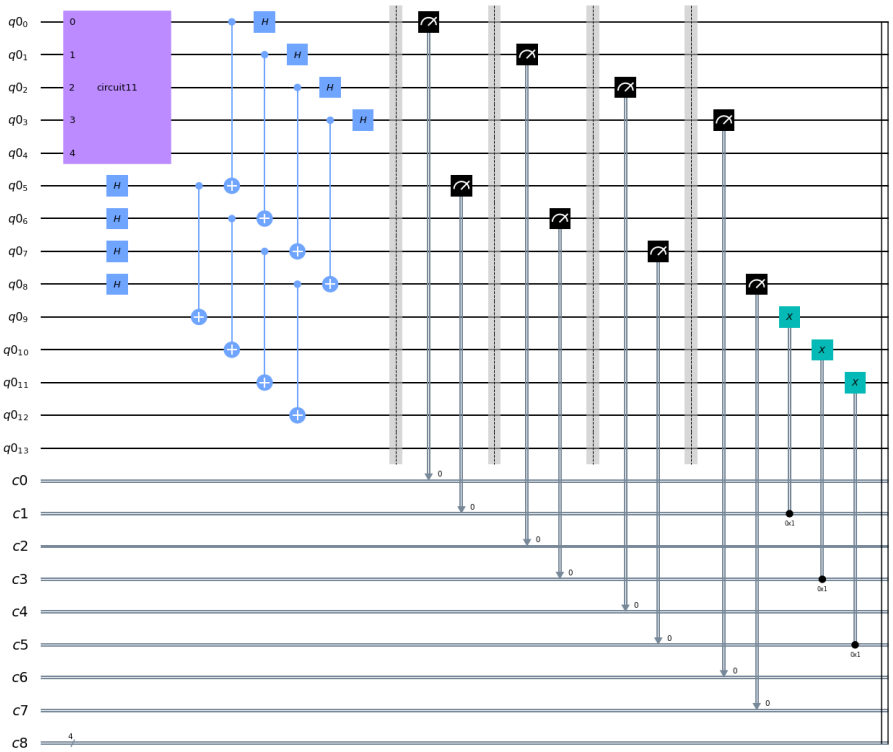
[66]:
```
def bob_gates(qc, qubit, crz, crx):
    qc.x(qubit).c_if(crx, 1) # Apply gates if the registers
    qc.z(qubit).c_if(crz, 1) # are in the state '1'
bob_gates(alice_bob_tele, 9, c11, c12)
bob_gates(alice_bob_tele, 10, c21, c22)
bob_gates(alice_bob_tele, 11, c31, c32)
bob_gates(alice_bob_tele, 12, c41, c42)
alice_bob_tele.draw()
```

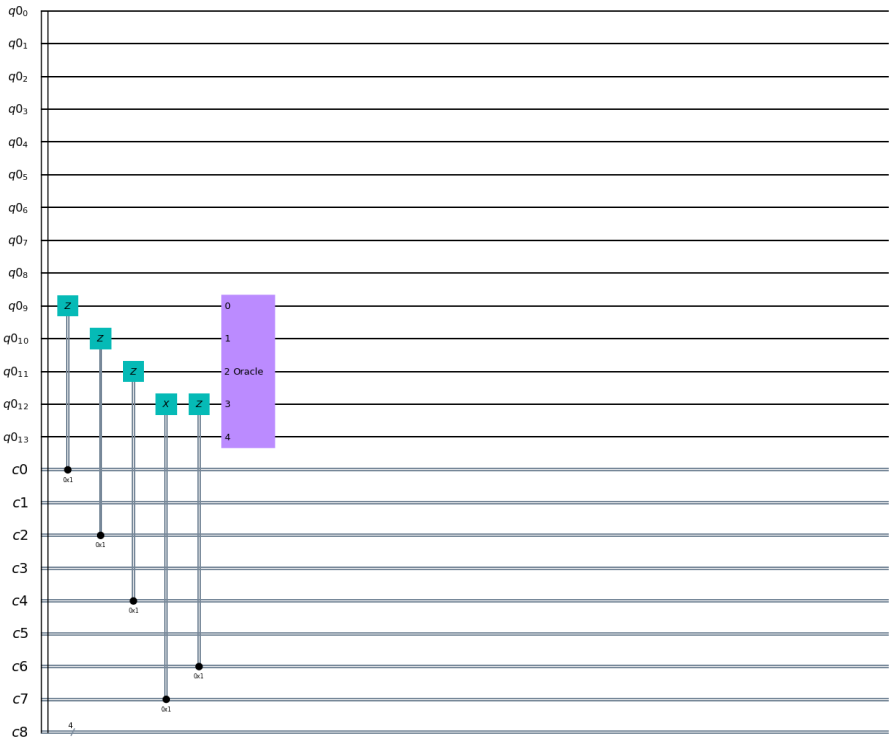
[66]:



[16]:
```
bob_oracle = dj_oracle('0101')
alice_bob_tele.append(bob_oracle, [9,10,11,12,13])
alice_bob_tele.draw()
```

[16]:

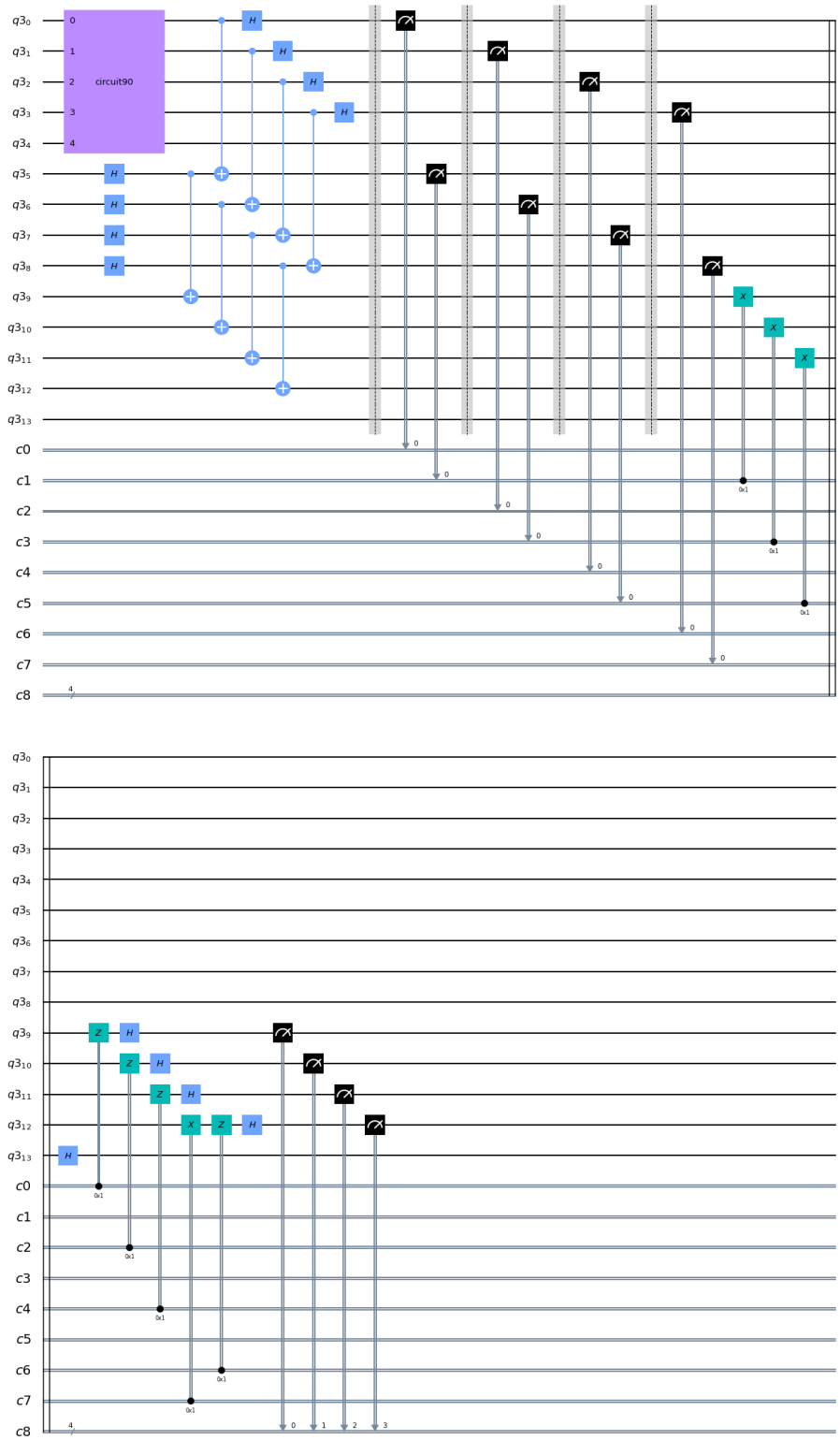




[67]:
```
for qubit in [9,10,11,12,13]:
        alice_bob_tele.h(qubit)

alice_bob_tele.measure(9, 8)
alice_bob_tele.measure(10, 9)
```

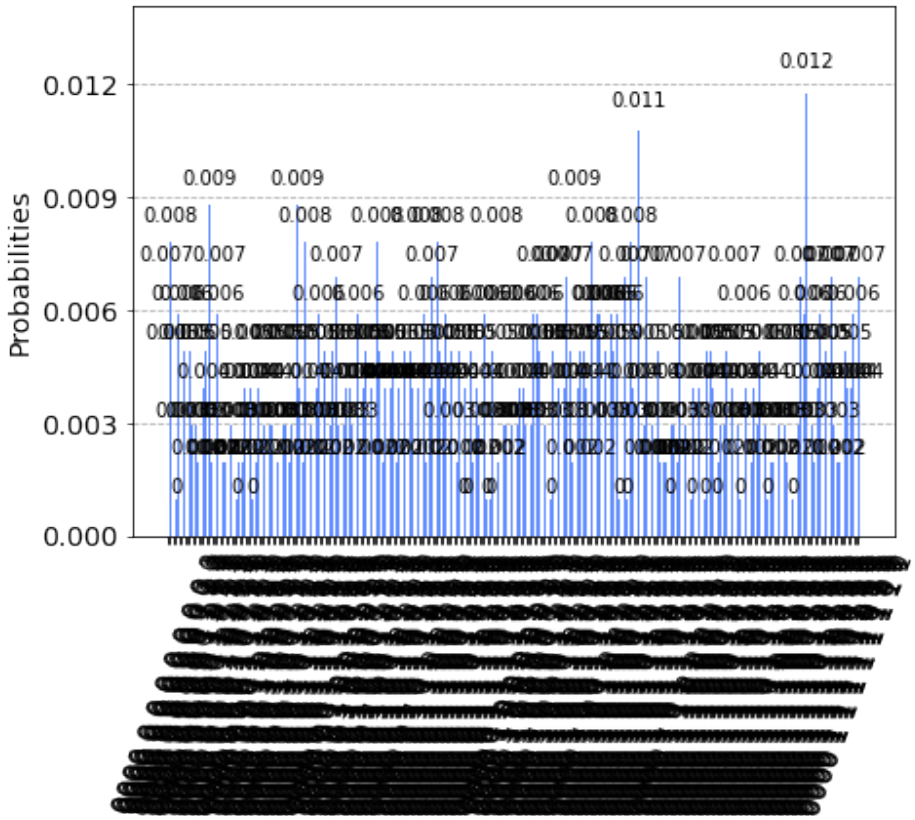
```
alice_bob_tele.measure(11, 10)
alice_bob_tele.measure(12, 11)

alice_bob_tele.draw()
```

[67]:



[108]:
```
backend = BasicAer.get_backend('qasm_simulator')
shots = 1024
results = execute(alice_bob_tele, backend=backend, shots=1024).
 ↪result()
answer = results.get_counts()
plot_histogram(answer)
```

[108]:



References

[1] Abraham, H., et al. Qiskit: An open-source framework for quantum computing, 2019.

[2] Babai, L., Frankl, P., and Simon, J. Complexity classes in communication complexity theory, 1986. Available at link.

[3] Brassard, G. Quantum communication complexity, 2001.

[4] Chattopadhyay, A., Radhakrishnan, J., and Rudra, A. Topology matters in communication, 2014. Available at link.

[5] Chuang, I. Quantum information science, 2006. Available at link.

[6] Cleve, R., and Buhrman, H. Substituting quantum entanglement for communication, 1997. Available at link.

[7] Cleve, R., Buhrman, H., and Wigderson, A. Quantum vs. classical communication and computation, 1998. Available at link.

[8] de Wolf, R. Quantum computing: Lecture notes, 2019.

[9] Holevo, A. Bounds for the quantity of information transmitted by a quantum communication channel, 1973.

[10] Kushilevitz, E., and Nisan, N. Communication complexity, 2009. Available at .

[11] Lee, T., and Shraibman, A. Lower bounds in communication complexity, 2009.

[12] Nielsen, M. A., and Chuang, I. L. Quantum computation and quantum information:, 2010.

[13] Phillips, J. M., Verbin, E., and Zhang, Q. Lower bounds for number-in-hand multiparty communication complexity, made easy, 2011. Available at link.

[14] Pitassi, T. Lecture notes in communication complexity: Applications and new directions, 2014. Available at link.

[15] Roughgarden, T. Communication complexity (for algorithm designers), 2015. Available at link.

[16] Sherstov, A. Lecture notes in communication complexity:, 2018. Available at link.

[17] Strang, G. 18.06sc linear algebra, Fall 2011. Available at link.

[18] Yao, A. C.-C. Quantum circuit complexity, 1993. Available at link.