

بسم الله الرحمن الرحيم



دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

بررسی کمینه‌ها در مسائل پیچیدگی ارتباطی کوانتومی در حوزه ساختمان داده‌ها

گزارش پروژه

نگار سخایی

اساتید راهنما

دکتر مریم موزرانی

دکتر رامین جوادی

۵ شهریور ۱۳۹۹

فهرست مطالب

صفحه	عنوان
چهار	فهرست مطالب
۱	فصل اول : مقدمه
۳	فصل دوم : پیچیدگی ارتباطی
۳	۱-۲ تعریف
۴	۲-۲ تکنیک‌های کمینه‌یابی
۵	۱-۲-۲ ماتریس مشخصه
۵	۲-۲-۲ پروتکل، درخت و مستطیل‌ها
۵	۳-۲-۲ قطعه بندی
۷	۴-۲-۲ مجموعه گول‌زننده
۸	۵-۲-۲ کران اندازه مستطیل
۹	۶-۲-۲ کمینه رتبه ماتریس
۱۰	فصل سوم : پیچیدگی ارتباطی غیرقطعی
۱۱	۱-۳ پوشش‌ها
۱۲	۲-۳ کلاس‌های پیچیدگی
۱۲	۳-۳ تکنیک‌های کمینه‌یابی
۱۳	۴-۳ نتیجه‌گیری
۱۴	فصل چهارم : پیچیدگی ارتباطی تصادفی
۱۴	۱-۴ مدل سکه خصوصی
۱۵	۲-۴ مدل سکه عمومی
۱۷	۳-۴ مدل توزیعی
۱۷	۴-۴ کمینه‌یابی
۱۷	۱-۴-۴ ناهمگنی
۱۸	۲-۴-۴ محدودکردن مقیاس ناهمگنی و کمینه‌یابی
۱۹	فصل پنجم : کاربرد پیچیدگی ارتباطی در ساختمان داده‌ها
۱۹	۱-۵ مدل جست‌وجوی سلول

۲۰	پیچیدگی ارتباطی نامتقارن
۲۲	کمین
۲۲	۱-۳-۵ تکنیک پیچیدگی ارتباطی حریصانه

۲۵	فصل ششم: مکانیک کوانتومی
۲۵	۱-۶ مقدمه‌ای در مورد مشاهده و اندازه‌گیری
۲۶	۲-۶ معنای حالت
۲۷	۳-۶ تداخل
۳۲	۴-۶ معادله شرودینگر
۳۲	۱-۴-۶ مکانیک همیلتونی
۳۳	۵-۶ اصول مکانیک کوانتومی
۳۳	۱-۵-۶ اصل اول - فضای حالات
۳۳	۲-۵-۶ اصل دوم - تحول زمانی
۳۵	۳-۵-۶ اصل سوم - اندازه‌گیری
۳۶	۴-۵-۶ اصل چهارم - سیستم‌های ترکیبی
۳۶	۶-۶ درهم‌تنیدگی
۳۷	۷-۶ اختتامیه‌ای بر عجایب مکانیک کوانتومی
۳۹	۸-۶ قضایای عدم امکان در مکانیک کوانتومی
۳۹	۱-۸-۶ تکثیر حالت‌های کوانتومی

۴۱	فصل هفتم: محاسبات و الگوریتم‌های کوانتومی
۴۱	۱-۰-۷ محدودیت‌های رایانش کلاسیک
۴۳	۱-۷ مبادله کوانتومی اطلاعات
۴۴	۲-۷ شبیه‌سازی کوانتومی
۴۶	۳-۷ فرابرد کوانتومی
۴۸	۴-۷ کدگذاری چگال
۴۹	۵-۷ الگوریتم‌های کوانتومی
۴۹	۱-۵-۷ کیوبیت
۵۰	۲-۵-۷ توازی کوانتومی
۵۰	۳-۵-۷ گیت کوانتومی
۵۱	۴-۵-۷ روند یک الگوریتم کوانتومی
۵۱	۶-۷ الگوریتم دوچ-جوزا
۵۱	۱-۶-۷ سوال پرسیدن کوانتومی
۵۲	۲-۶-۷ تبدیل فوری روی گروه Z_2^n
۵۳	۳-۶-۷ الگوریتم اصلی
۵۴	۷-۷ الگوریتم جست‌وجوی گرور

۵۴	مساله ۱-۷-۷
۵۴	مقدمه ۸-۷
۵۶	الگوریتم اصلی ۹-۷
۵۸		فصل هشتم: پیچیدگی ارتباطی کوانتومی
۵۹	یک سوال کوانتومی ۱-۸
۶۰	الگوریتم دوچ-جوزا: توزیع شده ۲-۸
۶۱	مساله اشتراک ۱-۲-۸
۶۱	مساله اشتراک ۲-۲-۸
۶۲		فصل نهم: شبیه‌سازی الگوریتم‌ها و پروتکل‌های کوانتومی
۶۲	مدار کوانتومی ۱-۹
۶۳	اندازه‌گیری ۱-۱-۹
۶۴	مدار جمع‌کننده ۲-۱-۹
۶۶	فرابرد کوانتومی ۲-۹
۶۷	الگوریتم دوچ-جوزا ۳-۹
۷۳	پیوست: مبانی ریاضی مکانیک کوانتومی ۱-
۷۳	فضای برداری ۱-۱-
۷۴	ضرب داخلی و اندازه ۲-۱-
۷۵	پایه ۳-۱-
۷۶	فضای کامل و هیلبرت ۴-۱-
۷۷	تبدیلات خطی ۵-۱-
۷۸	جمع نیمه‌مستقیم دو زیرفضا ۶-۱-
۷۹	مساله ویژه مقدار ۷-۱-
۸۰	عملگرهای هرمیتی، یکانی و به‌هنگار ۸-۱-
۸۱	نمادگذاری دیراک ۹-۱-
۸۳	ضرب تنسوری ۱۰-۱-
۸۵	مراجع

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 - مانند الگوریتم شور^۱ برای به‌دست آوردن عوامل اول یک عدد دلخواه در زمان بهینه - 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

¹Shore

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 - پیچیدگی قطعی، غیرقطعی و تصادفی - می‌پردازند. سپس در فصل پنجم، کاربرد خاصی از آن‌ها در حالت کلاسیک مطرح شده و نتایج 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 توزیع شده^۱ حل کند. منظور از حل به صورت توزیع شده 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.

۲-۱ 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.

¹Distributed

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 $A_v : X \rightarrow \{0, 1\}$ 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 $B_v : X \rightarrow \{0, 1\}$ 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 بفروشد و این حداکثر مکالمه مورد نیاز بین دو طرف است، برای یک تابع $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ ، $D(f) \leq n + 1$ است. نکته قابل توجه این است که همواره می‌توان یک درخت پروتکل را متوازن کرد. به عبارت دیگر، یک درخت پروتکل با N تا 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.

۲-۲ 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^۱ برای این نوع پیچیدگی، کمترین تعداد بیتی است که بین دو نفر جابه‌جا خواهد شد تا پاسخ مساله p با سبب 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.

^۱lower-bound

۲-۲-۱ ماتریس مشخصه

با توجه به تابع از قبل مشخص $f : X \times Y \rightarrow \{0, 1\}$ ، ماتریس مشخصه^۱ تابع f به صورت زیر است:

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

اگر $X = \{x_1, x_2, \dots, x_m\}$ و $Y = \{y_1, y_2, \dots, y_n\}$ ، 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 در مبحث پیچیدگی ارتباطی، می‌توانیم از تمامی هزینه‌ها به جز بیت‌های مخیره شده صرف نظر کنیم، چرا که برای هر یک از شرکت کنندگان قدرت محاسباتی بی‌نهایت در نظر گرفته‌ایم.

۲-۲-۲ 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

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

شکل ۲-۱: ماتریس مشخصه یک تابع دلخواه $f : X \times Y \rightarrow \{0, 1\}$ با $X = Y = \{00, 01, 10, 11\}$.

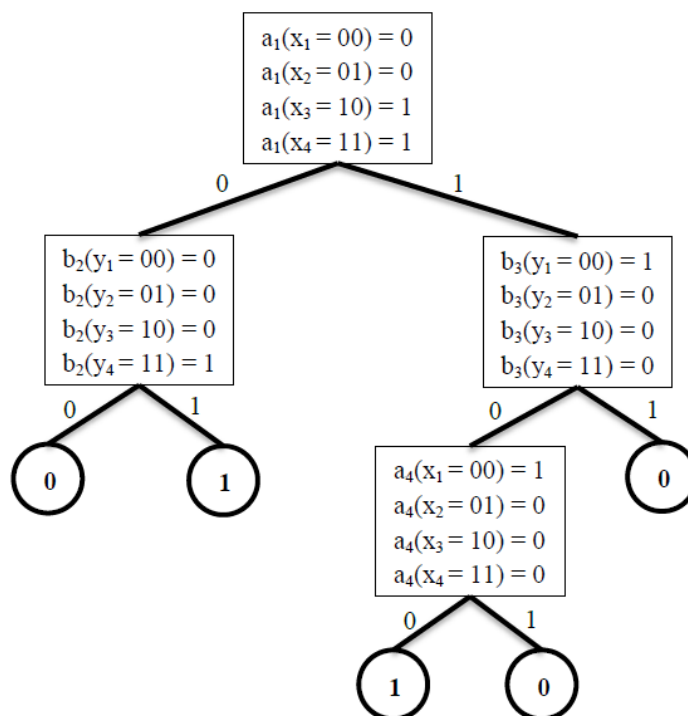
$f : X \times Y \rightarrow \{0, 1\}$ به واسطه ماتریس مشخصه خود در ۲-۲-۲ داده شده باشد. یک پروتکل معتبر برای f در شکل ۲-۲-۲ نشان داده شده است.

۲-۲-۳ قطعه بندی

تعریف ۱. تابع $f : X \times Y \rightarrow \{0, 1\}$ را در نظر بگیرید. یک زیر مجموعه $S \subseteq X \times Y$ -تک‌رنگی^۲ است اگر تابع f روی S ثابت باشد.

^۱Characteristic Matrix

^۲f-monochromatic



شکل ۲-۲: یک پروتکل صحیح برای مخابره تابع مشخص شده در زیر قسمت ۲-۲-۲

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 f -تک‌رنگی جدا از هم قطعه‌بندی^۱ می‌کند. در واقع، حداکثر تعداد مستطیل‌ها 2^C است که C هزینه ارتباطی پروتکل است (ارتفاع درخت).

بیشینه‌ای که در نتیجه فوق مطرح شده است 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 لزوماً معادل یک پروتکل نیست. به عنوان مثال، در شکل ۲-۲-۳ 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).

¹partition

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

شکل ۲-۳: قطع‌بندی‌ای که نمی‌تواند به یک پروتکل نظیر شود. هیچ برشی در قطعه‌بندی وجود ندارد که با انتخاب آن، ماتریس به دو زیرماتریس تبدیل شود.

۲-۲-۴ مجموعه گول‌زننده

به عنوان یک روش برای محاسبه کردن کمینه پیچیدگی ارتباطی یک مساله، می‌توانیم از ابزاری به نام مجموعه گول‌زننده^۱ استفاده کنیم.

تعریف ۲. تابع $f : X \times Y \rightarrow \{0, 1\}$ داده شده است. یک مجموعه $S \subseteq X \times Y$ را مجموعه گول‌زننده 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 گول‌زننده‌ای برای f است.

اثبات. هیچ دوعضوی از مجموعه گول‌زننده S طبق تعریف نمی‌تواند عضو یک مستطیل در قطعه‌بندی باشند، در نتیجه حداقل به تعداد اعضای S ، مستطیل f -تک‌رنگی داریم. طبق نتیجه قبل، حکم ثابت می‌شود.

□

¹Fooling 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

$$\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$$
 به صورت زیر خواهد بود

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

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 ۱ تابع f است. چرا که هیچ دوتایی از ورودی‌هایی که خروجی ۱ دارند، در یک مستطیل نمی‌توانند باشند.

۲-۲-۵ کران اندازه مستطیل

کران اندازه مستطیل^۱ 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 $f : X \times Y \rightarrow \{0, 1\}$ داده شده است. روی اعضای $f^{-1}(1)$ یک توزیع احتمال μ تعریف می‌کنیم به طوری که برای هر مستطیل R شامل مقادیر ۱، $\mu(R)$ کوچک باشد. به همین طریق می‌توانیم برای مقادیر ۰ 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 در نظر بگیرید. در نتیجه

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

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

^۱Rectangle Size Bounds

۲-۲-۶ کمینه رتبه ماتریس^۱

قضیه ۳. تابع $f : X \times Y \rightarrow \{0, 1\}$ داده شده است. داریم $D(f) \geq \log_2(2 \times \text{rank}_F(M_f - 1))$ 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. \square

¹Matrix Rank

فصل سوم

پیچیدگی ارتباطی غیرقطعی

در این بخش، سعی بر این است که مشابه تئوری پیچیدگی محاسباتی، مدل غیرقطعی^۱ 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 $f : X \times Y \rightarrow \{0, 1\}$ ، یک پروتکل غیرقطعی دو بخش خواهد داشت. در ابتدا، یک پیشگو^۲ 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 پروتکلی است که f را محاسبه می‌کند. متناظر

^۱Non-deterministic

^۲Oracle

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 در نظر بگیرید. تعریف رسمی این تابع به شکل زیر می‌باشد:

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

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 (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.

۳-۱ پوشش‌ها

مشابه ارتباط پیچیدگی قطعی با مستطیل‌ها، پیچیدگی غیرقطعی ارتباط مستقیمی با پوشش‌ها^۱ دارد.

تعریف ۳. برای هر $z \in \{0, 1\}$ ، یک z -پوشش^۲ برای f ، مجموعه‌ای از مستطیل‌های R_1, \dots, R_N است که ممکن است اشتراک داشته باشند، به طوری که $f^{-1}(z) = \cup R_i$. حداقل ساینز 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.

^۱Covers

^۲z-Cover

۳-۲ کلاس‌های پیچیدگی

یکی از بزرگ‌ترین مسائل باز موجود در پیچیدگی محاسباتی، درستی تساوی $P = NP \cap coNP$ 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 $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ داریم:

$$D(f) = polylog(n) \Rightarrow f \in P^{CC} \bullet$$

$$N^1(f) = polylog(n) \Rightarrow f \in NP^{CC} \bullet$$

$$N^0(f) = polylog(n) \Rightarrow f \in coNP^{CC} \bullet$$

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.

$$D(f) = O(N^0(f)N^1(f)) \Rightarrow D(f) = O(N^0(f)N^1(f)) = O(\log^{c_1} n \log^{c_2} n) = O(\log^c n)$$

□

۳-۳ تکنیک‌های کمینه‌یابی

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

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

و یا از معادل آن استفاده می‌کنند:

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

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

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

۴-۳ نتیجه‌گیری

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

$$2^{\Theta(\sqrt{D(f)})} \leq C(f) \leq C^D(f) \leq C^P(f) \leq 2^{\Theta(D(f))} \quad (۲-۳)$$

• $C^P(f)$ 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 ساینز یک پوشش z -برای تابع f است.

• $C(f) = C^0(f) + C^1(f)$

نامساوی اول مستقیماً 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]

۴-۱ 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^۱ به شکل زیر خواهد بود. در هر راس درخت (v) ، توابع مشخص‌کننده مسیر A_v, B_v توابع تصادفی هستند. به بیان دیگر، $A_v : X \rightarrow [0, 1]$ 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.

¹Private Coin

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

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

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:

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

۲-۴ مدل سکه عمومی

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

تعریف ۶. می‌گوییم پروتکل تصادفی Π تابع $f : X \times Y \rightarrow Z$ را با خطای ϵ و سکه‌های عمومی^۱ محاسبه می‌کند اگر:

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

هزینه حداقل پروتکلی که تابع f را با سکه عمومی محاسبه می‌کند را با $R_\epsilon^{pub}(f)$ 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 $\{2, \dots, 2n\}$ انتخاب می‌کند.

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

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

نبود صفر برمی‌گرداند.

¹Public 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 $x \bmod p = y \bmod p$. پس در این حالت، خطا وجود خواهد داشت. حال تلاش می‌کنیم مقدار خطا را محاسبه کنیم. فرض کنید که مجموعه $\{p_1, p_2, \dots, p_k\}$ مجموعه تمام اعداد اولی باشد که $x \bmod p_i = y \bmod p_i$ در نتیجه:

$$x \bmod P = y \bmod P \quad P = p_1 p_2 \dots p_k$$

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 مخاברה برای حالت قطعی، $O(n)$ است.

• مدل سکه عمومی: $r = r_1 \dots r_m$ بیت‌های تصادفی مشترک هستند.)

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

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

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.

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

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^۱ نتیجه این شبیه‌سازی را بیان می‌کند.

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

$$R_{\epsilon+\delta}(f) \leq R_{\epsilon}^{pub}(f) + O(\log n + \log \frac{1}{\delta}) \quad (۴-۴)$$

۳-۴ مدل توزیعی

تا به حال در تمام مدل‌های بررسی شده، عنصر تصادف در عملکرد پروتکل بوده است. در مدل توزیعی^۲ ورودی را تصادفی فرض می‌کنند.

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

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

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 مبتنی است:

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

$$\max_{\mu} D_{\epsilon}^{\mu} = R_{\epsilon}^{pub}(f) \quad (۶-۴)$$

۴-۴ کمینه‌یابی

۱-۴-۴ 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 $f : X \times Y \rightarrow Z$ و μ یک توزیع روی $X \times Y$ باشد، می‌توان برای هر مستطیل R ناهمگنی

¹Newman's lemma

²Distributional

^۱ را به صورت زیر تعریف کرد:

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

و

$$disc_{\mu}(f) = \max_R disc_{\mu}(f, R). \quad (۸-۴)$$

به صورت غیررسمی، معیار ناهمگنی پایین یعنی مستطیل‌های بزرگ تعداد تقریباً 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 ناهمگنی:

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

۴-۴-۲ محدود کردن 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، $R_{\epsilon}^{pub} = \Omega(c)$ خواهد بود.

با توجه به قضیه بالا، نیاز است که تکنیکی برای محدود کردن مقدار ناهمگنی بیابیم و از آن برای به دست آوردن کمینه‌هایی روی پیچیدگی تصادفی عمومی به دست آوریم. معروف ترین این تکنیک‌ها، تکنیک مقدار ویژه^۲ است.

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

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

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

¹Discrepancy

²eigenvalue

فصل پنجم

کاربرد پیچیدگی ارتباطی در ساختمان داده‌ها

در این بخش از گزارش، در مورد استفاده از پیچیدگی ارتباطی برای یافتن کمینه‌ها در حوزه ساختمان داده‌ها می‌پردازیم. برای شروع، تعریفی بر روی مدل جست‌وجوی سلول خواهیم داشت، ساختمان داده‌های ایستا و پویا را تعریف می‌کنیم و ارتباط پیچیدگی ارتباطی نامتقارن و مدل جست‌وجوی سلول را مطرح می‌کنیم. در ادامه، با معرفی تکنیک حریصانه در پیچیدگی ارتباطی، کمینه‌های ساختمان داده‌ای را به پیچیدگی مخابرات نزدیک می‌کنیم.

۵-۱ مدل جست‌وجوی سلول

می‌توانید مدل جست‌وجوی سلول^۱ را یک پردازنده و یک حافظه دسترسی تصادفی در نظر بگیرید. یک ساختمان داده را فرض کنید که در این حافظه ذخیره شده است و پردازنده باید با استفاده از این داده به یک جست‌وجو پاسخ دهد. برای ادامه بحث، s تعداد خانه‌های حافظه و w تعداد بیت در هر خانه است. پیچیدگی کاریه تعداد خانه‌هایی است که پردازنده در حین پاسخ به جست‌وجو به آن‌ها دسترسی می‌یابد. [۹]

این مدل، اصلی‌ترین مدل برای اثبات کمینه‌ها در ساختمان داده‌هاست. این بدین معناست که کمینه‌های این

^۱Cell Probe

مدل، کمینه‌های مدل‌های دیگر را در بر دارد. این موضوع برای بیشینه‌ها نیز صادق است.

تعریف ۹. یک مساله ساختمان داده ایستا، مساله‌ای است که با توجه به یک map مانند $f : Q \times D \rightarrow A$ است که در آن D یک مجموعه از داده‌ها است، Q یک مجموعه از جست‌وجوهاست و $f(q, d)$ پاسخ به جست‌وجوی q در مورد داده d است. A نیز مجموعه همه پاسخ‌هاست.

تعریف ۱۰. پاسخ به یک مساله ساختمان داده ایستا در مدل جست‌وجوی سلول با پارامترهای s و w و t ، یک روش برای کدگذاری هر داده مانند $d \in D$ در حافظه ماشین است در صورتی که از s خانه حافظه با w بیت استفاده کنیم در حالی که حداکثر لازم است t خانه را بررسی کنیم تا بتوانیم پاسخی بیابیم.

مثال ۵. با در دست داشتن یک مجموعه مرتب مانند $U = \{1, \dots, m\}$ و یک زیر مجموعه مانند $S \subseteq U$ ، به نحوی S را کدگذاری کنیم و در حافظه قرار دهیم که بتوانیم اولین نیاکان یک عضو مانند $x \in U$ را در S بیابیم.

تعریف ۱۱. ساختمان داده‌های پویا: ساختمان داده‌های پویا شباهت زیادی به ساختمان داده‌های ایستا دارند به جز آن‌که در این مسائل باید بتوان داده‌ها به صورت بهینه در ساختمان داده ذخیره کرد.

۵-۲ پیچیدگی ارتباطی نامتقارن

در این مساله، با پیچیدگی ارتباطی قطعی سروکار داریم. می‌توان هر مساله ساختمان داده را به یک مخابره تبدیل کرد: آلیس یک جست‌وجو مانند $q \in Q$ دریافت می‌کند. و باب یک داده $d \in D$ را دریافت می‌کند و هر دو تلاش می‌کند که تابع $f(q, d)$ را محاسبه کنند. [؟] البته بین این مدل و مدل اصلی مخابره تفاوتی وجود دارد. مثلاً، اندازه داده خیلی بیشتر از جست‌وجو است در نتیجه مخابرات به صورتی نامقارن است، یعنی بار ارتباطی سمتی از مخابره همواره بیشتر از سمتی دیگر است. همچنین تنها آلیس نیاز دارد که پاسخ را بداند. در ادامه، پیچیدگی ارتباطی این مدل باید به طور دیگری سنجیده شود. آلیس پیغام خود را از مجموعه $\{1, \dots, s\}$ انتخاب می‌کند و باب پیغام خود را از بین $\{1, \dots, 2^w - 1\}$ انتخاب می‌کند. پیچیدگی پروتکل همان ماکسیمم تعداد دورهای مخابره بین آلیس و باب است. به صورت رسمی:

تعریف ۱۲. می‌گوییم یک پروتکل مانند P ، یک $[t, (a, b)]^A$ -پروتکل برای تابع f است اگر همه پیام‌های آلیس حداکثر a بیت باشد و پیغام‌های باب حداکثر b بیت باشد و حداکثر t دور مخابره انجام شود در حالی که مخابره را آلیس شروع کرده است. یک $[t, (a, b)]^B$ -پروتکل به همین صورت تعریف می‌شود با تفاوت آن‌که باب مخابره را شروع می‌کند.

قضیه ۹. اگر یک پاسخ به مساله جست و جوی سلول از s خانه استفاده کند و حداکثر شامل t بار دسترسی به خانه‌های حافظه باشد، یک $[t, (\log s, w)]^A$ -پروتکل برای مساله متناظر معادل وجود دارد.

اثبات شبیه‌سازی مطرح شده در تعریف است.

از قضیه بالا می‌توان نتیجه گرفت برای آن که بتوانیم یک کمینه مانند $\Omega(f)$ برای یک مساله ایستا ثابت کنیم (فرض می‌کنیم که $s \in O(n)$) باید نشان دهیم که هیچ یک $[o(f), (\log n, w)]^A$ -پروتکلی برای مساله ارتباطی معادلش وجود ندارد.

در مرحله بعد، نشان می‌دهیم که یک مساله ایستا می‌تواند به یک مساله پویا کاهش یابد.

تعریف ۱۳. مساله ساختمان داده ایستا f متناظر با مساله پویا g به این صورت تعریف می‌شود: برای یک پارامتر d ، $f: Q \times D \rightarrow A$ تابع ایستای ماست که Q همان جست‌وجوهای مساله پویا است و D تمامی حالت‌های قابل دسترسی از حالت اولیه است که حداکثر d بار تغییر یافتن بر روی آن رخ داده‌است.

قضیه ۱۰. اگر یک پاسخ مساله جست و جوی سلول از $n^{O(1)}$ خانه حافظه استفاده کند و t بار دسترسی به حافظه انجام دهد برای تابع g که یک مساله پویاست، در نتیجه مساله معادل ایستای f یک پاسخ دارد که از $O(dt)$ خانه حافظه استفاده می‌کند و $O(t)$ دسترسی انجام می‌دهد.

اثبات. پاسخ ایستا به صورت ساده پاسخ پویا را شبیه‌سازی می‌کند. فرض کنید که ساختمان داده مساله پویا به نحوی در حافظه کدگذاری شده‌است که به طوری که حالت اولیه همه خانه‌ها برابر با 0 هستند. در پاسخ مساله ایستا، به جای ذخیره مقادیر خانه‌هایی که پاسخ پویا به آن‌ها دسترسی داشته است در جای خودشان، همه خانه‌هایی که مقدارشان تغییر کرده است را به همراه مقدار نهایی‌شان در یک دیکشنری قرار می‌دهیم، این عملیات در فضای $O(dt)$ امکان‌پذیر است. هر بار که پاسخ پویا می‌خواهد به یک خانه به‌خصوص دسترسی داشته باشد، ابتدا چک می‌کنیم که آن خانه در دیکشنری وجود دارد یا خیر. اگر داشت، مقدار نهایی را برمی‌گردانیم، در غیر این صورت، 0 برمی‌گردانیم. هر جست‌وجو $O(1)$ زمان می‌برد و نهایتاً باید $O(t)$ جست‌وجو بزنیم. \square

در نتیجه دیدیم که کمینه برای یک پروتکل مخابره، یک کمینه برای مساله ساختمان داده ایستا است؛ همچنین، هر کمینه برای ساختمان داده ایستا، یک کمینه برای ساختمان داده پویا است. از آنجایی که در پروتکل مخابره، آلیس می‌تواند کل ورودی را برای باب بفرستد، بهترین کمینه‌ای که می‌توانیم با استفاده از این مدل از کاهش به پیچیدگی ارتباطی برای مسائل ساختمان داده به دست آوریم برابر است با $t = \Omega\left(\frac{\log |Q|}{\log s}\right)$ اگر

تعداد جست‌وجوها یک چندجمله‌ای در n باشد، کمینه یک مقدار ثابت خواهد بود. به همین علت، تنها مسائلی که حداقل در n نمایی باشند در نظر می‌گیریم.

۳-۵ کمینه

تکنیک‌های اصلی اثبات کمینه برای مدل جست‌وجوی سلولی با استفاده از پیچیدگی ارتباطی استفاده از حذف دور^۱، تکنیک غنا^۲، تکنیک پیچیدگی ارتباطی حریصانه^۳ و کاهش به مساله اشتراک است. در اینجا به بررسی تکنیک حریصانه می‌پردازیم. [۴]

۱-۳-۵ تکنیک پیچیدگی ارتباطی حریصانه

تعریف ۱۴. شرط ردیف تک‌رنگ^۴: یک تابع مانند $h : A \times B \rightarrow C$ را در نظر بگیرید. $A' \subseteq A$ و $B' \subseteq B$ شرط ردیف تک‌رنگ را ارضا می‌کنند اگر:

$$\forall x \in A', \forall y, z \in B' : h(x, y) = h(x, z). \quad (۱-۵)$$

ایده اصلی آن است که با توجه به ماتریس مخابره آلیس و باب، نشان دهیم که همه مستطیل‌هایی که شرط ردیف تک‌رنگ را ارضا می‌کنند، کوچک هستند و تا بتوانیم قضیه بعد را اعمال کنیم و یک کمینه برای تعداد دورهای مکالمه به دست آوریم. از این به بعد، به مستطیل‌هایی که شرط ردیف تک‌رنگ را ارضا کند، مستطیل خوب می‌گوییم.

یک مساله مخابره مانند $h : A \times B \rightarrow C$ را در نظر بگیرید. آلیس ورودی $a \in A$ و باب ورودی $b \in B$ را دارد و بنا است که مقدار $h(a, b)$ محاسبه شود. همچنین، آلیس پیام‌های خود را از مجموعه $\{1, \dots, s\}$ انتخاب می‌کند و باب پیام‌های خود را از مجموعه $\{1, \dots, k\}$ انتخاب می‌کند.

قضیه ۱۱. اگر h یک پروتکل t دوری داشته باشد، یک $A' \subseteq A$ و $B' \subseteq B$ وجود دارد به طوری که $|A'| \geq |A|/s^t$ و $|B'| \geq |B|/k^t$ که شرط ردیف تک‌رنگی را ارضا می‌کنند.

اثبات. استقرا روی t . برای حکم پایه، $t = 0$ در نظر بگیرید. چون هیچ مخابره‌ای انجام نمی‌شود، خروجی فقط به ورودی آلیس وابسته است، پس همه ردیف‌های باید تک‌رنگی باشند تا جوابی برای پروتکل داشته باشیم. در این صورت، $A' = A$ و $B' = B$.

¹Round Elimination

²Richness Technique

³Greedy CC Technique

⁴Monochromatic Row

حال فرض کنید قضیه برای $t = k$ درست باشد. یک مساله ارتباطی با یک پروتکل $t + 1$ دوری در نظر بگیرید. برای هر $a \in \{1, \dots, s\}$ ، تعریف کنید A_a را از ورودی‌هایی مانند $x \in A$ که برای آن‌ها آلیس در ابتدا a را ارسال می‌کرده است. با توجه به اصل لانه کبوتری، می‌توانیم a را به نحوی ثابت نگه داریم که $|A_a| \geq |A|/s$. همین‌طور، تعریف کنید B_b را از ورودی‌هایی مانند $x \in B$ که برای آن‌ها باب در ابتدا b را ارسال می‌کرده است. با توجه به اصل لانه کبوتری، می‌توانیم b را به نحوی ثابت نگه داریم که $|B_b| \geq |B|/k$. یک پروتکل t دوری P' برای مساله ارتباطی محدود به $A_a \times B_b$ وجود دارد که همان پروتکل P را از مرحله دوم به بعد شبیه‌سازی می‌کند. با توجه به فرض استقرا، وجود دارد یک مستطیل ساخته شده از $A'_a \times B'_b$ به طوری که سائزشان حداقل برابر با $1/s^t$ و $1/k^t$ برابر A_a و B_b است. در نتیجه، برابر قراردادن $A' = A'_a$ و $B' = B'_b$ جواب دلخواه را به ما می‌دهد. \square

مثال ۶. کمینه $\Omega(n)$ برای مساله پویای ارزیابی چندجمله‌ای: ساختمان داده F^{n+1} $y \in$ ضرایب یک چندجمله‌ای است و جست‌وجوی مرتبط $x \in F^1$ است. پاسخ آن مشخص می‌کند که آیا این نقطه عضو چندجمله‌ای است یا خیر.

پاسخ بدیهی این سوال $t \in O(n)$ است. برای این که این را نشان دهیم، لازم است یک کمینه برای مساله ارتباطی معادل آن بیابیم.

فرض کنید که باب یک چندجمله‌ای f از درجه n دریافت می‌کند ($y \in F^{n+1}$). همچنین آلیس یک $x \in F$ دریافت می‌کند. هدف این مخابره، محاسبه $f(x)$ است. آلیس پیام‌های خود را از مجموعه $\{1, \dots, s\}$ و باب پیام‌های خود را از مجموعه $\{1, \dots, |F|\}$ انتخاب می‌کند. حالتی را فرض کنید که $F \geq 2^{n \log n}$. حال با استفاده از ویژگی‌های چند جمله‌ای‌ها، مشخص می‌کنیم چگونه سائز مستطیل‌های خوب باید کوچک باشد. برای هر دو چندجمله‌ای متفاوت از درجه n ، حداکثر در n نقطه با هم اشتراک دارند. پس برای یک مستطیل خوب $A' \times B'$ ، $|A'| \leq n$ یا $|B'| \leq 1$. حال می‌خواهیم قضیه را اعمال کنیم.

اگر $|A'| \leq n$ ، در نتیجه $n \geq |F|/s^t$ در نتیجه $(\log |F| - \log n)/(\log s) \in \Omega(n)$. اگر $|B'| \leq 1$ ، پس $1 \geq (|F|^{n+1})/|F|^t$ در نتیجه $t \geq n + 1$ و $t \in \Omega(n)$. همین پروتکل را برای حالت خاص مساله $DISJ$ در نظر بگیرید که در آن آلیس یک عضو دارد و باب یک زیرمجموعه l عضوی. آلیس مجموعه پیغام‌های خود را از مجموعه $\{0, 1\}^{l \log n}$ انتخاب می‌کند. کافی است نشان دهیم بهترین حالت این که آلیس کل ورودی را بفرستد. اگر اندازه مجموعه‌ای که آلیس از آن انتخاب می‌کند برابر با $N = 2^n$ باشد، ورودی آلیس n بیتی و ورودی باب N بیتی خواهد بود. برای یافتن مستطیل خوب لازم است توجه کنیم که دو زیرمجموعه متفاوت l تایی از N ، حداکثر در $l - 1$ عضو اشتراک دارند. پس طبق حالت قبل، سائز مستطیل

خوب محدود و پیچیدگی ارتباطی برابر با n خواهد بود.

فصل ششم

مکانیک کوانتومی

در این 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.

۶-۱ 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. در این دستگاه اندازه‌گیری اندازه میدان الکتریکی و مغناطیسی را چنان تغییر می‌دهیم که مسیر باریکه ذرات هیچ انحرافی حاصل نکند. در این صورت با استفاده 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 در اینجا اندازه‌گیری سرعت کاملاً به صورت غیرمستقیم و با اتکا بر یک چارچوب نظری بدست آمده است. در همین 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 میکروسکوپی 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 میکروسکوپی بعضی از خواص اشیاء هر نوع مقداری می‌توانند اتخاذ کنند؛ مثل جرم اندازه و تکانه و نظایران. 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؟

۶-۲ معنای حالت

برای تعیین کامل حالت ذرات می‌بایست تمام خاصیت‌های سازگار باهم آنها را 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 $\{|a_1\rangle, |a_2\rangle, \dots, |a_N\rangle\}$ (اگر بلافاصله از دستگاه اندازه‌گیری A بیرون آمده‌اند) قرار دارند و یا در یکی از حالت‌های $\{|b_1\rangle, |b_2\rangle, \dots, |b_N\rangle\}$ قرار دارند (اگر بلافاصله از دستگاه اندازه‌گیری B بیرون آمده‌اند) و نظایران. آزمایش‌گر می‌تواند ذرات را که در حالت $|\Psi\rangle$ قرار دارند را از دستگاه اندازه‌گیری A عبور دهد. در این جا، 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 در حالت $|\Psi\rangle$ به طور تصادفی خود را در حالت‌های $|a_1\rangle$ تا $|a_N\rangle$ نشان خواهد داد.

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

$$P(b, a) \quad (۱-۶)$$

خواص زیر برای این تابع احتمال برقرار است:

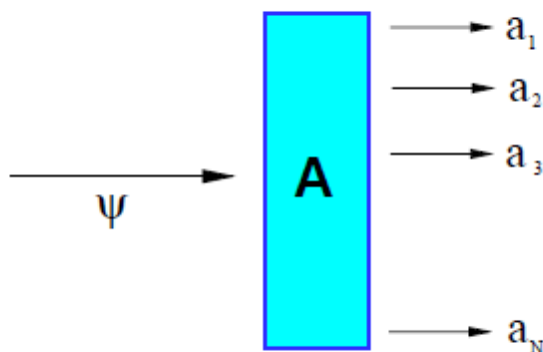
$$\sum_{j=1}^N P(b_j, a) = 1 \quad ۱.$$

$$P(a_i, b_j) = P(b_j, a_i) \quad ۲.$$

$$P(a_i, a_j) = \delta_{ij} \quad ۳.$$

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

شکل ۶-۱: دستگاه اندازه گیری A ذرات را به حالت های مختلف $|a_1\rangle$ تا $|a_N\rangle$ تجزیه می کند. حالت $|\Psi\rangle$ یک حالت ناشناخته است.



۳-۶ تداخل

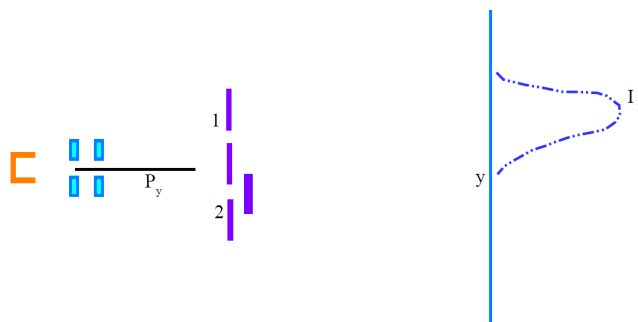
حال به مهم ترین خصلت دنیای میکروسکوپی می رسیم. در شکل درست چپ یک فیلامان حرارتی وجود دارد که بخاری از ذرات بار یونیزه را از خود متصاعد می کند. میدان های الکتریکی به همراه مجموعه ای از یکسوکننده ها ذرات در حالت $|P_y\rangle$ را جدا می کنند. شکاف پایینی مسدود شده است. هر ذره که از شکاف بالایی بگذرد در حالت $|1\rangle$ قرار می گیرد و سپس روی پرده در حالت $|y\rangle$ که نقطه نشستن آن روی پرده را (توسط یک آشکارساز) نشان می دهد، ثبت می شود. هرگاه این آزمایش را برای مدت طولانی انجام دهیم، در اثر نشستن ذرات روی یک پرده - مثلاً یک پرده فلورسانس - طرح I_1 بوجود خواهد آمد. $I_1(y)$ درواقع متناسب با تعداد ذرات نشسته شده روی نقطه y است. درحقیقت داریم

$$I_1(y) = P(y, 1)P(1, P_y) \quad (۲-۶)$$

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

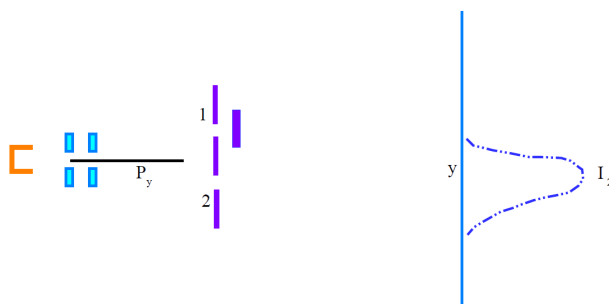
$$I_2 = P(y, 2)P(2, P_y) \quad (۳-۶)$$

شکل ۶-۲: 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 ۶-۳: آزمایش دو شکاف: تنها شکاف پایینی باز است و طرح I_2 روی پرده مشاهده می‌شود.



باشد:

$$I_{1+2} = P(y, 1)P(1, P_y) + P(y, 2)P(2, P_y) = I_1 + I_2 \quad (۶-۴)$$

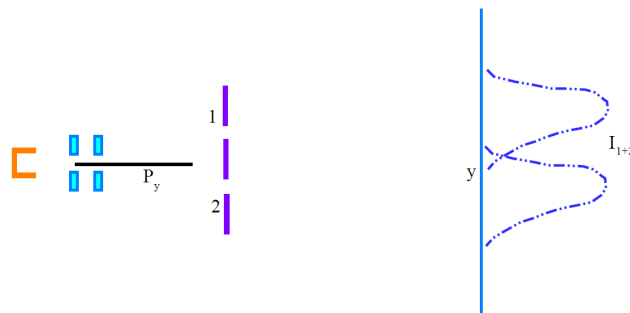
و شکل ۶-۴ مشاهده شود.

اما آنچه که در آزمایش می‌بینیم آن است که ذرات مطابق با طرح I_{12} که یک طرح تداخلی است روی پرده می‌نشینند. (شکل ۶-۵)

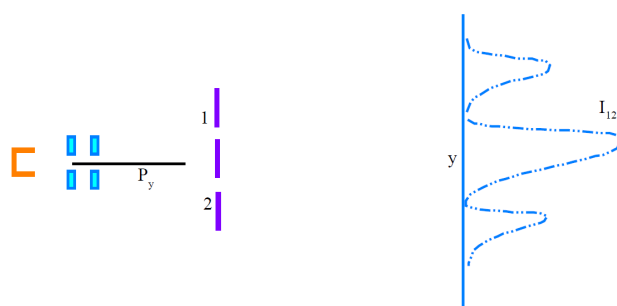
در این طرح چندین نکته جالب و شگفت‌انگیز وجود دارد:

- 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 باز بود به آن نقطه برسد. در جاهایی نیز مثل وسط پرده تعداد ذرات دو برابر آن مجموع تعداد ذراتی است که در صورت باز بودن هر کدام از شکاف‌ها به تنهایی به پرده می‌رسید.
- ب: برعکس در جاهای دیگری از ذرات باز کردن هر دو شکاف باعث شده است که تعداد ذراتی که به آن

شکل ۴-۶: آزمایش دو شکاف: هر دو شکاف باز هستند و طرح I_{1+2} روی پرده مورد انتظار است.



شکل ۵-۶: 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 در صورتی که هر دو شکاف باز می‌بود به آن نقطه می‌رسید.

ج: شکل این طرح تداخلی با رقیق کردن چشمه ذرات بطوری که در هر 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 به خوبی 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 دیگر از 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 می‌توان درست پشت شکاف ها آشکارسازهایی گذاشت تا بفهمیم که ذره درست موقع عبور از شکاف ها چگونه رفتار می‌کند. متوجه می‌شویم که در آنجا هم ذره به صورت یک ابر رفتار نمی‌کند بلکه به تمامی (با تمام جرم و بار و دیگر خصوصیات خود) در آشکارساز 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 آمده‌اند + تعداد ذراتی که از شکاف ۲ آمده‌اند. اما تعداد ذراتی که از شکاف ۱ عبور کرده و روی پرده نشسته‌اند برابر است با I_1 و تعداد ذراتی که از شکاف ۲ عبور کرده و روی پرده نشسته‌اند برابر است با I_2 . پس حتی بدون مشاهده نزدیکی شکاف‌ها می‌توانیم حکم کنیم که طرحی که سرانجام روی پرده ثبت می‌شود، می‌بایست برابر با $I_1 + I_2$ باشد. در صورتی که اتم‌ها مثل توپ فوتبال عمل کرده باشند استدلال بالا صحیح است. درمقابل ایراداتی از این نوع که «بالاخره الکترون یا از این شکاف عبور می‌کند و یا از آن شکاف و در این صورت نمی‌بایست طرح تداخلی داشته باشیم» تنها می‌توانیم به این بسنده کنیم که بگوییم وقتی سوال عبور الکترون از شکاف‌ها را به صورت عملی و تجربی بپرسیم می‌بینیم که طرح تداخلی واقعا از بین می‌رود و ما به تناقضی بر نمی‌خوریم. 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 پیدا کردن نظمی که در جستجوی آن هستیم به تجربیات خود در مورد 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 در مورد امواج چنین است:

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

به طوری که

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

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

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

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:

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

$$\phi_1 = \langle y|1\rangle \langle 1|P_y\rangle \quad (۹-۶)$$

$$\phi_2 = \langle y|2\rangle \langle 2|P_y\rangle \quad (۱۰-۶)$$

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

$$\langle y|P_y\rangle = \langle y|1\rangle \langle 1|P_y\rangle + \langle y|2\rangle \langle 2|P_y\rangle \quad (۱۱-۶)$$

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

$$\langle c_k|a_i\rangle = \sum_j \langle c_k|b_j\rangle \langle b_j|a_i\rangle \quad (۱۲-۶)$$

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:

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

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

با توجه به قانون برابری احتمال

$$P(a,b) = P(b,a) \longleftrightarrow \langle a|b\rangle = \langle b|a\rangle^* \quad (۱۴-۶)$$

پس طبق رابطی کلی زیر

$$\langle b_j|\Psi\rangle = \sum_i \langle b_j|a_i\rangle \langle a_i|\Psi\rangle \quad (۱۵-۶)$$

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، ضرب کردن همه مقادیر در یک فاز، احتمالات را در یک شاخص اندازه‌گیری عوض نخواهد کرد.

۴-۶ معادله شرودینگر

$$i\hbar \frac{\partial \psi}{\partial t} = H\psi \quad (۱۶-۶)$$

معادله شرودینگر^۱ نقش قوانین نیوتن در فیزیک کوانتوم را دارد. برای فهمیدن این معادله با فرمول بندی همیلتونی مکانیک کلاسیک^۲ شروع می‌کنیم.

۱-۴-۶ 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^۳ 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

$$H = T + V \quad (۱۷-۶)$$

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

$$\begin{cases} \dot{q} = \frac{\partial H}{\partial p} \\ \dot{p} = -\frac{\partial H}{\partial q} \end{cases} \quad (۱۸-۶)$$

از آنجا که V مستقل از p است، داریم

$$\frac{\partial H}{\partial p} = \frac{\partial T}{\partial p} = \frac{p}{m} \quad (۱۹-۶)$$

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

$$\dot{p} = -\frac{\partial V}{\partial q}. \quad (۲۰-۶)$$

در نتیجه از ترکیب این دو داریم

$$m\ddot{q} = -\frac{\partial V}{\partial q} \quad (۲۱-۶)$$

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.

^۱Schrodinger Equation

^۲Hamiltonian Mechanics

^۳momentum

۵-۶ اصول مکانیک کوانتومی ۱-۵-۶ اصل اول - 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 ۷. کیوبیت یک سیستم کوانتومی است که فضای هیلبرت H متناظر با آن دوبعدی باشد. اگر پایه تعامد یکه $\{|0\rangle, |1\rangle\}$ را برای این فضا در نظر بگیریم، آن‌گاه داریم:

$$\forall |\Psi\rangle \in H, \quad |\Psi\rangle = a|0\rangle + b|1\rangle, \quad a, b \in \mathbb{C} \quad (۲۲-۶)$$

$$\| |\Psi\rangle \| = 1 \Rightarrow |a|^2 + |b|^2 = 1 \quad (۲۳-۶)$$

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^۱ نامیده می‌شود. فضای برداری متناظر با یک کیودیت با پایه متعامد یکه زیر نمایش داده می‌شود:

$$\{|0\rangle, |1\rangle, \dots, |d-1\rangle\} \quad (۲۴-۶)$$

۲-۵-۶ اصل دوم - 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 $U\mathcal{H} \rightarrow \mathcal{H}$ یکانی وجود دارد که $U|\Psi\rangle = |\Psi'\rangle$ تنها وابسته به زمان است.

¹Qudit

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

$$i\hbar \frac{d}{dt} |\Psi(t)\rangle = H |\Psi(t)\rangle \quad (۲۵-۶)$$

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

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

حال اگر قرار دهیم

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

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 ۸. تحول زمانی یک کیوبیت با ماتریس‌های یکانی 2×2 مانند ماتریس‌های یکانی و هرمیتی زیر که آن‌ها را ماتریس پاولی^۱ می‌نامیم، بیان می‌شود:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (۲۸-۶)$$

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

این عملگرها به صورت زیر عمل می‌کنند:

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle \quad (۳۰-۶)$$

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle \quad (۳۱-۶)$$

یک مثال دیگر، عملگر یکانی هادامارد^۲ است:

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

^۱Pauli Matrices

^۲Hadamard 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

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

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

۳-۵-۶ اصل سوم - اندازه‌گیری

اندازه‌گیری بر روی یک سیستم با فضای هیلبرت \mathcal{H} با مجموعه‌ای به صورت

$$\{M_i : M_i : \mathcal{H} \rightarrow \mathcal{H}, i \in S\} \quad (۳۴-۶)$$

مشخص می‌شود که :

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

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

$$|\Psi'\rangle = \frac{M_i |\Psi\rangle}{\sqrt{p(i)}} \quad (۳۶-۶)$$

تغییر^۳ می‌کند.

مثال ۹. اندازه‌گیری یک کیوبیت، اگر $M_i = |v_i v_i\rangle\langle v_i v_i|$ باشد، آنگاه می‌توان نشان داد که $\{M_0, M_1, \dots, M_{d-1}\}$ یک اندازه‌گیری است. پس اگر حالت سیستم به صورت $|\Psi\rangle = \sum_i a_i |v_i\rangle$ باشد، آنگاه

$$p(i) = \langle \Psi | M_i^\dagger M_i | \Psi \rangle = |a_i|^2 \quad (۳۷-۶)$$

مثال ۱۰. 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 $\mathcal{H} = \bigoplus_{i \in S} W_i$ افزایش فضا به زیرفضاهای عمود بر هم است.

^۳collapse

مثال ۱۱. یک مشاهده‌پذیر^۴ فیزیکی با یک عملگر هرمیتی روی فضای هیلبرت مشخص می‌شود:

$$A : \mathcal{H} \rightarrow \mathcal{H} \quad (۳۸-۶)$$

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_i ها زیرفضاهای تولید شده توسط ویژه‌بردارهای متناظر با λ_i باشند، و P_i را عملگر تصویر عمود بر روی این زیرفضا بگیریم، آنگاه

$$A = \sum_i \lambda_i P_i \quad (۳۹-۶)$$

و از آنجا که بردارهای ویژه A کل \mathcal{H} را می‌پوشانند، داریم $\sum_i P_i = I$. پس اندازه‌گیری $\{P_i\}$ 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 مشاهده‌پذیر که با $\langle A \rangle$ نشان داده می‌شود برابر است با

$$\langle A \rangle = \sum_i \lambda_i p(i) = \sum_i \lambda_i \langle \Psi | P_i | \Psi \rangle = \langle \Psi | \sum_i \lambda_i P_i | \Psi \rangle = \langle \Psi | A | \Psi \rangle \quad (۴۰-۶)$$

۴-۵-۶ اصل چهارم - سیستم‌های 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 سیستم i -م \mathcal{H}_i باشد، فضای هیلبرت متناظر با کل n سیستم برابر است با

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n. \quad (۴۱-۶)$$

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

$$\Psi_1 \otimes \Psi_2 \otimes \dots \otimes \Psi_n. \quad (۴۲-۶)$$

است.

۶-۶ درهم‌تنیدگی^۱

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

^۴Observable
^۱Entanglement

این دو کیویت برابر است با

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{B} \quad (۴۳-۶)$$

که با پایه متعامد یکه

$$\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\} \quad (۴۴-۶)$$

مشخص می شود که برابر است با:

$$\{|00\rangle_{AB}, |01\rangle_{AB}, |10\rangle_{AB}, |11\rangle_{AB}\}. \quad (۴۵-۶)$$

هر $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ به صورت ترکیب خطی از چهار عضو مجموعه بالاست. اگر $|\psi\rangle_{AB}$ را $|\psi\rangle_{AB} = |v\rangle_A \otimes |w\rangle_B$ نمایش داد به این حالت، حالت ضربی^۱ و یا حالت جداپذیر^۲ گفته می شود. اگر چنین نمایشی برای $|\psi\rangle_{AB}$ وجود نداشته باشد، به آن حالت درهم تنیده^۳ می گویند. مثال:

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

یک حالت ضربی است و

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (۴۷-۶)$$

یک حالت درهم تنیده است.

۷-۶ اختتامیه ای بر عجایب مکانیک کوانتومی

کنترل اتم های منفرد و به همراه آن گسترش رایانش و اطلاعات کوانتومی منجر به پیدایش سوال های جدید در ساختمان نظری مکانیک کوانتومی شده است. تلاش برای پاسخ گویی به این سوال ها به نوبه خود منجر به غنی شدن نظریه مکانیک کوانتومی از جهات متعدد شده است. به عنوان مثال، چگونه می توان درهم تنیدگی دو حالت مثل

$$|\phi\rangle = \sqrt{0.9}|0,0\rangle + \sqrt{0.1}|1,1\rangle \quad (۴۸-۶)$$

و

$$|\phi\rangle = \sqrt{0.8}|0,0\rangle + \sqrt{0.2}|1,1\rangle \quad (۴۹-۶)$$

^۱Product State

^۲Seperable State

^۳Entangled 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 فوتون‌هایی را که بیش از یکصد و پنجاه کیلومتر از یکدیگر دور هستند، درهم‌تنیده کنیم. سوال این است که چگونه می‌توانیم با انجام آزمایش در هر کدام از آزمایشگاه‌ها مقدار این درهم‌تنیدگی را کم و زیاد کنیم. چگونه می‌توانیم این کار را برای جفت فوتون‌هایی که بین زمین و ماهواره‌ها درهم‌تنیده هستند انجام دهیم؟ چگونه می‌توانیم اتم‌های ساکن دور از هم را درهم‌تنیده کنیم؟ آیا می‌توانیم شبکه‌ای از حالت‌های درهم‌تنیده بین نقاط مختلف و دور از هم درست کنیم و از آن برای مبادله اطلاعات کوانتومی و فرابرد کوانتومی استفاده کنیم؟

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

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

بیشترین میزان درهم‌تنیدگی را دارد و تمام حالت‌های دیگر را با اعمال موضعی می‌توان از این حالت درست کرد. در واقع می‌توانیم با سنجش درهم‌تنیدگی تمام بردارهای فضای هیلبرت، دو ذره را مرتب کنیم. ولی به محض اینکه به فضای هیلبرت سه کیوبیت می‌رسیم با انواع سوال‌های جدید و بی‌پاسخ مواجه می‌شویم و این وضعیت ساده از بین می‌رود. هیچ ملاک مقایسه‌ای نداریم که بر مبنای آن بگوییم کدام یک از دو حالت

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

یا

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

در هم تنیدگی بیشتری دارند. این گونه مطالعات به ما کمک می‌کنند که ملاک‌های معینی برای دسته‌بندی 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 درهم‌تنیدگی نیستند و حوزه‌های خیلی وسیعی را در بر می‌گیرند. در ادامه به یک نوع دیگر از این سوال‌ها می‌پردازیم.

۶-۸ 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^۱ اهمیت نظری و عملی بسیار زیادی دارند. به عنوان مثال قضیه عدم تکثیر^۲ 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.

۶-۸-۱ تکثیر حالت‌های کوانتومی

نخست ساده ترین حالت را در نظر می‌گیریم. حالتی که می‌خواهیم آن را تکثیر کنیم با $|\phi\rangle$ نشان می‌دهیم. حالتی را که می‌خواهیم 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 می‌دهیم. فرض کنید که یک عمل یکانی وجود دارد که برای هر حالت ورودی کار زیر را انجام می‌دهد:

$$U(|\phi\rangle \otimes |b\rangle \otimes |m\rangle) = |\phi\rangle \otimes |\phi\rangle \otimes |m_\phi\rangle \quad (۶-۵۳)$$

در این 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. در خروجی 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:

$$|+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \quad (۶-۵۴)$$

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

$$U(|0\rangle \otimes |b\rangle \otimes |m\rangle) = |0\rangle \otimes |0\rangle \otimes |m_0\rangle \quad (۶-۵۵)$$

و

$$U(|1\rangle \otimes |b\rangle \otimes |m\rangle) = |1\rangle \otimes |1\rangle \otimes |m_1\rangle \quad (۶-۵۶)$$

و

$$U(|+\rangle \otimes |b\rangle \otimes |m\rangle) = |+\rangle \otimes |+\rangle \otimes |m_+\rangle \quad (۶-۵۷)$$

^۱No go theorems

^۲No Cloning Theorem

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

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

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

$$|m_+\rangle = \sqrt{2}|m_0\rangle = \sqrt{2}|m_1\rangle \quad (۵۹-۶)$$

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

$$|0\rangle|1\rangle + |1\rangle|0\rangle = 0 \quad (۶۰-۶)$$

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

فصل هفتم

محاسبات و الگوریتم‌های کوانتومی

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

۷-۱۰ 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 ویژه‌ای 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^۱ 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

^۱Diophantine

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 تر که به نام تر چرچ - 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^۲ می‌تواند 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^۳ 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 می‌شوند، می‌توانند این مسئله را در زمان خیلی کوتاه‌تری حل کنند.

^۲Qubit

^۳Quantum Parallelism

برهم‌نهی حالت‌ها اگرچه یکی از ویژگی‌های سیستم‌های کوانتومی است ولی ویژگی‌ای نیست که تنها مختص سیستم‌های کوانتومی باشد. مثلاً 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 درهم‌تنیدگی^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 اندازه‌گیری این فاصله را طی کرده باشد. امروزه، با آزمایش‌های دقیق اپتیکی می‌توانیم فوتون‌هایی 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 جنبه‌های معنایی درهم‌تنیدگی شده بود نخستین کاربردهای مهم و تکان‌دهنده درهم‌تنیدگی پدیدار شدند. نخست در سال ۱۹۹۱ معلوم شد که از حالت‌های درهم‌تنیده می‌توان برای توزیع کوانتومی کلید^۱ برای رمزنگاری^۱ 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 شیء چیزی نیست جز حالت کوانتومی آن، این پدیده که به آن فرابرد کوانتومی^۲ می‌گوییم، در واقع نخستین نمونه از جابجایی اشیا با سرعت نور خواهد بود. اینکه یک شیء 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. اخیراً 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

^۱Non-locality^۲Entanglement^۱Quantum Key Distribution^۱Quantum Cryptography^۲Quantum 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 برهم‌کنش‌هایی که با محیط خود دارد بلافاصله حالت او را به یکی از دو حالت تقلیل می‌دهد. این پدیده که به آن وادوسی^۱ می‌گوییم، برای اشیای ماکروسکوپی با سرعت سرسام‌آوری رخ می‌دهد به نحوی که این اشیاء هرگز در چنین حالت‌هایی دیده نمی‌شوند و حال آنکه اشیای میکروسکوپی مثل الکترون و اتم می‌توانند در چنین 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 شیء 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 شیء و تعداد زیاد اتم‌های موجود در آن باشد که در این صورت انجام فرایند کوانتومی برای این گونه اشیاء به کلی منتفی خواهد بود. به هر حال این موضوع که دقیقاً 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.

۷-۲ 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 آنجا 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 هر کدام 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

¹Decoherence

در یک کامپیوتر شبیه‌سازی کرد و توسط این برنامه شبیه‌سازی می‌توان کسوف‌ها 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 سیستم‌های 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 خوشه‌های 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 $10^{300} = 2^{1000}$ 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^۲ 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 می‌گیرند. می‌توان روی این اتم‌ها انواع گیت‌های کوانتومی را اعمال کرد که مثل این

²Optical 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 می‌دهیم 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 اندازه‌گیری کنیم. این اندازه‌گیری 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 شبیه‌سازی کند. از نظر فناوری دیر نخواهد بود که ما بتوانیم در شبیه‌ساز کوانتومی خود میدان‌های کوانتومی ای نظیر میدان الکتروضعیف و یا میدان کرومودینامیک را شبیه‌سازی کنیم و بتوانیم به سوال‌های بنیادی در مورد ساختار ماده پاسخ گوئیم.

۷-۳ فرابرد کوانتومی

درفربرد کوانتومی، هدف ما آن است که بامخبره اطلاعات کلاسیک حالت کوانتومی یک شی را به نقطه‌ای دوردست انتقال دهیم. در ساده‌ترین 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 اصولاً 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 مخبره بشوند که برای مخبره دقیق این مقادیر نیاز به بی‌نهایت مخبره داریم، حتی تخمین آن‌ها هم مخبره 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

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (۱-۷)$$

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^۳ را برای فضای دو کیوبیت در نظر بگیرید:

$$\mathcal{B} = \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\} \quad (۲-۷)$$

که در آن

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

توجه کنید که داریم:

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

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

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

اگر ماتریس‌های پاولی را به خط بیاوریم:

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

خواهیم داشت

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

³Bell basis

$$(۷-۷)$$

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

$$M_1 = |\Phi^+\rangle\langle\Phi^+|, \quad M_2 = |\Phi^-\rangle\langle\Phi^-|, \quad M_3 = |\Psi^+\rangle\langle\Psi^+|, \quad M_4 = |\Psi^-\rangle\langle\Psi^-| \quad (۸-۷)$$

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

$$(M_{1,SA} \otimes I_B) |v\rangle_S \otimes |\Phi^+\rangle_{AB} = (|\Phi^+\rangle\langle\Phi^+| \otimes I_B) |v\rangle_S \otimes |\Phi^+\rangle_{AB} = \frac{1}{2} |\Phi^+\rangle_{SA} |v\rangle_B \quad (۹-۷)$$

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:

$$M_1 \Rightarrow |V\rangle, \quad M_2 \Rightarrow Z|V\rangle, \quad (۱۰-۷)$$

$$M_3 \Rightarrow X|V\rangle, \quad M_4 \Rightarrow XZ|V\rangle.$$

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 ای-بیت^۴ نامیده می‌شود. به طور خلاصه

$$1 \text{ ebit} + 2 \text{ bit} \rightarrow 1 \text{ qubit} \quad (۱۱-۷)$$

۴-۷ کدگذاری چگال

مساله کدگذاری چگال^۵ دقیقاً 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

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (۱۲-۷)$$

^۴Entanglement bit or ebit

^۵Superdense 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

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

نمادگذاری زیر را در نظر بگیرید:

$$\sigma_{00} = I, \quad \sigma_{01} = X, \quad (۱۴-۷)$$

$$\sigma_{10} = Z, \quad \sigma_{11} = ZX.$$

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

$$\sigma_{00}^A \otimes I^B |\Phi^+\rangle = |\Phi^+\rangle, \quad \sigma_{01}^A \otimes I^B |\Phi^+\rangle = |\Phi^-\rangle, \quad (۱۵-۷)$$

$$\sigma_{10}^A \otimes I^B |\Phi^+\rangle = |\Psi^+\rangle, \quad \sigma_{11}^A \otimes I^B |\Phi^+\rangle = |\Psi^-\rangle,$$

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 $\sigma_{ij} \otimes I |\Phi^+\rangle$ بر هم عمودند، این اندازه‌گیری آنها را از هم بدون خطا تشخیص می‌دهد. پس باب از روی حاصل اندازه‌گیری، می‌تواند i, j را بیابد.

۵-۷ الگوریتم‌های کوانتومی

۱-۵-۷ کیوبیت

مفهوم مرکزی در کامپیوتر کوانتومی بیت کوانتومی یا کیوبیت است. یک حافظه کوانتومی n -کیوبیتی^۱ عبارت است از مجموعه‌ای متشکل از n کیوبیت. فضای هیلبرت این حافظه عبارت است از:

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

و بعد آن برابر است با 2^n . دقت کنید که این حافظه می‌بایست 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

^۱n-qubit Quantum Register

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

$$|\phi\rangle \otimes |\phi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle) \quad (17-7)$$

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

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad (18-7)$$

به صورت حاصل ضرب تنسوری 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.

۷-۵-۲ توازی کوانتومی

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

$$|\phi\rangle = \sum_{s=0}^{2^n-1} \phi_s |s\rangle, \quad (19-7)$$

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.

۷-۵-۳ 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. معمولاً 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 n تا 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.

۷-۵-۴ روند یک الگوریتم کوانتومی

الگوریتم کوانتومی در ساده‌ترین شکل آن به مجموعه‌ای از گیت‌های 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.

۷-۶ الگوریتم دوچ-جوزا

الگوریتم دوچ-جوزا^۱ که در سال ۱۹۸۲ مطرح شد به حل مسأله زیر می‌پردازد.

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

شرط: یا F به ازای تمامی ورودی‌ها ۰ 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^۱ از تابع، می‌تواند به جواب قطعی برسد.

۷-۶-۱ 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 $|x\rangle \rightarrow |F(x)\rangle$ مدل کنیم، ولی توجه کنید که سوال پرسیدن در دنیای کوانتومی باید یکانی باشد. حال آنکه $|x\rangle \rightarrow |F(x)\rangle$ یکانی نیست چون بعد فضای ورودی و خروجی یکسان

^۱Deutsch-Jozsa

^۱Quantum Query

نیست. حتی اگر عملگر $\left| \underbrace{000 \dots 0}_{n-1} \right\rangle$ در $|x\rangle \rightarrow |F(x)\rangle$ 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.

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

و یا

$$O_F |x\rangle |y\rangle = |x\rangle |F(x) \oplus y\rangle \quad (۲۱-۷)$$

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 هر دوی این عملگرها یکانی هستند و برای $|\psi\rangle = \sum_x \alpha_x |x\rangle$ داریم:

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

و

$$O_{F(x)} |\psi\rangle |0\rangle = \sum_x \alpha_x |x\rangle |F(x)\rangle. \quad (۲۳-۷)$$

۷-۶-۲ تبدیل فوری روی گروه \mathbb{Z}_2^n

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

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \quad (۲۴-۷)$$

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 $|x\rangle = |b_1\rangle, |b_2\rangle, |b_3\rangle, \dots, |b_n\rangle$ خروجی به صورت زیر خواهد بود:

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

که در آن $y = a_1 \dots a_n$ ، آنگاه $x \cdot y := a_1 b_1 + \dots + a_n b_n$

۷-۶-۳ الگوریتم اصلی

روند الگوریتم را به این صورت شروع می‌کنیم:

۱. حالت n کیوبیتی $|0\dots 0\rangle$ 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.

$$\begin{aligned}
 \left| \underbrace{0\dots 0}_n \right\rangle &\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \\
 &\xrightarrow{T_F} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{F(x)} |x\rangle \\
 &\xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{F(x)} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \\
 &= \frac{1}{2^n} \sum_{y \in \{0,1\}^n} \left(\sum_{x \in \{0,1\}^n} (-1)^{F(x) + x \cdot y} \right) |y\rangle
 \end{aligned} \tag{۷-۲۶}$$

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 $\left| \underbrace{0\dots 0}_n \right\rangle$ می‌دهد.

فرض کنید که در حالت دوم باشیم. با توجه به جمله آخر، ضریب حالت $\left| \underbrace{0\dots 0}_n \right\rangle$ در برهم‌نهی نهایی حساب می‌کنیم. چون $x \cdot y = 0$ 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 $\left| \underbrace{0\dots 0}_n \right\rangle$ عمود است 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.

۷-۷ الگوریتم جست و جوی گرور

مدل الگوریتم قبلی، از ساختار و ماهیت تابع به ما اطلاعی نمی دهند و صرفاً با سوال پرسیدن از مدل، مقدار تابع را در ورودی مورد نظر به ما می دهند. گویی این مدل یک جعبه سیاه^۱ است که ورودی را می گیرد و خروجی را با توجه به آنچه تابع روی آن اثر می کند، به ما می دهد. به این نوع مدل کردن، مدل جعبه-سیاه یا مدل جستاری می گویند. قابل توجه است که پیچیدگی مسائل در این مدل بر حسب تعداد سوال کردن ها محاسبه می شود.

۱-۷-۷ مساله

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

تعداد ورودی ها برابر با $N = 2^n$ می باشد. و به طور کلاسیک نمی توان این مساله را با پیچیدگی بهتر از $O(N)$ حل کرد. الگوریتم کوانتومی گرور^۲ توانایی حل این مساله را با $O(\sqrt{N})$ سوال را دارد.

۸-۷ مقدمه

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

$$T_f |x\rangle = (-1)^{f(x)} |x\rangle \quad (۲۷-۷)$$

تعریف کنید

$$|s\rangle := \frac{1}{\sqrt{N-1}} \sum_{y \in \{0,1\}^n, y \neq t} |y\rangle. \quad (۲۸-۷)$$

در نتیجه، $\langle s|t\rangle$ و

$$|\phi\rangle = \alpha |t\rangle + \beta |s\rangle \Rightarrow T_f |\phi\rangle = -\alpha |t\rangle + \beta |s\rangle \quad (۲۹-۷)$$

در واقع با توجه به شکل ۷-۱، اعمال T_f متناظر با قرینه کردن نسبت به بردار $|s\rangle$ است.

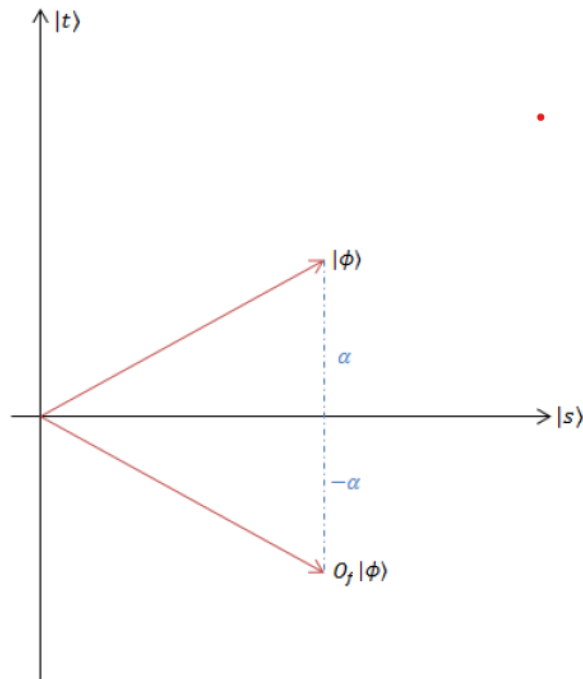
بردارهای $|v\rangle$ و $|w\rangle$ را به صورت زیر تعریف کنید

$$|v\rangle := \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \Rightarrow |v\rangle = \sqrt{\frac{N-1}{N}} |s\rangle + \frac{1}{\sqrt{N}} |t\rangle \quad (۳۰-۷)$$

$$|w\rangle := \frac{1}{\sqrt{N}} |s\rangle - \sqrt{\frac{N-1}{N}} |t\rangle \Rightarrow \langle v|w\rangle = 0$$

^۱Black Box^۲Grover

شکل ۷-۱: اعمال T_f که در واقع عمل قرینه‌کردن نسبت به $|s\rangle$ است.



تبدیل یکانی U را در نظر بگیرید:

$$U := H^{\otimes n} (2 |0\dots 0\rangle\langle 0\dots 0| - I) H^{\otimes n} = 2H^{\otimes n} |0\dots 0\rangle\langle 0\dots 0| H^{\otimes n} - I \quad (۷-۳۱)$$

می‌دانیم

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

در نتیجه،

$$U = 2 |v\rangle\langle v| - I \quad (۷-۳۳)$$

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

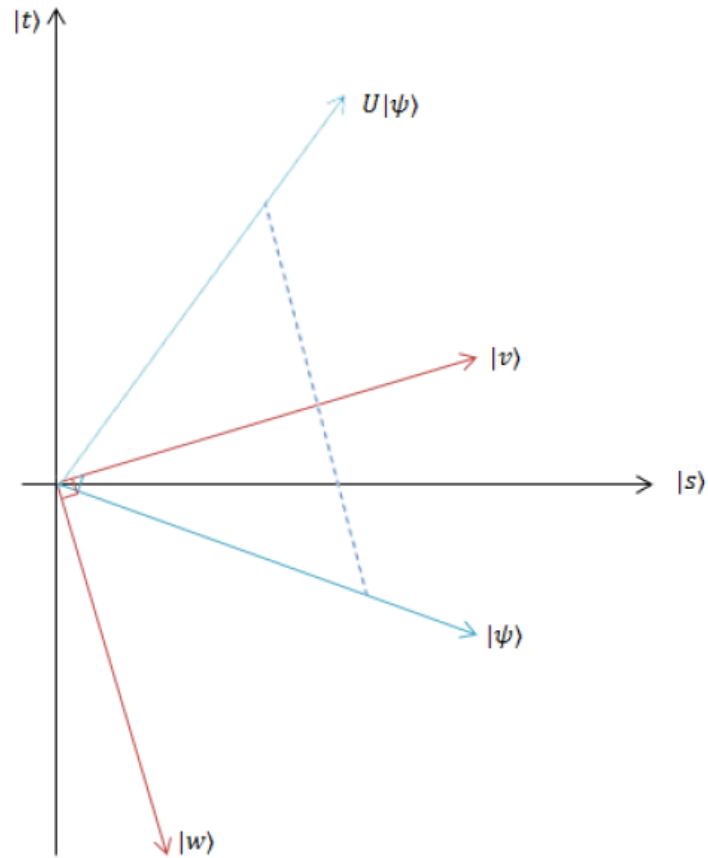
$$U |\psi\rangle = \gamma U |v\rangle + \lambda U |w\rangle = \gamma |v\rangle - \lambda |w\rangle \quad (۷-۳۴)$$

نتیجه می‌شود که U نسبت به $|v\rangle$ عمل قرینه انجام می‌دهد. (شکل ۷-۲)

همانطور که می‌دانیم، ترکیب دو عمل قرینه، یک عمل دوران بدست می‌دهد. (شکل ۷-۳)

$$f = R_{2\theta} \quad (۷-۳۵)$$

شکل ۷-۲: اعمال U که در واقع عمل قرینه‌کردن نسبت به $|v\rangle$ است.



که در آن

$$\cos\theta = \langle v|s \rangle = \sqrt{\frac{N-1}{N}} \Rightarrow \theta \approx \frac{1}{\sqrt{N}} \quad (۷-۳۶)$$

۷-۹ الگوریتم اصلی

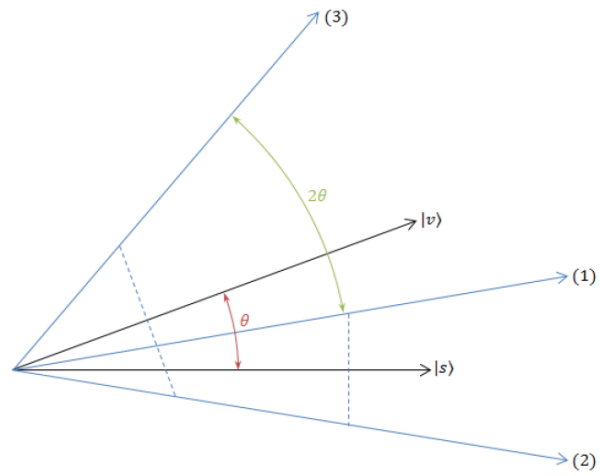
با n کیوبیت که همگی در حالت $|0\rangle$ آماده‌سازی شده‌اند شروع می‌کنیم. ابتدا، روی هر یک از n کیوبیت عملگرد هامارد را اعمال می‌کنیم و بعد $R_{2\theta}$ را q بار و در آخر همه n کیوبیت را اندازه‌گیری می‌کنیم:

$$|0\dots 0\rangle \xrightarrow{H^{\otimes n}} |v\rangle \xrightarrow{(UT_f)^q} |\tau\rangle \rightarrow \text{measurement} \quad (۷-۳۷)$$

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

$$p(t) = \|\langle t|(UT_f)^q|v\rangle\|^2 = \|\langle t|\tau\rangle\|^2 \quad (۷-۳۸)$$

شکل ۷-۳: $(2) = T_f(1), (3) = U(2)$



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^۱ 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] البته در این صورت هم فقط می‌توان دو برابر 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.

¹Holevo's Theorem

۸-۱ 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 $f: X \times Y \rightarrow \{0, 1\}$ به صورت $|y\rangle|0\rangle|x\rangle$ 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 ای-بیت‌ها را. پروتکلی با این سیستم را می‌توان با استفاده از پروتکل مدل اول با سربار ۲ 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 کیوبیت 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 ۱ بیت است. مفهومی که مرز مخابره و محاسبه توزیع شده را جدا می‌کند، در مثال‌های زیر به خوبی نمایش داده شده است.

۸-۲ الگوریتم دوچ-جوزا: توزیع شده

اولین فاصله پیچیدگی ارتباطی کوانتومی و کلاسیک، در همتای ارتباطی و توزیع شده الگوریتم پرسوجوی دوچ-جوزا 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^۱ از مساله برابری است. وعده مذکور به شرح زیر است:

مساله دوچ-جوزا توزیع شده: یا $x = y$ و یا x و y دقیقاً در $n/2$ بیت‌ها با هم اختلاف دارند (n سائز 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 $-\log n$ 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 $|0\dots 0\rangle$ و عملگر یکانی T_f به دست می‌آید.

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

۳. اگر خروجی اندازه‌گیری برابر با $|0^{\log n}\rangle$ بود، خروجی ۱ می‌دهد و در غیر این صورت خروجی ۱.

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:

$$H^{\otimes \log n} \left(\frac{1}{\sqrt{n}} \sum_{i=1}^n (-1)^{x_i + y_i} |i\rangle \right) = \frac{1}{n} \sum_{i=1}^n (-1)^{x_i + y_i} + \sum_{j \in \{0,1\}^{\log n}} (-1)^{i \cdot j} |j\rangle \quad (۱-۸)$$

تنها مساله‌ای که در مورد عبارت فوق باید به آن توجه کنیم آن است که ضریب پایه $|0^{\log n}\rangle$ 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.

¹Promise Problem

۱-۲-۸ مساله اشتراک
۲-۲-۸ 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 بهینه برای این مساله ارائه دهیم. [۷] لازم است ابتدا بدانیم ورودی مساله جست‌وجوی ما چیست.

قرار دهید که

$$z_i = x_i \wedge y_i. \quad (۲-۸)$$

در نتیجه مساله جست‌وجو برابر با یافتن i ی 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

$$|\phi\rangle = \sum_{i=1}^n \alpha_i |i\rangle \quad (۳-۸)$$

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:

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

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.

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

آلیس آخرین کیوبیت را برابر با $|0\rangle$ می‌گذارد (چون x را دارد این عمل یکانی است). پس در نتیجه، آلیس $|\phi\rangle$ 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

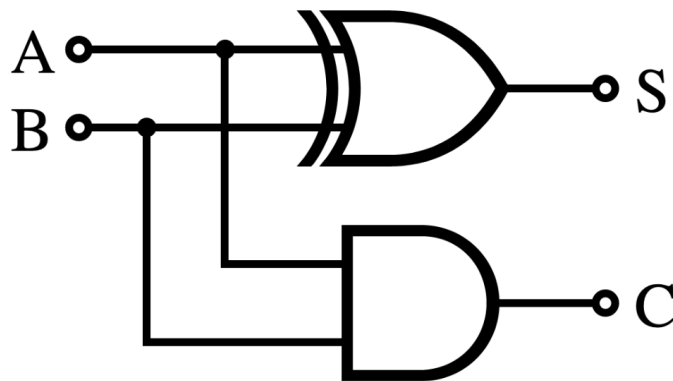
شبیه‌سازی الگوریتم‌ها و پروتکل‌های کوانتومی

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 قانده 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.

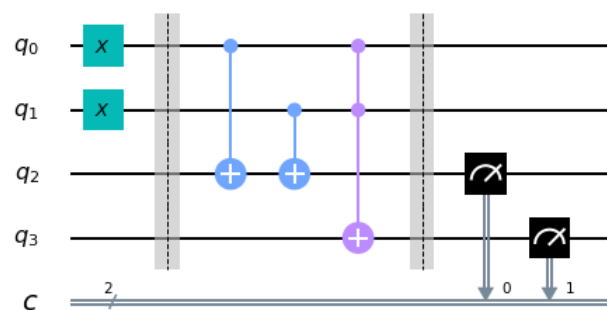
۹-۱ مدار کوانتومی

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 ۹-۱ را به یاد بیاورید. در مورد دنیای محاسبات کوانتومی نیز همین مساله صادق است. مثلاً مدار کوانتومی شکل ۹-۲ کار مدار دیجیتالی شکل ۹-۱ 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 *qiskit* [۱] محصول شرکت *IBM* از پیشروهای علم محاسبات

شکل ۹-۱: مدار دیجیتالی ساده



شکل ۹-۲: مدار کوانتومی ساده



کوانتومی است.

۹-۱-۱ اندازه‌گیری

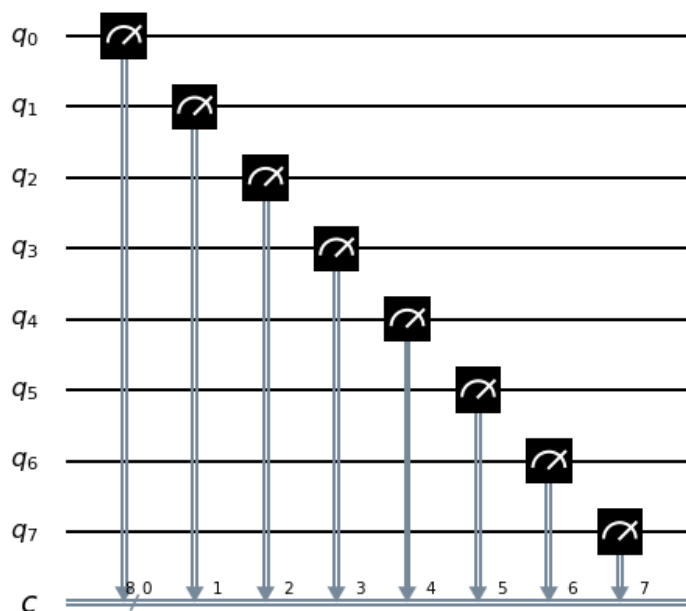
در شکل کد ۹-۳ تلاش می‌کنیم یک مدار کوانتومی ساده با اندازه اولیه ۸ کیوبیت که همه در حالت $|0\rangle$ بسازیم و سپس آن‌ها را اندازه بگیریم. شکل مدار به صورت ۹-۴ خواهد بود. به نمادی که برای اندازه‌گیری مشخص

شکل ۹-۳: ساخت مدار کوانتومی با ۸ 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، گاهی نتایج چندین بار تکرار می‌شود تا به صورت آماری-احتمالی نتایج بررسی شود.

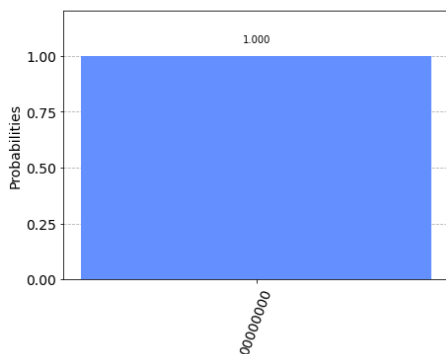
شکل ۹-۴: مدار کوانتومی اندازه‌گیری



مانند شکل ۹-۵. همچنین خوب است بدانیم که چون این ماشین‌های کلاسیک هستند که عملکرد ماشین

شکل ۹-۵: 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 می‌کند، توانایی بیشتر از 30 کیوبیت محاسبه را ندارند.

۹-۱-۲ 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

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (۹-۱)$$

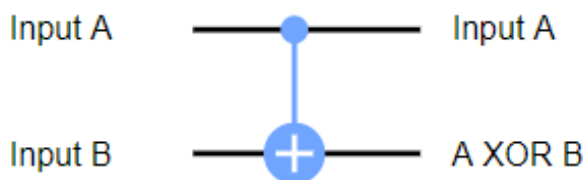
$$Z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (۲-۹)$$

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

$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (۴-۹)$$

همه گیت‌های منطقی کوانتومی برگشت‌پذیر هستند. توجه کنید که عملگر دو کیوبیتی CX یا نات^۱ کنترل‌شده^۱ 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 ۹-۶ توجه کنید. همانطور که می‌بینید، این عملگر همان XOR است، اما برگشت‌پذیر هم هست! نکته‌ای که در دنیای دیجیتال

شکل ۹-۶: گیت CX



نداریم.

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

$$CCX = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (۵-۹)$$

^۱Controlled-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 این کارها، ۴ کیوبیت تعریف می‌کنیم. دو ورودی، دو خروجی و دو بیت کلاسیک برای اندازه‌گیری.

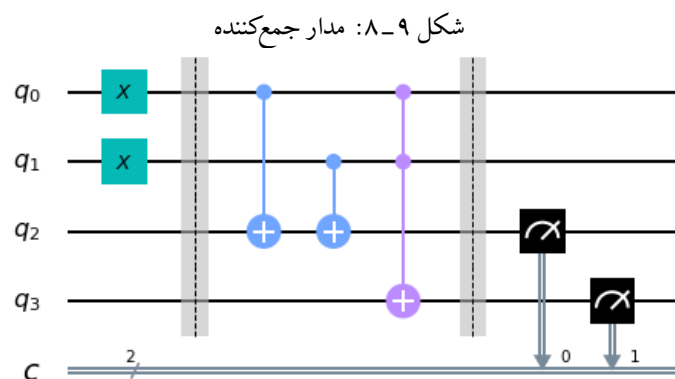
کد شکل ۹-۷ قرار است دو کیوبیت در حالت $|1\rangle$ و $|1\rangle$ را جمع کند. مدار نهایی در شکل ۹-۸ نشان داده

شکل ۹-۷: 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

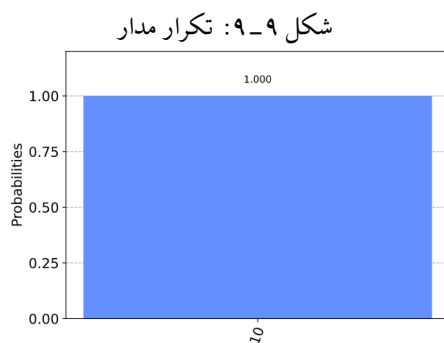
qc_ha.draw()
```

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



۹-۲ فرابرد کوانتومی

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



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 ۹-۱۰ کد مربوط به این کار را می‌بینید. در شکل ۹-۱۱ 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 ۹-۱۱ است.

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

۹-۳ الگوریتم دوچ-جوزا

برای یادآوری، مراحل زیر یک اجرای الگوریتم دوچ-جوزا 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.

$$|\psi_0\rangle = |0\rangle^{\otimes 0} |1\rangle \quad (۹-۶)$$

شکل ۹-۱۰: 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 عملگر هادامارد را روی هر کیوبیت اجرا می‌کنیم.

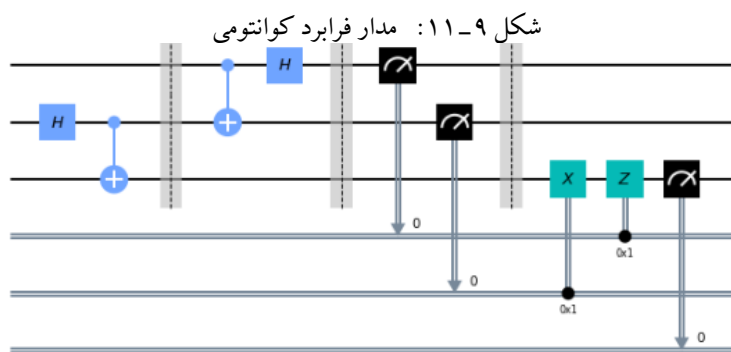
$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle) \quad (۷-۹)$$

۳. جعبه سیاه تابع f را به این صورت اعمال می‌کنیم که در شکل ۹-۱۳ نشان داده شده است.

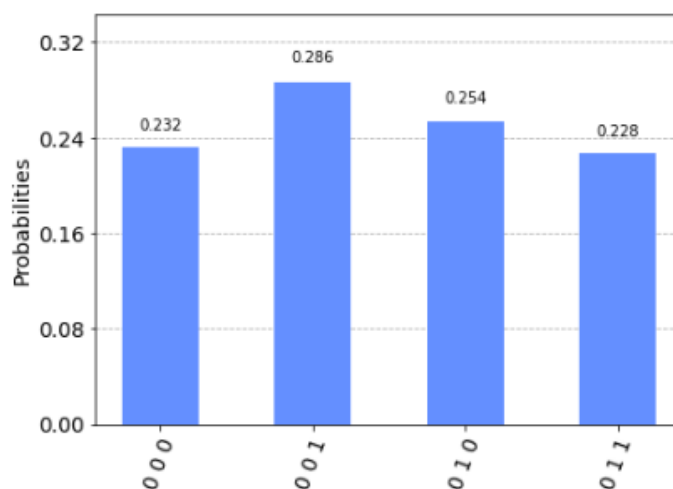
$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|f(x)\rangle - |f(x) \oplus 1\rangle) \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle) \end{aligned} \quad (۸-۹)$$

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

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



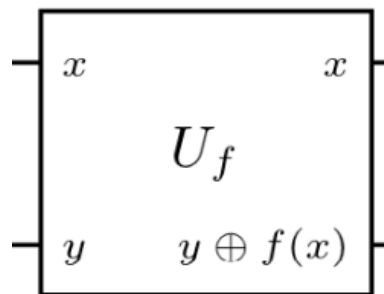
شکل ۹-۱۲: نتیجه اجرای کد به تعداد زیاد



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

در مرحله اول، تلاش می‌کنیم که یک جعبه سیاه 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 ۹-۱۴، دقیقاً 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 ۹-۱۵ 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 ۹-۱۶ توجه کنید. که مدار آن را در شکل ۹-۱۷ می‌بینیم. در نهایت، اجرای چندباره این الگوریتم با این تابع نشان می‌دهد احتمال گرفتن 0000 در خروجی 0 است. (شکل ۹-۱۸)

شکل ۹-۱۳: جعبه سیاه تابع f



شکل ۹-۱۴: کد دوچ-جوزا - 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()

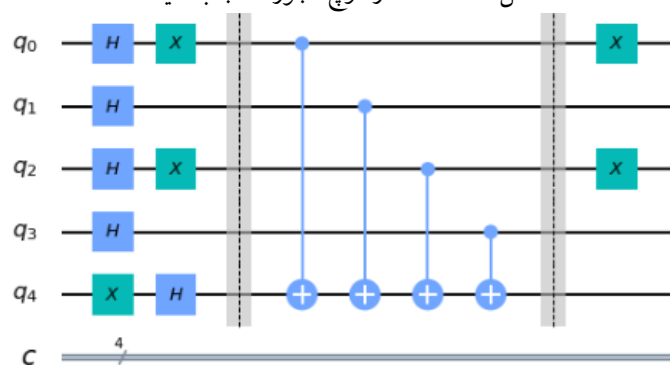
# Controlled-NOT gates
for qubit in range(4):
    balanced_oracle.cx(qubit, 4)

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()
```

شکل ۹-۱۵: مدار دوچ-جوزا - جعبه سیاه



شکل ۹-۱۶: کد دوچ-جوزا

```

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

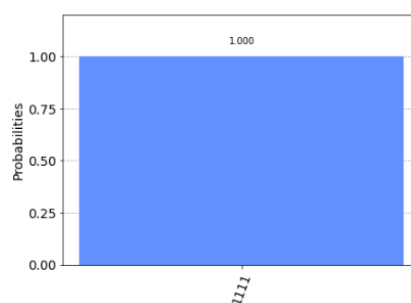
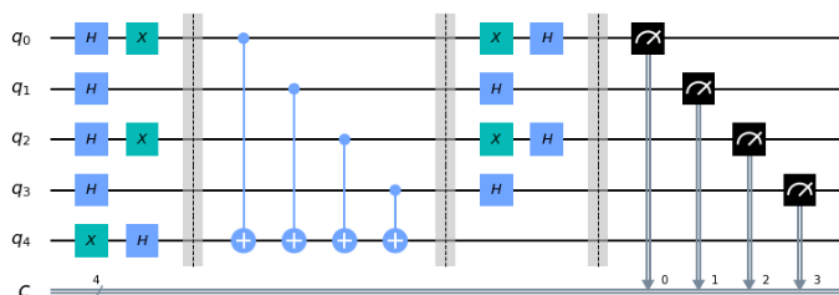
# Repeat H-gates
for qubit in range(4):
    dj_circuit.h(qubit)
dj_circuit.barrier()

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

# Display circuit
dj_circuit.draw()

```

شکل ۹-۱۷: مدار دوچ-جوزا



شکل ۹-۱۸: نتیجه اجرای چند باره این الگوریتم. احتمال خروجی ۱۱۱۱ برابر با ۱۰۰٪ به دست آمده است.

۱- پیوست: مبانی ریاضی مکانیک کوانتومی

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

۱-۱- فضای برداری

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

$$+ : V \times V \rightarrow V, \quad \cdot : F \times V \rightarrow V \quad (10)$$

و دارای خواص زیر باشند:

$$A_1 : x + y = y + x$$

$$A_2 : (x + y) + z = x + (y + z)$$

$$A_3 : \exists 0 \in V | 0 + x = x$$

$$A_4 : \forall x \in V | -x + x = 0$$

(11)

$$M_1 : \alpha(x + y) = \alpha x + \alpha y$$

$$M_2 : (\alpha + \beta)x = \alpha x + \beta x$$

$$M_3 : \alpha(\beta x) = (\alpha\beta)x$$

$$M_4 : 1x = x$$

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

مثال ۱۲. مجموعه‌های زیر هرکدام یک فضای برداری هستند.

۱. R^n یا مجموعه n -تایی‌های مرتب حقیقی

۲. C^n یا مجموعه n -تایی‌های 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 ۱۵. هرگاه V یک فضای برداری و $W \subset V$ یک زیر مجموعه از آن باشد، آنگاه W را یک زیرفضای V گوئیم اگر W نسبت به جمع بردارها و ضرب اعداد در بردارها بسته باشد.

۱-۲ ضرب داخلی و اندازه

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

$$\langle x, y + \alpha z \rangle = \langle x, y \rangle + \alpha \langle x, z \rangle \quad (12)$$

$$\langle x, y \rangle = \langle y, x \rangle^* \quad (13)$$

$$\langle x, x \rangle \geq 0 \quad (14)$$

$$\langle x, x \rangle = 0 \rightarrow x = 0 \quad (15)$$

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

قضیه ۱۲. کوشی-شوارتز: در فضای ضرب داخلی داریم:

$$|\langle x, y \rangle| = \langle x, x \rangle \langle y, y \rangle. \quad (16)$$

تعریف ۱۶. اندازه یک بردار: در هر فضای ضرب داخلی، می توان اندازه یک بردار را به شکل زیر تعریف کرد:

$$|x| := \sqrt{\langle x, x \rangle} \quad (17)$$

با توجه به نامساوی کوشی-شوارتز می توان نوشت:

$$|\langle x, y \rangle| = |x| |y| \quad (18)$$

تعریف ۱۷. فضای نرم یا اندازه‌دار: یک فضای برداری V که در آن نگاشت $\| \cdot \| : V \rightarrow R$ تعریف شده باشد را فضای برداری اندازه‌دار^۱ می‌گوییم هرگاه شرایط زیر برقرار باشد:

$$\|v\| \geq 0 \quad \forall v \quad (۱۹)$$

$$\|v\| = 0 \rightarrow v = 0 \quad (۲۰)$$

$$\|\alpha v\| = |\alpha| \|v\| \quad (۲۱)$$

$$\|v + w\| \leq \|v\| + \|w\| \quad (۲۲)$$

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 لزوماً 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.

۳-۱- پایه

پایه به‌هنگار^۲ $\{e_i, i = 1, \dots, N\}$ را برای فضای برداری V در نظر می‌گیریم. به‌هنگار 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:

$$x = \sum_{i=1}^N x_i e_i \quad (۲۳)$$

بدیهی است که

$$x_i = \langle e_i, x \rangle \quad (۲۴)$$

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

^۱Normed Vector Space

^۲Normal

استخراج کنیم. در نظر بگیرید $e'_i = S_{li}e_l$:

$$x'_i = \langle e'_i, x \rangle = \langle S_{li}e_l, x \rangle = S_{li}x_l \quad (25)$$

و یا به صورت فشرده‌تر:

$$x' = xS. \quad (26)$$

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:

$$S^\dagger S = I \quad (27)$$

چنین ماتریسی را ماتریس‌های یکانی^۱ می‌گوییم.

که در آن S^\dagger ماتریس الحاقی^۱ S است و چنین تعریف می‌شود:

$$S^\dagger = (S^*)^T \quad \text{or} \quad S_{ij}^\dagger = (S^*)_{ji} \quad (28)$$

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

$$S^\dagger = S. \quad (29)$$

۴-۱- فضای کامل و هیلبرت

تعریف ۱۸. دنباله کوشی: در یک فضای برداری، دنباله‌ای از بردارها مانند $\{x_1, x_2, \dots, x_n, \dots\}$ در نظر می‌گیریم. این دنباله، یک دنباله کوشی نامیده می‌شود هرگاه فاصله بین بردارها به تدریج کم شود؛ به عبارت دقیق‌تر، هرگاه به ازای هر $\epsilon > 0$ عددی مانند N یافت شود که

$$\forall m, n > N \rightarrow |x_n - x_m| \leq \epsilon \quad (30)$$

در یک فضای برداری، لزوماً حد کوشی در خود فضا قرار ندارد. مثلاً، هرگاه میدان اعداد گویا را به عنوان یک فضای برداری روی خودش در نظر 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.

^۱Unitary

^۱Conjugate Transpose

تعریف ۱۹. یک فضای برداری را فضای برداری کامل گوئیم هرگاه حد دنباله کوشی را در خود داشته باشد.

تعریف ۲۰. یک فضای برداری با ضرب داخلی کامل را فضای هیلبرت^۱ می‌نامیم. از آنجایی که میدان اعداد حقیقی و مختلط کامل است، می‌توان ثابت کرد هر فضا با بعد محدود روی این میدان‌ها هیلبرت است.

۵-۱- تبدیلات خطی

در یک فضای برداری V ، نگاشت $\hat{T} : V \rightarrow V$ را یک تبدیل خطی یا یک عملگر خطی^۱ می‌گوئیم هرگاه دارای خاصیت زیر باشد:

$$\hat{T}(x + \alpha y) = \hat{T}(x) + \alpha \hat{T}(y) \quad \forall \alpha \in F, x, y \in V \quad (31)$$

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

$$\langle e_j, \hat{T}e_i \rangle = T_{ji} \quad (32)$$

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

$$\hat{T}x = \hat{T}x_i e_i = x_i (\hat{T}e_i) = x_i T_{ji} e_j = (T_{ji} x_i) e_j = (Tx)_j e_j \quad (33)$$

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

همچنین، با تعویض پایه، ماتریس تغییر می‌یابد:

$$T'_{ij} = \langle e'_i, \hat{T}e'_j \rangle = \langle S_{li} e_l, \hat{T} S_{mj} e_m \rangle = S_{li}^* T_{lm} S_{mj} \quad (34)$$

که به صورت زیر قابل بازنویسی است:

$$T' = S^\dagger T S \quad (35)$$

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. در نتیجه، 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

$$(AB)x := A(Bx) \quad (36)$$

¹Hilbert Space

¹Linear 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 یک‌دار^۲ 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:

$$\langle A, B \rangle = tr(AB^\dagger) \quad (۳۷)$$

که در آن رد^۱ ماتریس $tr(A)$ برای ماتریس مربعی A برابر با مجموعه درایه‌های قطر اصلی است.

۱-۶ جمع نیمه‌مستقیم دو زیرفضا

تعریف ۲۱. هرگاه V یک فضای برداری و U و W دو زیرفضای آن باشند، $U + W$ را به عنوان مجموعه زیر تعریف می‌کنیم:

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

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

تعریف ۲۲. فرض کنید که V یک فضای برداری و U و W دو زیرفضای آن باشند به طوری که:

$$V = W + U \quad ۱.$$

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

در این صورت V جمع نیمه‌مستقیم^۲ U و W می‌گوییم و می‌نویسیم

$$V = U \oplus W \quad (۳۹)$$

قضیه ۱۳. اگر $V = W \oplus U$ 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 ۱۴. اگر $V = U + W$ آنگاه $dim(V) = dim(U) + dim(W)$.

^۲Unital

^۱Trace

^۲Semi-direct Sum

تعریف ۲۳. فرض کنید که $V = V_1 \oplus V_2 \oplus \dots \oplus V_r$. در این صورت، هر بردار $v \in V$ به صورت یکتای $v = v_1 + v_2 + \dots + v_r$ تجزیه می‌شود. P_j را عملگری تعریف کنید که:

$$P_j v = v_j \quad (۴۰)$$

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

قضیه ۱۵. عملگرهای تصویری^۱ خواص زیر را دارند:

$$P_j P_k = \delta_{jk} P_j \quad ۱.$$

$$\sum_{j=1}^r P_j = I \quad ۲.$$

قضیه ۱۶. هرگاه V یک فضای ضرب داخلی باشد و $V = \bigoplus_{j=1}^r V_j$ که در آن V_j ها بر هم عمود هستند، آنگاه عملگرهای P_j هرمیتی^۲ هستند.

۷-۱- مساله ویژه مقدار

عملگر $T: V \rightarrow V$ را در نظر می‌گیریم. مساله ویژه مقدار^۱ عبارت است از یافتن بردارهای غیرصفری که تحت اثر T به مضربی از خود تبدیل بشوند:

$$Tx = \lambda x \quad (۴۱)$$

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

$$\det(T - \lambda I) = 0 \quad (۴۲)$$

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

بردار مربوط به λ_i که در معادله $Tv_i = \lambda_i v_i$ صدق می‌کند را ویژه‌بردار^۲ متناظر با آن ویژه‌مقدار می‌خوانیم. هرگاه x و y ویژه‌بردارهای مربوط به λ باشند، بدیهی است که هر ترکیب خطی از آن‌ها هم ویژه‌بردار^۳ از λ است. بنابراین، مجموعه بردارهای متعلق به یک ویژه‌مقدار تشکیل یک زیرفضا را می‌دهند که به آن ویژه‌فضای^۳ آن ویژه‌مقدار می‌گویند.

^۱Image Operators

^۲Hermitian

^۱Eigenvalue

^۲Eigenvector

^۳Eigenspace

۸-۱ عملگرهای هرمیتی، یکانی و بهنجار

تعریف ۲۴. در یک فضای ضرب داخلی، الحاقی یک عملگر T عملگری مانند T^\dagger است که در شرط زیر صدق کند:

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

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

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

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

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

$$(A^\dagger)^\dagger = A \quad ۴.$$

تعریف ۲۵. 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 ۲۶. در یک فضای ضرب داخلی، عملگر یکانی U به عملگری گفته می‌شود که ضرب داخلی بردارها رو حفظ کند، یعنی

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

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

تعریف ۲۷. عملگر نرمال یا بهنجار عملگری است که با الحاقی خود جابه‌جا شود. عملگرهای هرمیتی و یکانی نرمال هستند.

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

قضیه ۱۷. فرض کنید که A یک عملگر بهنجار است. در این صورت اگر $Ax = \lambda x$ آنگاه $A^\dagger x = \lambda^* x$.

نتیجه: ویژه‌مقادیر یک عملگر هرمیتی حقیقی هستند.

قضیه ۱۸. ویژه‌بردارهای متناظر با ویژه‌مقدارهای متمایز یک عملگر بهنجار بر هم عمودند.

تعریف ۲۸. عملگر مثبت نیمه معین^۱ عملگری است که

$$\forall v \in V : \quad \langle x, Tx \rangle \geq 0 \quad (۴۶)$$

همچنین عملگر مثبت معین^۲ عملگری است که

$$\forall v \in V : \quad \langle x, Tx \rangle > 0 \quad (۴۷)$$

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

$$A = \sum_{i=0}^{d-1} \lambda_i |v_i\rangle\langle v_i| \quad (۴۸)$$

آنگاه تعریف می‌کنیم:

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

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

۹-۱- نمادگذاری دیراک

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

$$v = \sum_{i=1}^N v_i e_i \quad (۵۰)$$

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

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

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:

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

$$\langle v| = (v_1^* \quad v_2^* \quad \dots \quad v_N^*) \quad (۵۳)$$

^۱Positive Semidefinite

^۲Definite 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:

$$\langle v|v\rangle = \sum_{i=1}^N v_i^* v_i = \langle v, v\rangle \quad (54)$$

بردارهای پایه e_1, \dots, e_N نیز شکل زیر را پیدا می‌کنند:

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

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

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

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

بنابراین داریم

$$|v\rangle = \sum_{i=1}^N v_i |i\rangle \quad (55)$$

$$\langle v| = \sum_{i=1}^N v_i^* \langle i| \quad (56)$$

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

خواص زیر برای این نمادگذاری وجود دارد:

$$1. \quad \langle v|w\rangle = \langle v, w\rangle$$

$$2. \quad \langle v|w + w'\rangle = \langle v|w\rangle + \langle v|w'\rangle$$

$$3. \quad \langle v|cw\rangle = c \langle v|w\rangle$$

$$4. \quad \langle cv|w\rangle = c^* \langle v|w\rangle$$

$$5. \quad \langle v|v\rangle \geq 0$$

$$6. \quad \langle v|v\rangle = 0 \rightarrow |v\rangle = \langle v| = 0$$

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

$$\langle i|v\rangle = v_i \quad .۸$$

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

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

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

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

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

$$\sum_i |i\rangle \langle i| = I \quad .۱۴$$

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

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

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

-۱- ضرب تنسوری

هرگاه $(A)_{m \times n}$ و $(B)_{p \times q}$ دو ماتریس با ابعاد داده شده باشند، می توان ضرب تنسوری^۳ آن ها را که ماتریسی با ابعاد $mp \times nq$ است را به شکل زیر تعریف کرد

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

به لحاظ عملی ضرب این دو ماتریس به شکل زیر محاسبه می شود:

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

^۳Tensor Product

ضرب تنسوری خواص زیر را دارد:

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

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

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

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

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

حال اگر فضای برداری V با بردارهای پایه $\{|i\rangle, i = 1, \dots, m\}$ و فضای برداری W با بردارهای پایه $\{|\mu\rangle, \mu = 1, \dots, m\}$ را در نظر 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^۴ می‌کنند که با بعد mn است که آن را فضای برداری ضرب تنسوری V و W 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

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

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

^۴Span

References

- [1] ABRAHAM, H., ET AL. Qiskit: An open-source framework for quantum computing, 2019.
- [2] AJTAI, M. A lower bound for finding predecessors in yao’s cell probe model, 1988. Available at [link](#).
- [3] BABAI, L., FRANKL, P., AND SIMON, J. Complexity classes in communication complexity theory, 1986. Available at [link](#).
- [4] BRASSARD, G. Quantum communication complexity, 2001.
- [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 [link](#).
- [11] LEE, T., AND SHRAIBMAN, A. Lower bounds in communication complexity, 2009.
- [12] MILTERSEN, P. B., NISAN, N., SAFRA, S., AND WIGDERSON, A. On data structures and asymmetric communication complexity, 1998. Available at [link](#).
- [13] NIELSEN, M. A., AND CHUANG, I. L. Quantum computation and quantum information, 2010.

- [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](#).