دانشکده فیزیک

تبدیل فوریه کوانتومی

دانشجو:

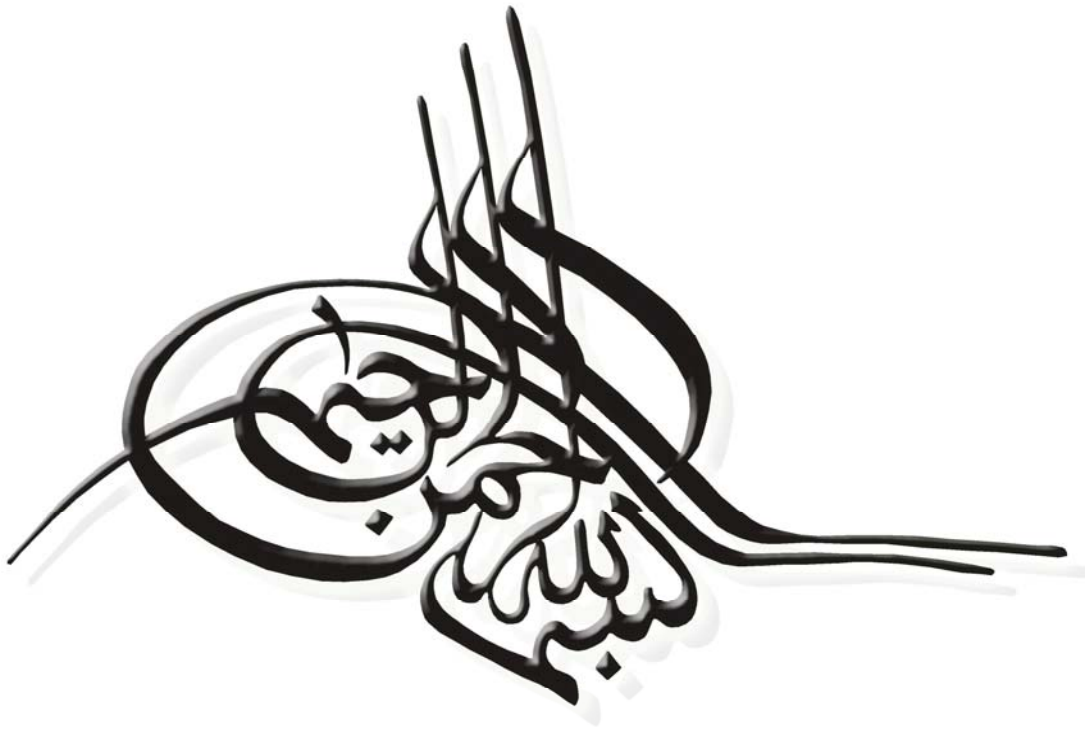
رضا مکرمی رستمی

استاد راهنما:

دکتر حسین موحدیان

پایان‌نامه ارشد جهت اخذ درجه کارشناسی ارشد

تیر ۱۳۸۸


بسم الله الرحمن الرحيم

پیوست شماره ۲

دانشگاه صنعتی شاهرود

دانشکده :فیزیک

پایان نامه ارشد رضا مکرمی رستمی

تحت عنوان:
تبدیل فوریه کوانتمی

در تاریخ ۸۸/۴/۳۰ توسط کمیته تخصصی زیر جهت اخذ مدرک کارشناسی ارشد مورد ارزیابی و با

درجه بسیار خوب مورد پذیرش قرار گرفت.

اساتید راهنما:	امضاء	اساتید مشاور:	امضاء
نام و نام خانوادگی: دکتر حسین موحدیان		نام و نام خانوادگی:	
نام و نام خانوادگی: دکتر		نام و نام خانوادگی :	

اساتید داور:	امضاء	نماینده تحصیلات تکمیلی	امضاء
نام و نام خانوادگی: دکتر علی اکبر رجبی		نام و نام خانوادگی : دکتر محمدرضا شجاعی	
نام و نام خانوادگی: دکتر کاظم بی تقصیر فدافن			
نام و نام خانوادگی:			
نام و نام خانوادگی:			

تقدیم به خانواده و تمام عزیزانم

آنان که خمیدند تا راست قامت بمانم

آنان که موی سپید کردند تا روی سپید بمانم

تقدیر و تشکر

بر خود لازم می دانم که از تمامی عزیزانی که در طول انجام پایان نامه از راهنمایی هایشان استفاده کرده ام تشکر کنم. از استاد راهنمای عزیز جناب آقای دکتر حسین موحدیان که در بسیاری از مواقع از راهنمایی های ارزنده ایشان استفاده نمودم کمال تشکر و امتنان را دارم.

از زحمات بی دریغ اساتید گرامی دانشکده فیزیک دانشگاه صنعتی شاهرود آقایان دکتر رجبی، دکتر عشقی، دکتر قاضی، دکتر ایزدیفرد، دکتر بی تقصیرو... تشکر می کنم.

از کلیه دوستانم که در طی دوران تحصیل فضایی آرام و دوستانه و فرهنگی را با ایشان تجربه کردم سپاس گزاری می کنم.

از پدر و مادر و خانواده ام که مرا یاری کرده اند تشکر می کنم.

از برادر عزیزم که همیشه پشتیبان و مشوقم بوده است سپاس گزارم.

در پایان از همسرم که در این مدت همیشه یار و یاور من بوده قدردانی می کنم.

تعهد نامه

اینجانب ..... رضا مکرمی رستمی ..... دانشجوی دوره کارشناسی ارشد / دکتری رشته فیزیک ذرات بنیادی .....

دانشکده ..... فیزیک ..... دانشگاه صنعتی شاهرود نویسنده پایان نامه/ رساله تبدیل فوریه کوانتومی .....

..... تحت راهنمائی دکتر حسین موحدیان تعهد می شوم .

- تحقیقات در این پایان نامه/ رساله توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است .
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است .
- مطالب مندرج در پایان نامه/ رساله تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است .
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می باشد و مقالات مستخرج با نام « دانشگاه صنعتی شاهرود » و یا « Shahrood University of Technology » به چاپ خواهد رسید .
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان نامه / رساله تأثیرگذار بوده اند در مقالات مستخرج از پایان نامه/ رساله رعایت می گردد.
- در کلیه مراحل انجام این پایان نامه/رساله ، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است .
- در کلیه مراحل انجام این پایان نامه/رساله ، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری ، ضوابط و اصول اخلاق انسانی رعایت شده است .

تاریخ :

امضای دانشجو

مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج ، کتاب ، برنامه های رایانه ای ، نرم افزار ها و تجهیزات ساخته شده است) متعلق به دانشگاه صنعتی شاهرود می باشد . این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود .
- استفاده از اطلاعات و نتایج موجود در پایان نامه / رساله بدون ذکر مرجع مجاز نمی باشد.

* متن این صفحه نیز باید در ابتدای نسخه های تکثیر شده پایان نامه/ رساله وجود داشته باشد .

چکیده:

همان طور که می‌دانیم تبدیل فوریه کوانتومی از سال ۱۹۵۸ میلادی مورد بررسی قرار گرفته است. پژوهش حاضر حالت‌های درهم‌تنیده و حالت‌های برهم‌نهیده در نظریه کوانتومی و ویژگی‌های آنها را بررسی می‌کند. همچنین به بررسی تبدیل فوریه کوانتومی و امکان بهینه سازی سرعت تجزیه به عوامل اول با استفاده از تبدیل فوریه کوانتومی می‌پردازد. اهمیت بررسی و تحقیق در مورد تبدیل فوریه کوانتومی به علت استفاده بسیار گسترده آن در عملیات اساسی و بنیادی کامپیوترهای کوانتومی است. تبدیل فوریه کوانتومی در بسیاری از مسائل کامپیوترهای کوانتومی کاربرد دارد از جمله در مسئله تجزیه اعداد به عوامل اول، مسئله پیدا کردن ترتیب، مسئله جوابهای شمارش، مسئله زیر گروه‌های مخفی و مسئله لگاریتم گسسته. با بررسی تبدیل فوریه کوانتومی و موارد ذکر شده‌ی فوق بویژه تجزیه اعداد به عوامل اول، با استفاده از الگوریتم تجزیه شر که نتیجه‌ای از تبدیل فوریه است، اعداد در کامپیوترهای کوانتومی با سرعت بیشتری تجزیه می‌شوند. در این پژوهش الگوریتم تجزیه مورد تحلیل و بررسی قرار گرفت.

کلمات کلیدی:

تبدیل فوریه کوانتومی، درهم‌تنیدگی، برهم‌نهی، تجزیه، نظریه‌کوانتومی، عملگر چگالی، کیوبیت، گیت، تخمین فاز، الگوریتم تجزیه شر.

عنوان صفحه

فهرست مطالب

فصل اول: مقدماتی درباره مکانیک کوانتومی

فصل دوم: معرفی گیت‌های کلاسیکی و کوانتومی

فصل سوم:معرفی محاسبات کوانتومی

فصل چهارم: تبدیل فوریه کوانتومی و کاربردهای آن

فهرست اشکال

فهرست جداول

فصل اول:

مقدماتی درباره مکانیک کوانتومی

مقدماتی درباره مکانیک کوانتومی

۱-۱- مقدمه

بر طبق اصل موضوع نظریه کوانتومی می‌توانیم حالت یک سیستم را با یک بـردار در فـضای هیلبـرت تعیین کنیم. با هر اندازه‌گیری بر روی مشاهده پذیر سیستم این بردار بر ویژه بردارهـای عملگـر مـورد نظر تصویر می‌شود. بیشتر وقتها به اجـزای سیـستم کوانتـومی علاقـه منـدیم و بـه کلیـات آن توجـه نمی‌کنیم. همان طور که گفتیم حالت یک سیستم با یک بردار توصیف مـی شـود حـال مـی خـواهیم حالت اجزای سیستم را بررسی کنیم و اینکه ببینیم چگونه می توان آنها را توصیف کرد.

۱- ۲- قواعد مکانیک کوانتومی

نظریه کوانتومی یک الگوی ریاضی از جهان فیزیکی است. برای مشخص کردن این الگو لازم اسـت تـا حالتها، مشاهده پذیر ها، اندازه‌گیری ها و دینامیک را مشخص کنیم.

۱-۲-۱- حالتها:

یک حالت، یک توصیف کامل از یک سیستم فیزیکی است. در مکانیک کوانتومی یک حالت یک پرتو[1] در فضای هیلبرت است.

فضای هیلبرت چیست؟

الف) فضای هیلبرت یک فضای برداری از اعداد مختلط C است. بردارها با $|\psi\rangle$ (نمایش کت دیراک) نشان داده می شوند.

ب) در فضای هیلبرت یک ضرب داخلی به صورت $\langle\psi|\varphi\rangle$ تعریف می‌شود که یک جفت بـردار را بـه عدد C نگاشت می دهد و با خواص زیر نشان داده می شود.

۱. ضرب بردارها مثبت است. یعنی برای همه $|\psi\rangle \neq 0$ داریم $\langle\psi|\psi\rangle > 0$.

[1] . ray

۲. ضرب بردارها خطی است. یعنی برای تمام a وb های متعلق به اعداد حقیقی داریم:

$$\langle\varphi|\big(a|\psi_1\rangle+b|\psi_2\rangle\big)=a\langle\varphi|\psi_1\rangle+b\langle\varphi|\psi_2\rangle$$

۳. این ضرب پاد یکانی است. یعنی برای $|\psi\rangle$ و $|\varphi\rangle$ در این فضا داریم:

$$\langle\varphi|\psi\rangle=\langle\psi|\varphi\rangle^*$$

ج) فضای هیلبرت کامل است. یعنی بردارها از رابطه زیر پیروی می‌کنند:

$$\|\psi\|=\langle\psi|\psi\rangle^{\frac{1}{2}}$$

(کامل بودن یک شرط مهم در فضای تابع با ابعاد نامحدود است. چون همگرایی ویژه تابع معین را تضمین می کند.)

پرتو چیست؟

یک نوع هم‌ارزی از بردارهاست که با ضرب به وسیله یک اسکالر مختلط غیر صفر، متفاوت است. ما می توانیم یک نمایش از این نوع را (برای هر بردار غیر صفر) با داشتن مقدار واحد انتخاب کنیم.

$$\langle\psi|\psi\rangle=1 \qquad (۱-۱)$$

همچنین می‌دانیم $|\psi\rangle$ و $e^{i\alpha}|\psi\rangle$ یک حالت فیزیکی یکسان را توصیف می کنند چون $|e^{i\alpha}|=1$.

توجه شود که هر پرتو به یک حالت ممکن مربوط است. بنابراین با داشتن دو حالت $|\varphi\rangle$ و $|\psi\rangle$، می توانیم یک شکل دیگر به صورت $a|\varphi\rangle+b|\psi\rangle$ که اصل ترکیب[1] نامیده می‌شود داشته باشیم. فاز نسبی در این ترکیب دارای یک اثر فیزیکی است.

($a|\varphi\rangle+b|\psi\rangle$ را با $e^{i\alpha}\big(a|\varphi\rangle+b|\psi\rangle\big)$ می شناسیم نه با $a|\varphi\rangle+e^{i\alpha}b|\psi\rangle$).

۱-۲-۲- مشاهده پذیرها:

یک مشاهده پذیر یک خاصیت از سیستم فیزیکی است که می تواند اندازه‌گیری شود. در مکانیک کوانتومی مشاهده پذیر، یک عملگر خود الحاقی است. یک عملگر یک نگاشت خطی است که بردارها

[1] .superposition

را به بردارها می برد:

$$A:|\psi\rangle \to A|\psi\rangle \qquad (۲-۱)$$

$$A\left(a|\varphi\rangle + b|\psi\rangle\right) = aA|\varphi\rangle + bA|\psi\rangle$$

الحاقی عملگر A به وسیله رابطه زیر برای همه‌ی بردارهای $|\varphi\rangle$ و $|\psi\rangle$ تعریف می شود:

$$\langle\phi|A\psi\rangle = \langle A^{\dagger}\phi|\psi\rangle \qquad (۳-۱)$$

در اینجا $A|\psi\rangle$ را با $|A\psi\rangle$ نشان داده‌ایم. عملگرA یک عملگر خودالحاقی است اگر داشته باشیم:

$$A = A^{\dagger} \qquad (۴-۱)$$

اگر A و B خود الحاقی باشند بنابراین A+B نیز عملگر خود الحاقی است چون:

$$(A+B)^{\dagger} = A^{\dagger} + B^{\dagger} \qquad (۵-۱)$$

هر عملگر خود الحاقی در یک فضای هیلبرت H یک نمایش طیفی دارد که به صورت زیر نشان داده می شود:

$$A = \sum_n a_n\ p_n \qquad (۶-۱)$$

که هر a_n یک ویژه مقدار A و P_n مربوط به تصویرگر عمودی ویژه بردار با ویژه مقدار a_n است.

(اگر a_n تبهگن نباشد پس $p_n = |n\rangle\langle n|$ تصویر بر روی ویژه بردار مربوطه است).

p_n ها شرط زیر را برآورده می کنند.

$$p_n p_m = \delta_{n,m} p_n$$
$$p_n{}^{+} = p_n \qquad (۷-۱)$$

۱-۲-۳- اندازه‌گیری:

در مکانیک کوانتومی خروجی عددی یک اندازه گیری هر مشاهده پذیر A یک ویژه مقدار A است. درست بعد از اندازه‌گیری، حالت کوانتومی در یک ویژه حالت A، با ویژه مقدار اندازه گیری شده قرار می‌گیرد. اگر حالت کوانتومی درست قبل از اندازه گیری $|\psi\rangle$ باشد، پس نتیجه a_n با احتمال زیر بدست می آید.

$$prob(a_n) = \left\| \langle P_n | \psi \rangle \right\|^2 = \langle \psi | p_n | \psi \rangle \qquad (۸-۱)$$

اگر نتیجه a_n بدست بیاید، حالت کوانتومی نرمال به صورت زیر است:

$$\frac{p_n|\psi\rangle}{\left(\langle \psi | p_n | \psi \rangle\right)^{\frac{1}{2}}} \qquad (۹-۱)$$

توجه شود که اگر سیستم بلافاصله بعد از اندازه گیری اول دوباره اندازه‌گیری شود نتیجه یکسان با احتمال یک بدست می آید.

۱-۲-۴- دینامیک:

دینامیک تحول زمانی یک حالت کوانتومی یکانی است. آنچه که به وسیله عملگرخودالحاقی بدست می آید، هامیلتونین سیستم نامیده می شود. در تصویر شرودینگر[1] از دینامیک، بردار توصیف کننده حرکت سیستم در زمان، مطابق معادله شرودینگر[2] است:

$$\frac{d}{dt}|\psi(t)\rangle = -iH|\psi(t)\rangle \qquad (۱۰-۱)$$

که H هامیلتونین سیستم است. ممکن است این معادله با تقریب مرتبه اول در مقدار بی نهایت کوچک dt به صورت زیر نشان داده شود:

$$|\psi(t+dt)\rangle = (1 - iHdt)|\psi(t)\rangle \qquad (۱۱-۱)$$

عملگر $U(dt) = 1 - iHdt$ یکانی است. چون H خودالحاقی است شرط $UU^{\dagger} = 1$ با تقریب خطی مرتبه اول dt برآورده می شود. چون حاصلضرب عملگرهای یکانی محدوداست، تحول زمانی بر روی یک فاصله محدود یکانی است.

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \qquad (۱۲-۱)$$

در حالتی که H به t وابسته است می توان U را به صورت $U=e^{-itH}$ نوشت.

---

[1] .Schrodinger picture
[2]- Schrödinger equation

یک خاصیت جالب معادله شرودینگر این است که خطی است، در حالی که درفیزیک کلاسیک با معادلات دینامیکی غیر خطی آشنا بودیم.

اگر $|\psi(0)\rangle$ را مشخص کنیم تحول زمانی حالت $|\psi(t)\rangle$ را بعد از گذشت زمان t پیشگویی می کند.

۱-۳- کیوبیت[1]

واحد تجزیه ناپذیر اطلاعات کلاسیکی بیت نام دارد که یکی از دو مقدار ممکن $\{0,1\}$ را می گیرد. واحد معادل در اطلاعات کوانتومی بیت کوانتومی یا اصطلاحاً کیوبیت نامیده می شود، که یک حالت را در ساده ترین سیستم کوانتومی ممکن توصیف می کند. کوچکترین فضای هیلبرت غیر بدیهی دو بعدی است. پایه های یک فضای برداری دو بعدی را به صورت $\{|0\rangle,|1\rangle\}$ نشان می دهیم. عمومی‌ترین حالت نرمالیزه شده به صورت زیر بیان می شود:

$$a|0\rangle + b|1\rangle \qquad (۱۳-۱)$$

که a و b اعداد مختلط هستند که شرط $|a|^2 + |b|^2 = 1$ را برآورده می کنند. یک کیوبیت حالتی در یک فضای هیلبرت دو بعدی است که می تواند هر مقدار رابه شکل معادله (۱-۱۳) بگیرد. می توانیم یک اندازه‌گیری انجام دهیم که کیوبیت را در پایه های $\{|0\rangle,|1\rangle\}$ تصویر کند. در نتیجه بعد از اندازه‌گیری با احتمال $|a|^2$ حالت $|0\rangle$ را خواهیم داشت و با احتمال $|b|^2$ حالت $|1\rangle$ بدست می‌آید. اگر مقدار کیوبیت اولیه نامعلوم باشد، هیچ راهی وجود ندارد که a و b را با یک اندازه‌گیری یا با هر اندازه‌گیری ممکن تعیین کرد. اما بعد از اندازه گیری کیوبیت در یک حالت شناخته شده‌ی معلوم $|0\rangle$ یا $|1\rangle$ قرار می گیرد که عموماً با حالتی که از قبل داشت متفاوت است. به همین دلیل یک کیوبیت با یک بیت کلاسیکی متفاوت است. می توانیم یک بیت کلاسیکی را بدون برهم زدن آن اندازه بگیریم و می‌توانیم تمام اطلاعات بیت کلاسیکی را کشف کنیم. فرض می کنیم یک بیت کلاسیکی داریم که واقعاً یک مقدار محدود (صفر یا یک) را دارد، اما مقدار اولیه نامشخص است. بنا بر اطلاعات در

[1] .qbit

دسترس فقط می توانیم بگوییم که با احتمال p_0 بیت مقدار صفر را دارد و با احتمال p_1 مقدار یک را دارد که $p_0+p_1=1$. وقتی که بیت رااندازه بگیریم، اطلاعات اضافی بدست می آوریم. بعد از این مقدار بیت را با اطمینان ۱۰۰٪ می دانیم.

۱-۳-۱- اسپین $\frac{1}{2}$:

ضرایب a و b در معادله (۱-۱۳)، کاری بیش از کدگذاری احتمالات حاصل از یک اندازه‌گیری در پایه‌های $\{|0\rangle,|1\rangle\}$ را انجام می‌دهند. به طور خاص، فاز نسبی a و b نیز دارای مفهوم فیزیکی است.

معادله (۱-۱۳) را می توان به صورت حالت یک شی (مثلاً الکترون) با اسپین $\frac{1}{2}$ تفسیر کرد که در آن $|0\rangle$ و $|1\rangle$ حالتهای اسپین بالا $(|\uparrow\rangle)$ و اسپین پایین $(|\downarrow\rangle)$ در طول یک محور خاص مثل محور z هستند. دو عدد حقیقی مشخص کننده کیوبیت، اسپین را در فضای سه بعدی نشان می دهند (بر طبق کره بلاخ که در آن θ زاویه قطبی و φ زاویه سمتی است.).

۱-۳-۲- تقارن:

در اینجا به طور خلاصه بعضی خصوصیات نظریه تقارن مکانیک کوانتومی را بیان می کنیم. یک تقارن یک تبدیل است که بر روی یک حالت از یک سیستم عمل می کند به طوری که همچنان تمام خصوصیات مشاهده پذیرهای سیستم بدون تغییر می ماند. در مکانیک کوانتومی مشاهده‌ها همان اندازه‌گیری عملگرهای خودالحاقی هستند. اگر A در حالت $|\psi\rangle$ اندازه‌گیری شده باشد، آنگاه نتیجه $|a\rangle$ (یک ویژه بردار A) با احتمال $|\langle a|\psi\rangle|^2$ رخ می دهد. با انجام یک عمل تقارن وقتی که هم سیستم و هم دستگاه راچرخش دهیم نباید این احتمال را تغییر دهد.

پس یک تقارن یک نگاشت از بردارها در فضای هیلبرت است به صورت:

$$|\psi\rangle \to |\psi'\rangle \qquad (۱۴-۱)$$

که مقادیر قدر مطلق ضرب داخلی را برای همه $|\varphi\rangle$ و $|\psi\rangle$ ها طبق رابطه زیر حفظ می کند:

$$\left|\langle\varphi|\psi\rangle\right| = \left|\langle\varphi'|\psi'\rangle\right| \qquad (۱۵-۱)$$

بر طبق قضیه مشهور ویگنر[1]، یک نگاشت با این خصوصیات (با اتخاذ یک فاز مناسب) را همواره هم می‌توان به عنوان یکانی و هم به عنوان پاد یکانی در نظر گرفت. پاد یکانی با وجود اهمیت در تقارن‌های گسسته، برای تقارن‌های پیوسته قابل کاربرد نیست. پس تقارن به صورت زیر عمل می کند:

$$|\psi\rangle \to |\psi'\rangle = U|\psi\rangle \qquad (۱۶-۱)$$

که U یکانی و در حالت خاص خطی است.

۱-۳-۳- شکل تقارن‌های یک گروه:

عمل تقارن شرایط گروه را برآورده می‌کند. چون یک تبدیل متقارن می تواند معکوس شود و همچنین حاصلضرب دوتقارن یک تقارن است. برای هر عمل تقارنی R عمل کننده بر روی سیستم فیزیکی، یک تبدیل یکانی U(R) وجود دارد. ضرب این عملگرهای یکانی می‌بایست از قانون ضرب گروه تقارن پیروی کند. به کار بردن R_1o R_2 باید معادل به کار بردن ابتدا R_2 و سپس R_1 باشد. پس باید داشته باشیم:

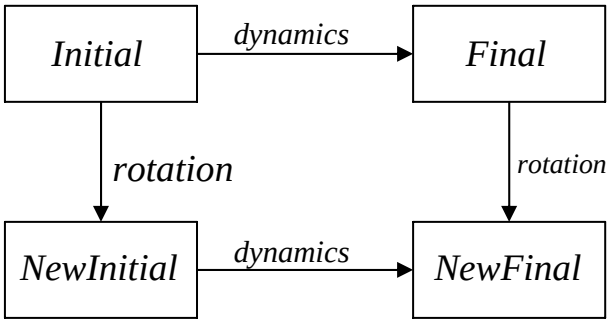
$$U(R_1)U(R_2) = Phase(R_1, R_2)U(R_1 o R_2) \qquad (۱۷-۱)$$

فاز در معادله بالا نادیده گرفته می شود چون حالت های کوانتومی پرتو هستند، فقط احتیاج داریم که $U(R_1 o R_2)$ به شکل یکسان به صورت $U(R_1)U(R_2)$ به روی پرتوها عمل کند - نه بر روی بردارها- U(R) یک نمایش یکانی از گروه متقارن فراهم می کند.

تا کنون عقیده داشتیم تقارن با دینامیک ارتباط ندارد. معمولاً از تقارن می خواهیم که تحول دینامیکی یک سیستم را نشان دهد. یعنی اگر ابتدا سیستم را تبدیل کنیم و سپس تحول را انجام دهیم نباید با زمانی که ابتدا تحول را انجام می دهیم و سپس تبدیل را، تفاوت داشته باشد.

[1]- Wigner

به عبارت دیگر طبق نمودار زیر جابجا پذیر است.



شکل (۱-۱):تقارن و تحول.

این بدین معناست که عملگر تحول زمانی e^{-itH} باید با تبدیل تقارن U(R) جابجا شود:

$$U(R)e^{-itH} = e^{-itH}U(R) \qquad (۱۸-۱)$$

و با بسط دادن رابطه فوق به صورت خطی از مرتبه t بدست می‌آوریم:

$$U(R)H = HU(R) \qquad (۱۹-۱)$$

اگر R را خیلی کوچک به صورت $R = I + \varepsilon T$ انتخاب کنیم، که در آن I تبدیل یکانی و T یک چرخش است، و U نزدیک 1 باشد:

$$U = 1 - i\varepsilon Q + O(\varepsilon^2) \qquad (۲۰-۱)$$

از یکانی بودن U (از مرتبه ε) نشان داده می شود که Q یک مشاهده پذیر است و $Q = Q^{\dagger}$. با بسط رابطه (۱-۱۹) ازمرتبه ε داریم:

$$[Q, H] = 0 \qquad (۲۱-۱)$$

یعنی مشاهده پذیر Q با هامیلتونین H جابجا می شود.

معادله (۱-۲۱) یک قانون پایستگی است. این رابطه برای مثال بیان می کند که اگر یک ویژه حالت از Q فراهم کنیم، پس تحول زمانی تعیین شده به وسیله معادله شرودینگر ویژه حالت را در همان حالت حفظ می‌کند.

۱-۳-۴- ارتباط نظریه چرخش با اندازه حرکت زاویه‌ای:

به طور خلاصه نشان می دهیم که چگونه نظریه عمومی با چرخش خاص و اندازه حرکت زاویه ای به کار می‌رود. یک چرخش بی نهایت کوچک به اندازه $d\theta$ حول محور معین با بردار واحد مانند بردار $\hat{n} = (n_1, n_2, n_3)$ و با استفاده از رابطه (۱-۲۰) و جاگذاری $d\theta$ به جای ε و $\hat{n}.\vec{J}$ به جای Q به صورت زیر نشان داده می شود:

$$R(\hat{n}, d\theta) = I - id\theta\hat{n}.\vec{j} \qquad (۱-۲۲)$$

که درآن (J_1,J_2,J_3) مولفه های اندازه حرکت زاویه‌ای هستند. یک چرخش محدود به صورت زیر نشان داه می‌شود.

$$R(\hat{n}, \theta) = \exp\left(-i\theta\hat{n}.\vec{j}\right) \qquad (۱-۲۳)$$

چرخش ها حول محور مشخص جابجا نمی‌شوند. از این خصوصیت ذاتی چرخش ها، رابطه جابجایی زیر را بدست می‌آوریم:

$$\left[J_k, J_l\right] = i\varepsilon_{klm}J_m \qquad (۱-۲۴)$$

که ε_{klm} تانسور پاد متقارن کلی با $\varepsilon_{123} = 1$ است و اندیسها پی در پی جمع بسته می‌شوند. با انجام چرخش ها بر روی سیستم کوانتومی، عملگرهای خودالحاقی J_1, J_2, J_3 را درفضای هیلبرت پیدا می کنیم که شرط این رابطه را برآورده می کنند. تعریف نمایش گروه چرخش در سه بعد است، اما ساده ترین نمایش غیربدیهی غیرقابل تبدیل، دو بعدی است که به وسیله رابطه زیر داده می شود:

$$J_k = \frac{1}{2}\sigma_k \qquad (۱-۲۵)$$

که با توجه به آن ماتریسهای پائولی زیر را داریم:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad (۱-۲۶)$$

چون ویژه مقادیر J_k برابر $\pm\frac{1}{2}$ هستند، به این نمایش اسپین $\frac{1}{2}$ می‌گوییم. یکی ازخواص ماتریسهای پائولی این است که به صورت دو به دو دارای خاصیت پاد جابجایی هستند، و داریم:

$$\sigma_k\sigma_l + \sigma_l\sigma_k = 2\sigma_{kl}I \qquad (۲۷-۱)$$

بنابراین وقتی که $\hat{n} = (n_1, n_2, n_3)$ و $\vec{\sigma}$ ماتریس پائولی است داریم:

$$(\hat{n}.\vec{\sigma})^2 = n_k n_l \sigma_k \sigma_l = n_k n_l I = I \qquad (۲۸-۱)$$

که در آن n_k و n_l ها مولفه‌های $\hat{n}$ هستند. با بسط سری نمایی، چرخشهای محدود به صورت زیر نمایش داده می شوند:

$$U(\hat{n},\theta) = e^{-i\frac{\theta}{2}\hat{n}.\vec{\sigma}} = I\cos\frac{\theta}{2} - i\hat{n}.\vec{\sigma}\sin\frac{\theta}{2} \qquad (۲۹-۱)$$

بیشتر ماتریسهای یکانی 2×2 با دترمینان 1 می توانند به این شکل بیان شوند. بنابراین می‌توان کیوبیت را به صورت حالتی از شی با اسپین $\frac{1}{2}$ در نظرگرفت، و هرتبدیل یکانی دلخواه که بر روی یک حالت اثر می کند، یک چرخش اسپین است. یک خاصیت ویژه نمایش $U(\hat{n},\theta)$، دو مقداری بودن آن است. به خصوص با یک چرخش به اندازه 2π حول هر محور به صورت زیر نمایش داده می شود:

$$U(\hat{n},\theta = 2\pi) = -1 \qquad (۳۰-۱)$$

این نمایش دو مقداری بودن چرخش اسپینور نامیده می شود. در حالی که این درست است که یک چرخش به اندازه 2π هیچ اثری بر روی یک شی با اسپین $\frac{1}{2}$ ندارد، ولی این اشتباه است که نتیجه بگیریم خاصیت اسپینور هیچ نتایج مشاهده‌پذیری ندارد. ماشینی را در نظر می‌گیریم که بر روی یک جفت اسپین اثر می کند. اگر اسپین اول بالا[1] باشد ماشین هیچ عملی انجام نمی دهد، اما اگر اسپین اول پایین[2] باشد، این ماشین اسپین دوم را به اندازه 2π می چرخاند. حال این ماشین بر روی اسپین اول که در یک ترکیب از اسپینهای بالا و پایین است اثر می‌کند، حال چه اتفاقی می‌افتد؟

---

[1] . up
[2] . down

نتیجه به صورت زیر است:

$$\frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_1+\left|\downarrow\right\rangle_1\right)\left|\uparrow\right\rangle_2 \rightarrow \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_1-\left|\downarrow\right\rangle_1\right)\left|\uparrow\right\rangle_2 \qquad (۳۱-۱)$$

در حالی که هیچ اثر قابل آشکاری برروی اسپین دوم وجود ندارد، حالت اول به یک حالت عمود بر هم تبدیل می شود که قابل مشاهده است.

سه مؤلفه تبدیل اندازه حرکت زاویه‌ای تحت چرخش به صورت یک بردار به صورت زیراست:

$$U\left(R\right)J_k U\left(R\right)^{\dagger}=R_{kl}J_l \qquad (۳۲-۱)$$

بنابراین اگر یک حالت $\left|m\right\rangle$ یک ویژه حالت J_3 باشد:

$$J_3\left|m\right\rangle=m\left|m\right\rangle \qquad (۳۳-۱)$$

پس $U(R)\left|m\right\rangle$ یک ویژه حالت RJ_3 با همان ویژه مقدار به صورت زیر است:

$$\begin{aligned} &RJ_3\left(U\left(R\right)\left|m\right\rangle\right)=U\left(R\right)J_3U\left(R\right)^{\dagger}U\left(R\right)\left|m\right\rangle \\ &=U\left(R\right)J_3\left|m\right\rangle=m\left(U\left(R\right)\left|m\right\rangle\right) \end{aligned} \qquad (۳۴-۱)$$

بنابراین می توان ویژه حالتهای اندازه حرکت زاویه‌ای را در امتداد محور $\hat{n}=\left(\sin\theta\cos\varphi,\sin\theta\sin\varphi,\cos\theta\right)$ با به کار بردن یک چرخش به اندازه θ، حول محور $\hat{n}'=\left(-\sin\varphi,\cos\varphi,o\right)$ با یک ویژه حالت J_3 ساخت. برای نمایش اسپین $\frac{1}{2}$ این چرخش به صورت زیر است:

$$\begin{aligned} &U(\hat{n}',\theta)=\exp\left[-i\frac{\theta}{2}\hat{n}'.\vec{\sigma}\right]=\exp\left[-i\frac{\theta}{2}(n_1'\sigma_1+n_2'\sigma_2+n_3'\sigma_3)\right]= \\ &=\exp\left[\frac{\theta}{2}\begin{pmatrix}0 & -e^{-i\varphi}\\ e^{i\varphi} & 0\end{pmatrix}\right]=\begin{pmatrix}\cos\frac{\theta}{2} & -e^{-i\varphi}\sin\frac{\theta}{2}\\ e^{i\varphi}\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix} \end{aligned} \qquad (۳۵-۱)$$

و با به کار بردن آن با $\begin{pmatrix}1\\0\end{pmatrix}$، ویژه حالت J_3 با ویژه مقدار 1، بدست می آوریم:

$$|\psi(\theta,\varphi)\rangle = \begin{pmatrix} e^{-i\frac{\varphi}{2}}\cos\frac{\theta}{2} \\ e^{i\frac{\varphi}{2}}\sin\frac{\theta}{2} \end{pmatrix} \qquad (۳۶-۱)$$

می‌توان مستقیماً بررسی کرد که $|\psi(\theta,\varphi)\rangle$ یک ویژه حالت $\hat{n}.\vec{\sigma}$ با ویژه مقدار ۱ است.

$$\begin{aligned} \hat{n}.\vec{\sigma} &= n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3 \\ &= \sin\theta\cos\varphi\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \sin\theta\sin\varphi\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + \cos\theta\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta & \sin\theta(\cos\varphi - i\sin\varphi) \\ \sin\theta(\cos\varphi - i\sin\varphi) & -\cos\theta \end{pmatrix} \qquad (۳۷-۱) \\ &= \begin{pmatrix} \cos\theta & \sin\theta e^{-i\varphi} \\ \sin\theta e^{i\varphi} & -\cos\theta \end{pmatrix} \end{aligned}$$

بنابراین با استفاده از معادله (۱-۱۳) با $a = e^{-i\frac{\varphi}{2}}\cos\frac{\theta}{2}$ و $b = e^{i\frac{\varphi}{2}}\sin\frac{\theta}{2}$ می‌توانیم آن را به صورت یک اسپین در جهت (θ,ϕ)نشان دهیم.

باید توجه داشت که تنها با یک اندازه‌گیری نمی‌توانیم a و b را تعیین کرد. حتی با چند کپی از حالت، نمی توان حالت را کاملاً با اندازه‌گیری هرکپی تنها حول محور z تعیین کرد. این کار فقط ما را قادر می سازد که $|a|$ و $|b|$ را تخمین بزنیم، اما چیزی درباره فاز نسبی a و b نمی‌دانیم. باید مؤلفه اسپین حول محور z را پیدا کنیم:

$$\langle\psi(\theta,\varphi)|\sigma_3|\psi(\theta,\varphi)\rangle = \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} = \cos\theta \qquad (۳۸-۱)$$

مسئله تعیین $|\psi\rangle$ به وسیله اندازه‌گیری، معادل تعیین بردار واحد $\hat{n}$ با اندازه گیری مؤلفه های آن حول محورهای گوناگون است. البته اندازه‌گیری حول سه محور متفاوت لازم است. از $\langle\sigma_1\rangle$ و $\langle\sigma_3\rangle$، n_1 و n_3 را تعیین می کنیم، اما n_2 همچنان غیر قابل تعیین می ماند.

اگرچرخش اسپین را ندیده بگیریم، اندازه‌گیری در امتداد محور $\hat{z}$ کافی خواهد بود. اندازه‌گیری یک اسپین درامتداد محور $\hat{n}$ معادل حالتی است که ابتدا محور $\hat{n}$ را حول محور $\hat{z}$ بچرخانیم، و سپس

درامتداد $\hat{z}$ اندازه‌گیری کنیم.

در یک حالت خاص $\theta = \frac{\pi}{2}$ و $\varphi = 0$ (محور $\hat{x}$) حالت اسپین به صورت زیراست: (اسپین بالا درامتداد محور x)

$$\left|\uparrow_x\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_z\right\rangle + \left|\downarrow_z\right\rangle\right) \qquad (۳۹-۱)$$

حالت عمود برآن به صورت زیر است (اسپین پایین درامتداد محور x):

$$\left|\downarrow_x\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_z\right\rangle - \left|\downarrow_z\right\rangle\right) \qquad (۴۰-۱)$$

برای هرکدام از این حالتها، اگر اسپین را در امتداد محور z اندازه بگیریم، $\left|\uparrow_z\right\rangle$ را با احتمال $\frac{1}{2}$ و $\left|\downarrow_z\right\rangle$ را هم با احتمال $\frac{1}{2}$ بدست خواهیم آورد. حال ترکیب زیر را در نظرمی‌گیریم:

$$\frac{1}{\sqrt{2}}\left(\left|\uparrow_x\right\rangle + \left|\downarrow_x\right\rangle\right) \qquad (۴۱-۱)$$

این حالت این خاصیت رادارد که اگر اسپین رادر امتداد محور x اندازه بگیریم، $\left|\uparrow_x\right\rangle$ یا $\left|\downarrow_x\right\rangle$ هر کدام را با احتمال $\frac{1}{2}$ بدست می آوریم. حال اگر حالت فوق را در امتداد محور z اندازه بگیریم چه اتفاقی می افتد؟

اگر این حالت بیتهای کلاسیکی باشند، پاسخ واضح است. حالت در معادله (۱-۴۱) دریکی از دو حالت است، و برای هرکدام ازاین دو حالت احتمال برای جهت بالا یا پایین در امتداد محور z برابر $\frac{1}{2}$ است.

اما برای کیوبیت‌ها این چنین نیست. با جمع کردن معادلات (۱-۳۹) و (۱-۴۰)، می بینیم که حالت معادله (۱-۴۱) واقعاً $\left|\uparrow_z\right\rangle$ است. وقتی که در امتداد محور z اندازه گیری می کنیم، همیشه $\left|\uparrow_z\right\rangle$ را پیدا می کنیم نه $\left|\downarrow_z\right\rangle$ را. برای کیوبیت‌ها، به صورت مخالف با حالت بیتهای کلاسیکی احتمالی، به راحتی می بینیم که احتمال می تواند در راه‌های مختلف جمع بسته شود. این پدیده مداخله کوانتومی نامیده می شود و یک رفتارمهم اطلاعات کوانتومی است.

۱-۴- ماتریس چگالی

۱-۴-۱- سیستم کوانتومی دو قسمتی:

دراین قسمت به سیستم های کوانتومی دو قسمتی می پردازیم. گام برداشتن ازیک کیوبیت به دو کیوبیت همان طور که انتظار می‌رود خیز بزرگی است. آنچه درباره‌ی مکانیک کوانتومی عجیب‌تر است این است که می توان مکانیک کوانتومی را به وسیله خواص فرض شده از حالت‌های کوانتومی دو کیوبیت بیان کرد. قواعد قسمت ۱-۲ یک فرمول بندی عمومی کاملاً قابل قبول از نظریه کوانتومی فراهم می کند. ولی تحت رویدادهای زیادی این قواعد با شکست مواجه می شوند. قصد نداریم سعی کنیم فیزیک تمام جهان اطراف را بفهمیم، ولی با مشاهده فقط گوشه کوچکی از جهان راضی هستیم. همیشه مشاهدات را به تکه کوچکی ازیک سیستم بزرگ محدود می کنیم. وقتی که توجه خود را به قسمتی از یک سیستم بزرگتر محدود کنیم پس در این صورت:

۱- حالتها پرتو نیستند.

۲- اندازه‌گیری‌ها تصویرهای متعامد نیستند.

۳- تحول یکانی نیست.

می‌توان این نکات را با در نظر گرفتن یک مثال ساده فهمید. ساده‌ترین مثال ممکن این است که یک جهان دو کیوبیتی داریم که فقط یکی از کیوبیت‌ها رامشاهده می کنیم.

یک سیستم دو کیوبیتی در نظر بگیرید که کیوبیت A به هر طریقی قابل مشاهده و اداره کردن است و به کیوبیت B دسترسی نداریم. بعضی ازحالات کوانتومی دوکیوبیت داده شده‌اند، می خواهیم یک راه پیدا کنیم که بتواند مشاهده‌ای را مشخص کند که بر روی کیوبیت A به تنهایی انجام شود.

از حالتهای $\{|0\rangle_A, |1\rangle_A\}$ و $\{|0\rangle_B, |1\rangle_B\}$ که به ترتیب پایه های متعامد کیوبیت A و B را مشخص می کنند استفاده خواهیم کرد. یک حالت کوانتومی دوکیوبیتی به شکل زیر در نظر بگیرید:

$$|\psi\rangle_{AB} = a|0\rangle_A \otimes |0\rangle_B + b|1\rangle_A \otimes |1\rangle_B \qquad (۴۲-۱)$$

دراین حالت کیوبیت‌های A و B به هم وابسته‌اند. فرض کنید می‌خواهیم کیوبیت A را با تصویر کردن بر روی پایه $\{|0\rangle_A,|1\rangle_A\}$ اندازه بگیریم. پس با احتمال $|a|^2$ نتیجه $|0\rangle_A$ رابدست می آوریم، و بـا یـک اندازه‌گیری حالت زیر را تهیه می‌شود:

$$|0\rangle_A \otimes |0\rangle_B \qquad (۴۳-۱)$$

و بااحتمال $|b|^2$ نتیجه $|1\rangle_A$ را بدست می آوریم و حالت زیر تهیه می شود:

$$|1\rangle_A \otimes |1\rangle_B \qquad (۴۴-۱)$$

درحالت دیگر، یک حالت از کیوبیت B به وسیله اندازه‌گیری انتخاب می شود. اگـر بعـداً کیوبیـت B را اندازه بگیریم و اگر $|0\rangle_A$ را پیدا کرده باشیم، مطمئناً بااحتمال یک، $|0\rangle_B$ را پیدا می کنیم و تضمین می کنیم که $|1\rangle_B$را پیـدا کنـیم اگـر $|1\rangle_A$را پیـدا کـرده باشـیم. بـه ایـن ترتیـب نتیجـه انـدازه‌گیـری $\{|0\rangle_A,|1\rangle_A\}$ و $\{|0\rangle_B,|1\rangle_B\}$ کاملاً به حالت ψ_{AB} مربوط است.

حال یک مشاهده پذیر عمومی کاملاً تصادفی که بر روی کیوبیت A عمل می‌کند را درنظر مـی‌گیـریم ونتیجه اندازه‌گیری را برای A به تنهایی مشخص می‌کنیم. یک مشاهده پذیر که فقط بر روی کیوبیـت A عمل می کند می‌تواند به صورت زیر بیان شود:

$$M_A \otimes I_B \qquad (۴۵-۱)$$

که M_A عملگر خودالحاقی عمل‌کننده بر روی A است و I_B اپراتـور یکـانی عمـل‌کننـده بـر روی B است. مقدار چشمداشتی مشاهده پذیر در حالت $|\psi\rangle$ به صورت زیراست:

$$\langle\psi|M_A \otimes I_B|\psi\rangle = \left(a^*{}_A\langle 0|\otimes_B\langle 0| + b^*{}_A\langle 1|\otimes_B\langle 1|\right)\left(M_A \otimes I_B\right)\left(a|0\rangle_A \otimes |0\rangle_B + b|1\rangle_A \otimes |1\rangle_B\right)$$
$$= |a|^2{}_A\langle 0|M_A|0\rangle_A + |b|^2{}_A\langle 1|M_A|1\rangle_A$$

(۴۶-۱)

(که از خاصیت تعامد $|0\rangle_B$و $|1\rangle_B$ استفاده کرده ایم). این نمایش را می‌توان دوباره به شکل زیرنوشت:

$$\langle M_A\rangle = tr\left(M_A\rho_A\right) \qquad (۴۷-۱)$$

$$\rho_A = |a|^2 |0\rangle_{A\,A}\langle 0| + |b|^2 |1\rangle_{A\,A}\langle 1| \qquad (۴۸-۱)$$

و tr(…) به معنی رد ماتریس است. عملگر ρ_A عملگر چگالی (یا ماتریس چگالی) برای کیوبیت A نامیده می شود و این عملگر خودالحاقی، مثبت (ویژه مقادیر آن نامنفی هستند) است و دارای رد واحد می‌باشد (چون $|\psi\rangle$ یک حالت نرمال است).

چون $\langle M_A \rangle$ برای هر مشاهده پذیر M_A که بر روی کیوبیت A عمل می‌کند به صورت معادله (۱-۴۷) است، بنابراین ρ_A نشان‌دهنده‌ی یک آنسامبل از حالتهای کوانتومی ممکن می‌باشد که هر یک با احتمال مشخص اتفاق می‌افتند. اگر کیوبیت A در یکی ازدو حالت کوانتومی باشد، باید دقیقاً نتیجه یکسان برای $\langle M_A \rangle$ بدست آوریم؛ کیوبیت A با احتمال $P_0 = |a|^2$ در حالت کوانتومی $|0\rangle_A$ و با احتمال $P_1 = |b|^2$ در حالت کوانتومی $|1\rangle_A$ است. اگر به نتیجه هر اندازه‌گیری ممکن علاقمند باشیم، می توانیم M_A را به صورت تصویر $E_A(a)$ در ویژه فضای مربوطه از مشاهده‌پذیر خاص درنظر بگیریم. آنگاه:

$$prob(a) = P_{0\,A}\langle 0|E_A(a)|0\rangle_A + P_{1\,A}\langle 1|E_A(a)|1\rangle_A \qquad (۴۹ -۱)$$

که همان احتمال بدست‌آوردن نتیجه a است که روی تمام آنسامبل جمع بسته شده است.

تاکید می‌کنیم که بین یک حالت حاصل از برهم‌نهش $|0\rangle_A$ و $|1\rangle_A$ با یک آنسامبل احتمالی که در آن $|0\rangle_A$ و $|1\rangle_A$ هر یک با احتمال مشخص رخ می‌دهند، تفاوت اساسی وجود دارد. برای مثال برای در اسپین $\frac{1}{2}$، اگر σ_1 را در حالت $\frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle + |\downarrow_z\rangle\right)$ اندازه بگیریم، نتیجه $|\uparrow_x\rangle$ را با احتمال یک بدست خواهیم آورد. اما آنسامبلی که در آن $|\uparrow_z\rangle$ و $|\downarrow_z\rangle$ هر کدام با احتمال $\frac{1}{2}$ اتفاق می افتند با عملگر چگالی زیر نشان داده می شود:

$$\rho = \frac{1}{2}\left(|\uparrow_z\rangle\langle\uparrow_z| + |\downarrow_z\rangle\langle\downarrow_z|\right) = \frac{1}{2} I \qquad (۵۰ -۱)$$

و تصویر بر $|\uparrow_x\rangle$ مقدار چشمداشتی زیر را دارد:

$$tr\left(\left|\uparrow_x\right\rangle\left\langle\uparrow_x\right|\rho\right)=\frac{1}{2} \qquad (۵۱ -۱)$$

در حقیقت می‌بینیم که هر حالت از یک کیوبیت نشان داده شده به وسیله یک پرتو، می‌تواند به صورت یک اسپین در بعضی جهات معلوم نشان داده شود. حالت $|\psi(\theta,\varphi)\rangle$ با به کار بردن یک تبدیل یکانی مناسب با $\left|\uparrow_z\right\rangle$ بدست می اید، برای ρ داده شده به وسیله معادله (۱- ۵۰) داریم:

$$tr\left(\left|\psi(\theta,\varphi)\right\rangle\left\langle\psi(\theta,\varphi)\right|\rho\right)=\frac{1}{2} \qquad (۵۲ -۱)$$

بنابراین اگر برای حالت $|\psi\rangle_{AB}$که در معادله (۱- ۵۳) تهیه شده است، با احتمال $|a|^2=|b|^2=\frac{1}{2}$ اسپین A را در امتداد هر محور اندازه بگیریم، یک نتیجه کاملاً تصادفی بدست می آوریم: اسپین بالا یا اسپین پایین هر کدام می تواند با احتمال $\frac{1}{2}$ رخ دهد.

بحث مربوط به حالت $|\psi\rangle_{AB}$ دو کیوبیتی به آسانی به یک حالت دلخواه از هر سیستم کوانتومی دو قسمتی (یک سیستم تقسیم شده به دو قسمت) تعمیم داده می‌شود. فضای هیلبرت یک سیستم دو قسمتی $H_A\otimes H_B$ است که $H_{A,B}$ فضاهای هیلبرت دو قسمتی هستند. این بدین معنی است که اگر $\{|i\rangle_A\}$ یک پایه اورتونرمال H_A و$\{|\mu\rangle_B\}$ یک پایه اورتونرمال H_B باشد، پس$\{|i\rangle_A\otimes|\mu\rangle_B\}$ یک پایه اورتونرمال $H_A\otimes H_B$است. بنابراین یک حالت خالص دلخواه $H_A\otimes H_B$ می تواند به صورت زیر بسط داده شود:

$$|\psi\rangle_{AB}=\sum_{i,\mu}a_{i\mu}|i\rangle_A\otimes|\mu\rangle_B \qquad (۵۳ -۱)$$

که $\sum_{i,\mu}|a_{i,\mu}|=1$. مقدار چشمداشتی یک مشاهده پذیر $M_A\otimes I_B$، که فقط روی یک زیرسیستم A عمل می کند به صورت زیر است:

$$\begin{aligned}\langle M_A\rangle &={}_{AB}\langle\psi|M_A\otimes I_B|\psi\rangle_{AB}\\ &=\sum_{j,\nu}a^*_{j,\nu}\left({}_A\langle j|\otimes{}_B\langle\nu|\right)(M_A\otimes I_B)\sum_{i,\mu}a_{i\mu}\left(|i\rangle_A\otimes|\mu\rangle_B\right)\end{aligned}$$

$$= \sum_{i,j,\mu} a^*_{j\mu} a_{i\mu\ A} \langle j | M_A | i \rangle_A$$
$$= tr(M_A \rho_A) \qquad (۵۴-۱)$$

که در آن :

$$\rho_A = tr_B \left(|\psi\rangle_{AB\ AB} \langle \psi| \right)$$
$$\equiv \sum_{i,j,\mu} a_{i\mu} a^*_{j\mu} |i\rangle_{A\ A} \langle j| \qquad (۵۵-۱)$$

عملگر چگالی ρ_A برای زیر سیستم A به وسیله انجام یک رد جزئی بر روی زیر سیستم B از ماتریس چگالی سیستم مرکب AB بدست می آید.

از تعریف معادله (۱- ۵۵) می توان به خصوصیات ρ_A پی برد که:

۱. ρ_A هرمیتی است. یعنی: $\rho_A = \rho_A^\dagger$.

۲. ρ_A برای هر $|\psi\rangle_{A\ A} \langle \psi|\rho_A|\psi\rangle_A = \sum_\mu \left| \sum_i a_{i\mu\ A} \langle \psi | i \rangle_A \right|^2 \geq 0$ مثبت است.

۳. $tr(\rho_A) = 1$. داریم $\rho_A = \sum_{i,\mu} |a_{i\mu}|^2 = 1$ چون $|\psi\rangle_{AB}$ نرمالیزه است.

در حالتی که حالت زیرسیستم پرتو است به حالت سیستم، خالص[1] می‌گوییم و در غیر این صورت حالت آمیخته[2] است. اگر حالت خالص $|\psi\rangle_A$ باشد، ماتریس های چگالی $\rho_A = |\psi\rangle_{A\ A} \langle \psi|$ تصویر بر روی فضای یک بعدی اندازه گرفته شده با $|\psi\rangle_A$ است. بنا براین یک ماتریس چگالی خالص دارای خاصیت $\rho^2 = \rho$ است. یک ماتریس چگالی عمومی در پایه هایی که قطری هستند به شکل زیر نشان داده می شود:

$$\rho_A = \sum_a P_a |\psi_a\rangle \langle_a \psi| \qquad (۵۶-۱)$$

که $0 < P_a \leq 1$ و $\sum_a P_a = 1$. اگر حالت خالص نباشد، بیشتر از دو یا چند قسمت در این جمع وجود دارد، و $\rho^2 \neq \rho$؛ در حقیقت $\rho^2 = \sum_a P_a{}^2 < \sum_a P_a = 1$. در این صورت می‌گوییم که ρ یک ترکیب نا همدوس از حالت های $\{|\psi_a\rangle\}$ است. نا همدوسی یعنی فازهای نسبی $|\psi_a\rangle$ به صورت

[1] .pure
[2] . mixed

ریاضی غیر قابل دسترس هستند.

چون مقدار چشمداشتی هرمشاهده پذیر M عمل‌کننده برروی زیرسیستم می‌تواند به صورت زیر بیان شود:

$$\langle M \rangle = tr(M\rho) = \sum_a P_a \langle \psi_a | M | \psi_a \rangle \qquad (۵۷-۱)$$

از قبل دیدیم که ممکن است ρ را به صورت توضیح یک آنسامبل حالت های کوانتومی خالص تفسیر کنیم، که در آن حالت $|\psi_a\rangle$ با احتمال P_a رخ می دهد. در مکانیک کوانتومی وقتی یک سیستم کوانتومی A با سیستم کوانتومی دیگرB برهمکنش دارد، فهمیدن اینکه چگونه احتمالات رخ می دهد خیلی سخت است. A و B وقتی که به هم مربوط باشند در هم تنیده می شوند. به این ترتیب درهم‌تنیدگی، همدوسی ترکیبی از حالت های A را خراب می کند. بنا براین اگر فقط به A توجه کنیم بعضی فازها در ترکیب غیر قابل دسترس می‌شوند. این امکان وجود دارد که این وضعیت را با گفتن اینکه حالتی از سیستم A متلاشی شده است توضیح داد.

۱-۴-۲- کره بلاخ :

اکنون حالتی از سیستم دوکیوبیتی A را که شکلی از ماتریس چگالی عمومی است در نظر می گیریم. بیشتر ماتریسهای 2×2 یکانی هرمیتی چهار پارامتر حقیقی دارند و می‌توانند در پایه های $\{I, \sigma_1, \sigma_2, \sigma_3\}$ بیان شوند. چون هر σ_i بدون رد است، ضریب I در بسط ماتریس چگالی ρ باید $\frac{1}{2}$ باشد (چون $tr(\rho)=1$) و ρ ممکن است به صورت زیر نشان داده شود:

$$\begin{aligned}
\rho(\vec{P}) &= \frac{1}{2}(I + \vec{P}.\vec{\sigma}) \\
&\equiv \frac{1}{2}(I + P_1\sigma_1 + P_2\sigma_2 + P_3\sigma_3) \\
&= \frac{1}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + P_1\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} + P_2\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} + P_3\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right] \qquad (۵۸-۱) \\
&= \frac{1}{2}\begin{pmatrix}1+P_3 & P_1 - iP_2\\ P_1 + iP_2 & 1 - iP_3\end{pmatrix}
\end{aligned}$$

که می توان $\det\rho=\frac{1}{4}(1-\vec{P}^2)$ را محاسبه کرد. بنابراین یک شرط ضروری برای اینکه ρ مقادیر ویژه نامنفی داشته باشد این است که $\det\rho\geq 0$ یا $P^2\leq 1$.

این شرط کافی است، چون $tr(\rho)=1$ و ممکن نیست که ρ دو مقدار ویژه منفی داشته باشد. بنابراین یک رابطه یک به یک بین ماتریس چگالی یک سیستم تک کیوبیتی و نقاط روی یک کره سه بعدی وجود دارد. این کره سه بعدی کره بلاخ نام دارد.

چون $tr(\rho)=1$ بنابراین این ماتریس چگالی باید مقادیر ویژه 1,0 داشته باشد. آنها تصویرگرهای یک بعدی هستند، و دراینجا حالتهای خالص هستند. از قبل می دانیم که هرحالت خالص تک کیوبیتی به صورت $|\psi(\theta,\varphi)\rangle$ است و می توان طوری تصور کرد که اسپین در جهت (θ,φ) باشد. با استفاده از خاصیت:

$$(\hat{n}.\vec{\sigma})^2=I \qquad (۵۹-۱)$$

که $\hat{n}$ یک بردار یکه است، به آسانی می توان تحقیق کرد که ماتریس چگالی حالت خالص زیر:

$$\rho(\hat{n})=\frac{1}{2}(I+\hat{n}.\vec{\sigma}) \qquad (۶۰-۱)$$

شرط:

$$(\hat{n}.\vec{\sigma})\vec{\rho}(\hat{n})=\rho(\hat{n})(\hat{n}.\vec{\sigma})=\rho(\hat{n}) \qquad (۶۱-۱)$$

را برآورده می‌کند.

بنابراین داریم:

$$\rho(\hat{n})=|\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)| \qquad (۶۲-۱)$$

که $\hat{n}$ در امتداد جهت اسپین بالا می باشد. همچنین از رابطه:

$$|\psi(\theta,\varphi)\rangle=\begin{pmatrix} e^{-i\frac{\varphi}{2}} & \cos\frac{\theta}{2} \\ e^{i\frac{\varphi}{2}} & \sin\frac{\theta}{2}\end{pmatrix} \qquad (۶۳-۱)$$

مستقیماً رابطه زیر را محاسبه می کنیم.

$$\begin{aligned}\rho(\theta,\varphi) &= |\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)| \\ &= \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{-i\varphi} \\ \cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{i\varphi} & \sin^2\frac{\theta}{2} \end{pmatrix} \\ &= \frac{1}{2}I + \frac{1}{2}\begin{pmatrix} \cos\theta & \sin\theta\, e^{-i\varphi} \\ \sin\theta\, e^{i\varphi} & -\cos\theta \end{pmatrix} \\ &= \frac{1}{2}(I + \hat{n}.\vec{\sigma})\end{aligned} \qquad (۶۴-۱)$$

چون داریم:

$$\cos^2\frac{\theta}{2} = \frac{1}{2}(1+\cos\theta)$$
$$\sin\frac{\theta}{2}\cos\frac{\theta}{2} = \frac{1}{2}\sin\theta$$

که در آن $\hat{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$ است. یک خاصیت خوب از پارامتریزه کردن کره بلاخ از حالت خالص، این است که در حالی که $|\psi(\theta,\varphi)\rangle$ یک فاز سرتاسر دلخواه دارد که از نظر فیزیکی مهم نیست، هیچ ابهامی در فاز ماتریس چگالی $\rho(\theta,\varphi) = |\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)|$ وجود ندارد، تمام پارامترها در ρ یک معنی فیزیکی دارند.

از خاصیت :

$$\frac{1}{2}tr\sigma_i\sigma_j = \delta_{ij} \qquad (۶۵-۱)$$

می بینیم که:

$$\langle\hat{n}.\vec{\sigma}\rangle_{\vec{P}} = tr(\hat{n}.\vec{\sigma}\rho(\vec{P})) = \hat{n}.\vec{P} \qquad (۶۶-۱)$$

بنابراین بردار $\vec{P}$ در معادله (۱-۵۸) پلاریزاسیون اسپین را پارامتریزه می‌کند. اگر سیستم های تهیه شده‌ی یکسان زیادی در دسترس وجود داشته باشد، می توانیم $\vec{P}$ را با اندازه‌گیری $\langle\hat{n}.\vec{\sigma}\rangle$ در امتداد هر یک از سه محور وابسته تعیین کنیم.

۱-۴-۳- تحول عملگر چگالی:

اکنون تحول زمانی حالات ترکیب شده را توضیح می دهیم. فرض کنید که هـامیلتونین یـک سیـستم خالص دو قسمتی در $H_A \otimes H_B$ شکل زیر را دارد:

$$H_{AB} = H_A \otimes I_B + I_A \otimes H_B \qquad (۶۷-۱)$$

با این فرض هیچ نوع جفت شدگی بین دو زیر سیستم A و B وجود ندارد. بنابراین هـر نتیجـه‌گیـری مستقل است. اپراتور تحول زمانی برای سیستم مرکب زیر:

$$U_{AB}(t) = U_A(t) \otimes U_B(t) \qquad (۶۸-۱)$$

به اپراتورهای تحول زمانی یکانی جداپذیر عمل کننده بر روی هر سیستم تجزیه مـی‌شـود. در تـصویر شرودینگر از دینامیک، یک حالت خالص پایه $|\psi(0)\rangle_{AB}$ از سیستم دو قسمتی که بـا معادلـه (۱-۵۳) داده می شود به معادله زیر ساده می شود:

$$|\psi(t)\rangle_{AB} = \sum a_{i\mu} |i(t)\rangle_A \otimes |\mu(t)\rangle_B \qquad (۶۹-۱)$$

که در آن روابط:

$$\begin{cases} |i(t)\rangle_A = U_A(t)|i(0)\rangle_A \\ |\mu(t)\rangle_B = U_B(t)|\mu(0)\rangle_B \end{cases} \qquad (۷۰-۱)$$

را به عنوان پایه های متعامد جدید بـرای H_A و H_B تعریـف مـی‌کنـیم. (چـون $U_A(t)$ و $U_B(t)$ یکـانی هستند.) با گرفتن رد جزئی به صورت قبل داریم:

$$\begin{aligned} \rho_A(t) &= \sum_{i,j,\mu} a_{i\mu} a^*_{j\nu} |i(t)\rangle_{A\,A}\langle j(t)| \\ &= U_A(t) \rho_A(0) U_A(t)^+ \end{aligned} \qquad (۷۱-۱)$$

بنابراین $U_A(t)$ تحول زمانی ماتریس چگالی را معین می کند.

به خصوص در پایه هایی که $\rho_A(0)$ قطری است، داریم:

$$\rho_A(t) = \sum_a P_a U_A(t) |\psi_a(0)\rangle_{A\,A}\langle\psi_a(0)| U_A(t) \qquad (۷۲-۱)$$

معادله (۱-۷۲) نشان می دهد که تحول ρ_A کاملاً با تفسیر آنسامبل سازگار است. هر حالت در آنسامبل در زمان تعیین شده به وسیله $U_A(t)$ نتیجه می شود. اگر حالت $|\psi_a(0)\rangle$ با احتمال P_0 در زمان صفر رخ دهد، $|\psi_a(t)\rangle$ با احتمال P_a در زمان بعدی t رخ می دهد. از طرف دیگر کاملاً واضح است که معادله (۱-۷۲) فقط وقتی که فرض کنیم سیستم A و B با هامیلتونی جفت شده نیستند، به کار می رود.

۱-۵- تجزیه اشمیت

یک حالت خالص دو قسمتی می تواند در یک شکل استاندارد که خیلی مفید است نشان داده شود که تجزیه اشمیت نام دارد.

برای دست یافتن به این شکل باید توجه کرد که یک بردار دلخواه در $H_A \otimes H_B$ می تواند به صورت زیر بسط داده شود:

$$|\psi\rangle_{AB} = \sum_{i,\mu} a_{i\mu} |i\rangle_A |\mu\rangle_B \equiv \sum |i\rangle_A |\tilde{i}\rangle_B \qquad (۱-۷۳)$$

در اینجا $\{|i\rangle_B\}, \{|i\rangle_A\}$ به ترتیب پایه های متعامد H_A و H_B هستند که برای بدست آوردن طرف دوم در رابطه (۱-۷۳) تعریف می کنیم:

$$|\tilde{i}\rangle_B \equiv \sum_{\mu} a_{i\mu} |\mu\rangle_B \qquad (۱-۷۴)$$

توجه شود که لازم نیست از ابتدا $|\tilde{i}\rangle_B$ متعامد یا نرمالیزه باشد.

فرض می کنیم که پایه های $\{|i\rangle_A\}$ طوری انتخاب شده‌اند که ρ_A درآن قطری باشد، یعنی داریم:

$$\rho_A = \sum_i P_i |i\rangle_{A\,A} \langle i| \qquad (۱-۷۵)$$

همچنین می توان ρ_A را با انجام یک رد جزئی محاسبه کرد:

$$\rho_A = tr_B\left(|\psi\rangle_{AB\,AB}\langle\psi|\right) =$$

$$= tr_B\left(\sum_{ij}|i\rangle_{AA}\langle j|\otimes|\tilde{i}\rangle_{BB}\langle\tilde{j}|\right)$$
$$= \sum_{ij}{}_B\langle\tilde{j}|\tilde{i}\rangle_B\left(|i\rangle_{AA}\langle j|\right) \qquad (۷۶-۱)$$

که تساوی فوق را با توجه به رابطه زیر بدست آوردیم:

$$tr_B\left(|\tilde{i}\rangle_{BB}\langle\tilde{j}|\right)=\sum_k{}_B\langle k|\tilde{i}\rangle_{BB}\langle\tilde{j}|k\rangle_B$$
$$=\sum_k{}_B\langle\tilde{j}|k\rangle_{BB}\langle k|\tilde{i}\rangle_B={}_B\langle\tilde{j}|\tilde{i}\rangle_B \qquad (۷۷-۱)$$

که $\{|k\rangle_B\}$ یک پایه متعامد برای H_B است. با مقایسه معادلات (۱-۷۵) و (۱-۷۶) می بینیم که:

$${}_B\langle\tilde{j}|\tilde{i}\rangle_B = P_i\delta_{ij} \qquad (۷۸-۱)$$

بنا براین ثابت شد که$\{|\tilde{i}\rangle_B\}$ها متعامد هستند. بردارهای متعامد را به صورت زیر می نویسیم:

$$|i'\rangle_B = P_i^{-\frac{1}{2}}|i\rangle_B \qquad (۷۹-۱)$$

(می‌توانیم فرض کنیم که $P_i \neq 0$، چون معادله فوق را فقط برای i های ظاهر شده در معادلـه (۱-۷۵) احتیاج داریم)، بنابراین بسط زیر را بدست می آوریم:

$$|\psi\rangle_{AB} = \sum_i\sqrt{P_i}|i\rangle_A|i'\rangle_B \qquad (۸۰-۱)$$

که برحسب پایه های متعامد ویژه H_A و H_B است. معادله فوق تجزیه اشمیت حالت خالص دو قسمتی $|\psi\rangle_{AB}$ است. هر حالت خالص دو قسمتی می تواند به این شکل بیان شود، اما پایه ها باید به حـا لـت خالص که بسط داده می شود، وابسته باشند. به طور همزمـان نمـی‌تـوان $|\psi\rangle_{AB}$ و $|\varphi\rangle_{AB}$ متعلـق بـه $H_A\otimes H_B$ را با استفاده از پایه های متعامد یکسان برای H_A و H_B به شکل معادله (۱-۸۰) بسط داد.

با استفاده از معادله (۱-۸۰) می توان رد جزئی روی H_A معین کرد تا بدست بیاوریم:

$$\rho_B = tr_A\left(|\psi\rangle_{AB\,AB}\langle\psi|\right)=\sum P_i|i'\rangle_{BB}\langle i'| \qquad (۸۱-۱)$$

می بینیم که ρ_A و ρ_B مقادیر ویژه غیر صفر یکسانی دارند.

به صورت کلی می توان تجزیه اشمیت را به صورت زیر بیان کرد:

اگر $|\psi\rangle_{AB}$ یک حالت خالص از سیستم مرکب AB باشد بـه طوریکـه $\{|i\rangle_A\}$ و $\{|i\rangle_B\}$بردارهـای پایـه متعامد آن باشند داریم:

$$|\psi\rangle_{AB} = \sum_i \lambda_i |i\rangle_A |i\rangle_B \qquad (۸۲-۱)$$

به طوریکه λ_i ها اعداد حقیقی مثبت هـستند و شـرط $\sum_i \lambda_i^2 = 1$ را بـرآورده مـی کننـد. ایـن اعـداد ضرایب اشمیت نام دارند.

۱-۵-۱- درهم تنیدگی:

به هر حالت $|\psi\rangle_{AB}$ خالص دو قسمتی می توان یک عدد صحیح مثبت بـه نـام عـدد اشـمیت مربـوط ساخت، که این عدد تعداد مقادیر ویژه غیر صفر در ρ_A (یا ρ_B) می باشد. بنابراین تعـداد جمـلات در تجزیه اشمیت بر حسب این عدد می باشد. برحسب این مقدار می تـوانیم درهـم تنیـدگی بـرای یـک حالت خالص دو قسمتی را تعریف کنیم. $|\psi\rangle_{AB}$ درهم تنیده (غیرقابل تفکیک) است اگر عدد اشـمیت λ بزرگتر از یک باشد، در غیر اینصورت حالت جداپذیر(قابل تفکیک) است.

بنابراین یک حالت خالص دو قسمتی جداپذیر یک حاصلضرب تانسوری مستقیم از حالتهای خالص در H_A و H_B است که به صورت زیر می باشد:

$$|\psi\rangle_{AB} = |\varphi\rangle_A \otimes |\chi\rangle_B \qquad (۸۳-۱)$$

بنابراین ماتریسهای چگالی تحـول یافتـه $\rho_A = |\varphi\rangle_{A\,A}\langle\varphi|$ و $\rho_B = |\chi\rangle_{B\,B}\langle\chi|$ خـالص هـستند. هـر حالت را که نتوان به صورت حاصلضرب تانـسوری مـستقیم نـشان داد، حالـت درهـم تنیـده اسـت، و ماتریس های چگالی ρ_A و ρ_B حالتهای آمیخته هستند.

یکی از اهداف اصلی ما درک بهتـر درهـم تنیـدگی اسـت. اگـر $|\psi\rangle_{AB}$ جداپـذیر باشـد، بـه صـراحت نمی‌توان گفت که زیر سیستم های A وB به هم وابسته نیستند. دو اسپین در حالت جدا پذیر زیر

$$|\uparrow\rangle_A |\uparrow\rangle_B \qquad (۸۴-۱)$$

مطمئناً به هم مربوطند. هر دو اسپین یک جهت یکسان دارند. اما ارتباط بین A وB در یک حالت درهم تنیده، با وقتی که در حالت جداپذیر هستند خصوصیات متفاوتی دارد. مهم‌ترین تفاوت این است که درهم تنیدگی نمی تواند به صورت منطقه‌ای ایجاد شود. تنها راه برای اینکه A وB درهم تنیده باشند این است که دو زیر سیستم مستقیماً با هم برهمکنش داشته باشند.

می توانیم معادله (۱-۸۴) را بدون اینکه اسپینهای A و B با هم برخورد کنند بدست آوریم. احتیاج داریم که یک پیام کلاسیکی به دو تهیه کننده اسپین (آلیس و باب) بفرستیم و به هر دو آنها بگوییم که یک اسپین در جهت محور Z تهیه کنند. اما تنها راه برای اینکه حالت معادله (۱-۸۴) را به یک حالت درهم تنیده مثل حالت زیر تبدیل کنیم:

$$\frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A|\uparrow\rangle_B+|\downarrow\rangle_A|\downarrow\rangle_B\right) \qquad (۱-۸۵)$$

این است که یک تبدیل یکانی پیوسته بر روی حالت به کار بریم. تبدیل یکانی موضعی به شکل $U_A\otimes U_B$، و اندازه‌گیری انجام شده به وسیله آلیس یا باب، نمی تواند عدد اشمیت حالت دو کیوبیتی را افزایش دهد، بدون اینکه چگونگی بحث و انجام آن توسط آلیس و باب اهمیت داشته باشد. با درهم تنیده کردن دو کیوبیت باید آنها را به هم برسانیم و اجازه دهیم تا با یکدیگر برهمکنش داشته باشند.

۱-۶- نکاتی درباره آنسامبل و ماتریس های چگالی

۱-۶-۱- تحدب:

ابتدا یادآوری می‌کنیم که عملگر ρ که در فضای هیلبرت اثر می‌کند، اگر خصوصیات زیر را داشته باشد عملگر چگالی است:

۱- ρ عملگر خودالحاقی باشد.

۲- ρ غیر منفی باشد.

۳- $tr(\rho)=1$.

اگر دو ماتریس چگالی ρ_1 و ρ_2 داشته باشیم می‌توانیم یک ماتریس چگالی دیگر که ترکیب خطی محدب آنها است ایجاد کنیم:

$$\rho(\lambda) = \lambda\rho_1 + (1-\lambda)\rho_2 \qquad (۸۶-۱)$$

این رابطه برای هر λ که شرط $0\leq\lambda\leq1$ را برآورده کند برقرار است. به راحتی می بینیم که $\rho(\lambda)$ دو شرط ۱ و۳ را برآورده می کند و فقط باید شرط ۲ را بررسی کنیم.

$$\langle\psi|\rho(\lambda)|\psi\rangle = \lambda\langle\psi|\rho_1|\psi\rangle + (1-\lambda)\langle\psi|\rho_2|\psi\rangle \geq 0 \qquad (۸۷-۱)$$

$\langle\rho(\lambda)|$ مطمئناً غیر منفی است، چون $\langle\rho_1|$ و $\langle\rho_2|$ غیر منفی هستند. بنابراین نشان دادیم که در یک فضای هیلبرت N بعدی H، عملگرهای چگالی یک زیر مجموعه محدب از فضای برداری حقیقی ماتریس های هرمیتی N×N است. (در صورتی به یک زیر مجموعه از یک فضای برداری محدب گفته می شود که مجموعه شامل بخش خطی مستقیم باشد که هردو نقطه در مجموعه را به هم ارتباط دهد.)

بیشتر عملگرهای چگالی می توانند به صورت یک مجموع از عملگرهای دیگر به راه‌های مختلف بیان شوند. اما حالات خالص ممکن نیست که به صورت یک جمع محدب از دو حالت دیگر بیان شوند.

یک حالت خالص $\rho = |\psi\rangle\langle\psi|$ در نظر بگیرید و $|\psi_\perp\rangle$ را یک بردار متعامد $|\psi\rangle$ بگیرید، $\langle\psi_\perp|\psi\rangle = 0$. فرض کنید ρ می‌تواند به صورت معادله (۱-۸۶) بسط داده‌شود داریم:

$$\langle\psi_\perp|\rho|\psi_\perp\rangle = 0 = \lambda\langle\psi_\perp|\rho_1|\psi_\perp\rangle + (1-\lambda)\langle\psi_\perp|\rho_2|\psi_\perp\rangle \qquad (۸۸-۱)$$

چون سمت راست تساوی مجموع دو جمله غیر منفی است و چون مجموع صفر است پس هر دو جمله باید صفر باشند. اگر λ مخالف صفر یا یک باشد، نتیجه می‌گیریم که ρ_1 و ρ_2 بر $|\psi_\perp\rangle$ عمود هستند اما چون $|\psi_\perp\rangle$ می‌تواند هر بردار عمود بر $|\psi\rangle$ باشد، نتیجه می گیریم که:

$$\rho_1 = \rho_2 = \rho \qquad (۸۹-۱)$$

بردارهایی در یک زیر مجموعه محدب که نمی‌توانند به صورت یک ترکیب خطی از دیگر بردارهای مجموعه بیان شوند، نقاط اکسترمال مجموعه نامیده می‌شوند. نشان می‌دهیم که فقط حالتهای خالص

نقاط اکسترمال مجموعه ماتریس‌های چگالی هستند. تنها حالت‌های خالص نقاط اکسترمال هستند، چون هر حالت آمیخته می‌تواند به صورت $\rho = \sum_i |i\rangle\langle i|$ در پایه هایی که قطری هستند نوشته شود، و بنابراین یک مجموع محدب از حالتهای خالص است.

این نوع ساختار را قبلاً در کره بلاخ دیدیم. عملگرهای چگالی یک کره در مجموعه سه بعدی از ماتریس های 2×2 با رد واحد هستند. کره مجموعه محدب است و نقاط روی مرز نقاط اکسترمال هستند. به طور مشابه عملگرهای چگالی N×N یک زیر مجموعه محدب از مجموعه ماتریس های هرمیتی (N^2-1) بعدی با رد واحد هستند و نقاط اکسترمال مجموعه حالتهای خالص هستند.

۱-۶-۲- تهیه یک آنسامبل:

تحدب مجموعه ماتریس های چگالی یک تفسیر فیزیکی ساده و روشن دارد. فرض می کنیم تهیه آنسامبل با تهیه یکی از دو حالت ممکن توافق داشته باشد. با احتمال λ حالت ρ_1 تهیه شده و با احتمال (1-λ) حالت ρ_2 تهیه شده است. با محاسبه مقدار چشمداشتی هر مشاهده پذیر M روی هر دو انتخاب، متوسط را حساب می کنیم و نتیجه اندازه‌گیری کوانتومی به صورت زیر است :

$$\begin{aligned}\langle M\rangle &= \lambda\langle M\rangle_1 + (1-\lambda)\langle M\rangle_2 \\ &= \lambda tr(M\rho_1) + (1-\lambda)tr(M\rho_2) \\ &= tr(M\rho(\lambda))\end{aligned} \qquad (۹۰-۱)$$

اگر حالت $\rho(\lambda)$ به جای آنها تهیه شود از آنچه که بدست می آوریم همه مقادیر چشمداشتی غیر قابل تشخیص هستند. بنابراین یک روش معلوم برای تهیه هر ترکیب محدب از حالتهای ρ_1 و ρ_2 داریم که روش شناخته شده برای تهیه ρ_1 و ρ_2 است. برای تهیه حالت آمیخته روشهای گوناگونی وجود دارد ولی برای تهیه هر حالت خالص یک روش وجود دارد. هر حالت خالص یک ویژه حالت از چند مشاهده پذیر است. یعنی برای حالت $\rho = |\psi\rangle\langle\psi|$، اندازه‌گیری تصویر $E = |\psi\rangle\langle\psi|$ تضمین می‌کند که نتیجه یک را داشته باشیم. چون ρ تنها حالتی است که نتیجه اندازه گیری E با احتمال ٪۱۰۰ یک باشد، هیچ راهی وجود ندارد که این خاصیت مشاهده پذیر را با انتخاب یکی از چند روش تهیه ممکن تولید

کند. بنابراین تهیه حالت خالص واضح است، اما تهیه یک حالت آمیخته مبهم است.

۱-۶-۳- علت ابهام در تهیه حالت آمیخته :

چون ρ می‌تواند به صورت یک مجموع از حالتهای خالص نشان داده شود توجه خود را به این سوال محدود می‌کنیم. یک عملگر چگالی در چند روش به صورت یک مجموع محدب از حالتهای خالص بیان می شود؟ یا به صورت ریاضی ρ در چند روش به صورت مجموعی از حالتهای اکسترمال نوشته می شود؟

یک حالت آمیخته از یک کیوبیت در نظر می‌گیریم:

$$\rho = \frac{1}{2} I \qquad (۹۱-۱)$$

در واقع این حالت می‌تواند به صورت یک آنسامبل از حالتهای خالص در راه های متنوع تهیه شود. برای مثال:

$$\rho = \frac{1}{2}\left|\uparrow_z\right\rangle\left\langle\uparrow_z\right| + \frac{1}{2}\left|\downarrow_z\right\rangle\left\langle\downarrow_z\right| \qquad (۹۲-۱)$$

بنابراین اگر هر یک از حالتهای $\left|\uparrow_z\right\rangle$ یا $\left|\downarrow_z\right\rangle$ را با احتمال $\frac{1}{2}$ تهیه کرده باشیم ρ را بدست می‌آوریم. اما همچنین داریم:

$$\rho = \frac{1}{2}\left|\uparrow_x\right\rangle\left\langle\uparrow_x\right| + \frac{1}{2}\left|\downarrow_x\right\rangle\left\langle\downarrow_x\right| \qquad (۹۳-۱)$$

وبنابراین اگر هر یک از حالتهای $\left|\uparrow_x\right\rangle$ یا $\left|\downarrow_x\right\rangle$ را با احتمال $\frac{1}{2}$ تهیه کرده باشیم ρ را بدست می‌آوریم. پس تهیه روش‌هایی که انکارناپذیر هستند متفاوت است، ولی هیچ راهی وجود ندارد که تفاوت را با مشاهده کردن اسپین بیان کند.

به طور عمومی تر، نقطه واقع در مرکز کره بلاخ مجموعی از هر دو نقطه متقاطر درون کره است، که تهیه حالتهای $\left|\uparrow_{\hat{n}}\right\rangle$ یا $\left|\downarrow_{\hat{n}}\right\rangle$ هر یک با احتمال $\frac{1}{2}$ رخ می دهد که $\rho = \frac{1}{2} I$ را تولید خواهد کرد.

تنها در حالتی که ρ دارای بیشتر از دو یا چند ویژه مقدار تبهگن باشد، راه‌های واضحی برای تولید ρ از یک آنسامبل حالتهای خالص متعامد دو طرفه وجود خواهد داشت. اما این دلیل خوبی نیست که توجه خود را به آنسامبل حالتهای خالص متعامد دو طرفه محدود کنیم. ممکن است ما یک نقطه درون کره بلاخ در نظر بگیریم :

$$\rho(\vec{P}) = \frac{1}{2}(I + \vec{P}.\vec{\sigma}) \qquad (۹۴-۱)$$

که $0 < \left|\vec{P}\right| < 1$ است. همچنین این رابطه می‌تواند به صورت زیر بیان شود:

$$\rho(\vec{P}) = \lambda\rho(\hat{n}_1) + (1-\lambda)\rho(\hat{n}_2) \qquad (۹۵-۱)$$

اگر $P = \lambda\hat{n}_1 + (1-\lambda)\hat{n}_2$ باشد. (به عبارت دیگر اگر $\vec{P}$ در هر مکانی بر روی خط ارتباط قرار بگیرد، نقاط $\hat{n}_1$, $\hat{n}_2$ بر روی کره‌اند.)

این ابهام بزرگ طبیعی در تهیه یک حالت کوانتومی آمیخته یکی از خصوصیات ویژه اطلاعات کوانتومی است که به شدت با توزیع احتمال کلاسیکی مغایرت دارد. مثلاً یک حالت از یک توزیع احتمال برای یک تک بیت کلاسیکی در نظر بگیرید. این دو توزیع اکسترمال به صورتی هستند که صفر یا یک هر کدام با احتمال ٪۱۰۰ رخ می دهد. هر توزیع احتمالی برای این بیت یک مجموع محدب از این دو نقطه اکسترمال است. به طور مشابه اگرN حالت ممکن وجود داشته باشد، N توزیع احتمال وجود دارد و هر توزیع احتمال یک تجزیه واحد به اکسترمال اول دارد.

۱-۶-۴- ارتباط سریعتر از نور:

حال به دیگاه قبلی که یک حالت مخلوط از سیستم A رخ می‌دهد چون A با سیستم B درهم تنیده است برمی‌گردیم، به علاوه مفاهیم تهیه مبهم حالتهای آمیخته را در نظر می‌گیریم. اگر کیوبیت A ماتریس چگالی زیر را داشته باشد:

$$\rho_A = \frac{1}{2}\left|\uparrow_z\right\rangle_{A\,A}\left\langle\uparrow_z\right| + \frac{1}{2}\left|\downarrow_z\right\rangle_{A\,A}\left\langle\downarrow_z\right| \qquad (۹۶-۱)$$

این ماتریس چگالی باید از یک حالت خالص دو قسمتی در هم تنیده $|\psi\rangle_{AB}$ بـا تجزیـه اشـمیت زیـر ایجاد شده باشد:

$$|\psi\rangle_{AB}=\frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle_A{}_A\langle\uparrow_z|+|\downarrow_z\rangle_A{}_A\langle\downarrow_z|\right) \qquad (۹۷-۱)$$

بنابراین شرح آنسامبل ρ_A در حالیکه $|\uparrow_z\rangle_A$ یا $|\downarrow_z\rangle_A$ هر یک با احتمال $\frac{1}{2}$ تهیه شده‌اند مـی‌توانـد با انجام یک اندازه‌گیری از کیوبیت B بدسـت بیایـد. کیوبیـت B را در پایـه $\{|\uparrow_z\rangle_B,|\downarrow_z\rangle_B\}$ انـدازه می‌گیریم؛ اگر نتیجه $|\uparrow_z\rangle_B$ بدست بیاید $|\uparrow_z\rangle_A$ را تهیه کرده ایـم و اگـر نتیجـه $|\downarrow_z\rangle_B$ بدسـت بیایـد $|\downarrow_z\rangle_A$ را تهیه کرده‌ایم.

اما در این حالت چون ρ_A مقادیر ویژه تبهگن دارد، پایه اشمیت یکتا نیست. همزمان می‌توانیم تبدیل یکانی را روی کیوبیتهای A و B (U را با A و U^* را با B) بدون اصلاح کردن حالت خالص دو قسمتی $|\psi\rangle_{AB}$ به کار بریم. بنابراین برای هر بردار سه بعدی واحد $\hat{n}$ و $|\psi\rangle_{AB}$ یک تجزیه اشـمیت بـه شـکل زیر دارد:

$$|\psi\rangle_{AB}=\frac{1}{\sqrt{2}}\left(|\uparrow_{\hat{n}}\rangle_A|\uparrow_{\hat{n}'}\rangle_B+|\downarrow_{\hat{n}}\rangle_A|\downarrow_{\hat{n}'}\rangle_B\right) \qquad (۹۸-۱)$$

می بینیم که با اندازه‌گیری کیوبیت B در یک پایه مناسب می‌توانیم هـر تفـسیر از ρ_A را بـه صـورت آنسامبلی از دو حالت خالص بفهمیم.

حال با دانستن این خاصیت مکانیسمی برای ارتباط سـریعتراز نـور پیـشنهاد مـی‌کنـیم. فـرض کنیـد کپی‌های زیادی از $|\psi\rangle_{AB}$ تهیه شده‌اند. فرض آلـیس همـه کیوبیتهـای A را بـه یـک کهکـشان دیگـر می‌برد و باب همه کیوبیتهای B را روی زمین نگه می‌دارد. وقتی که باب می‌خواهد یک پیام یک بیتی به آلیس بفرستد، یک مقیاس اندازه‌گیری σ_1 یا σ_3 را برای همه اسپینهایش انتخاب می‌کند. بنابراین اسپین های آلیس در یکی از آنسامبل هـای $\{|\uparrow_z\rangle_A,|\downarrow_z\rangle_A\}$ یـا $\{|\uparrow_x\rangle_A,|\downarrow_x\rangle_A\}$ تهیـه مـی شـوند. (U واقعی است بنابراین $U=U^*$, $\hat{n}=\hat{n}'$). برای خواندن پیـام آلـیس بلافاصـله اسـپین هـایش را

اندازه می گیرد تا ببیند که از آنسامبل تهیه شده می باشد. اما به راحتی عیب این طرح آشکار است. دو روش تهیه اسپینها مطمئناً تفاوت دارند، هر دو آنسامبل توسط ماتریس چگالی ρ_A یکسان توضیح داده شده‌اند. بنابراین هیچ اندازه‌گیری ممکنی وجود ندارد تا آلیس بتواند دو آنسامبل را تشخیص بدهد، و هیچ راهی برای آلیس وجود ندارد تا بگوید باب چه عملی را انجام داده است. پیام غیر قابل خواندن است. چرا دو روش تهیه که انجام شد متفاوتند؟ با تردید فرض کردیم که باب هر یک از دو کار زیر را انجام دهد:

۱. باب همه اسپینهایش را در امتداد محور $\hat{z}$ اندازه بگیرد.
۲. باب همه اسپینهایش را در امتداد محور $\hat{x}$ اندازه بگیرد.

باب سپس به آلیس با تلفن بین کهکشانی صحبت می کند. باب به آلیس نمی گوید که کار (۱) یا (۲) را انجام داده بود، اما به آلیس نتایج تمام اندازه‌گیریهایش را که مثلاً اسپین اول بالا و اسپین دوم پایین بود و یا غیره را می گوید. حال آلیس هر یک از کارهای (۱) یا (۲) را روی اسپین های خود انجام می دهد. اگر آلیس و باب هر دو در امتداد یک محور اندازه‌گیری کرده باشند، آلیس می فهمد که نتایج تک تک اندازه‌گیری هایش با آنچه که باب فرستاده است توافق دارد. اما اگر آلیس و باب در امتداد محورهای (متعامد) متفاوت اندازه‌گیری کنند، پس آلیس خواهد فهمید که هیچ ارتباطی بین نتایج او و باب نیست. حدود نیمی از اندازه‌گیری هایش با اندازه‌گیریهای باب توافق دارد و نیمی دیگر اینگونه نیست. اگر باب قول دهد که کار (۱) یا (۲) را انجام دهد و اندازه‌گیری هایش را به گونه‌ی دیگر انجام ندهد، پس آلیس متوجه می‌شود که عمل باب نسبت به عمل او متفاوت است (حتی اگر باب به او چیزی نگوید) و خیلی زود یکی از اندازه‌گیری های او مخالف با آنچه که باب انجام داده است می‌شود. اگر همه اندازه‌گیری هایشان با هم توافق داشته باشد، اگر اسپین های زیادی اندازه‌گیری شوند، آلیس با آمار خیلی بالا اطمینان خواهد داشت که او و باب در امتداد یک محور یکسان اندازه‌گیری کرده‌اند. بنابراین آلیس روشی را انجام می‌دهد تا دو روش تهیه اسپین باب را تشخیص دهد. اما دراین حالت مطمئناً ارتباط سریعتر از نور وجود ندارد. زیرا آلیس قبل از اینکه بتواند آزمون خود را انجام دهد، تلفن باب را دریافت می کند. [1, 2]

فصل دوم:

معرفی گیت‌های کلاسیکی و کوانتومی

معرفی گیت های کلاسیکی و کوانتومی

۲-۱- مقدمه

اطلاعات کامپیوتری اطلاعات پایه‌ای هستند که به صورت داده های دیجیتالی پردازش می شوند. برای پردازش این داده ها به یک کامپیوتر نیاز داریم که توسط مجموعه دستورالعمل هایی که برنامه نویسی نامیده می‌شوند، داده را پردازش کنند. داده های ورودی و خروجی برحسب واحدهای اساسی بیان می‌شوند که بیت نام دارد.

در کامپیوترهای کلاسیکی تمام اطلاعات به شکل رشته‌ای از متغیرهای ۰ و ۱ ذخیره می شوند و پردازش داده‌ها از هر نوع که باشد چیزی جز انجام اعمال منطقی روی این رشته ها نیست.

هر نوع پردازش اطلاعات یک سلسله توابع پشت سرهم است که روی یک رشته ورودی انجام می شود. تمام این توابع را می‌توان با ترکیب مقدماتی که تنها روی یک بیت یا دو بیت اثر می‌کنند ساخت، که هر کدام از این توابع مقدماتی را اصطلاحاً گیت می نامند.

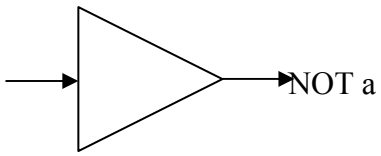
یک کامپیوتر الکترونیکی شامل صدها و هزارها میلیون گیت می باشد و هر کدام از این گیت ها فرآیند مربوط به خود را انجام می‌دهند. می‌توان گیت ها را همانند جعبه های سیاه کوچک با ورودی های خاص و خروجی های متناسب در نظر گرفت.

۲-۲ – گیت های کلاسیکی

گیت های کلاسیکی براساس تعداد ورودی ها طبقه بندی می شوند که شامل گیت های تک ورودی و گیت های دو ورودی هستند.

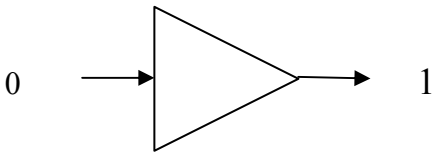
۲-۲-۱ – گیت های تک ورودی:

۱- گیت NoT:



این گیت مقدار ورودی را از ۰ به ۱ و بالعکس تغییر می دهد.

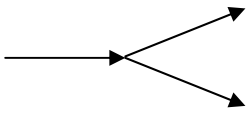
مثال :



$$NOT(0) = 1 \oplus 0 = \text{mod}\left(\frac{0+1}{2}\right) = 1 \qquad (۱-۲)$$

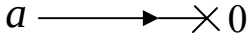
۲- گیت FANOUT (کپی) :

این گیت شامل یک ورودی و دو خروجی است که شاخه بیت ورودی را به دو شاخه بیت خروجی کـه حاصل دو بیت مشابه با بیت ورودی است، تبدیل می کند.



۳- گیت ERASE :

این گیت بیت ورودی را با صفر جایگزین می کند.



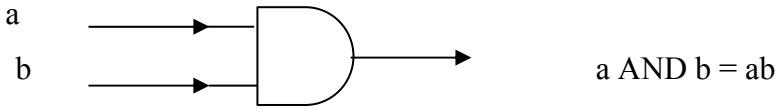
۲-۲-۲ – گیت های دو ورودی :

۱- گیت AND :

شامل دو ورودی و یک خروجی است، خروجی یک است تنها اگر هر دو ورودی یک باشند در غیر این صورت، خروجی برابر صفر می باشد.

عملیات ریاضی آن مانند حاصلضرب است.

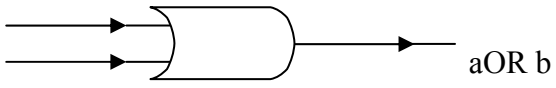
$$aANDb = ab \qquad (۲-۲)$$



شکل(۲-۱):گیت AND.

۲- گیت OR :

شامل دو ورودی و یک خروجی است. تنها اگر ورودی ها صفر باشند، خروجی صفر است و در غیر این صورت خروجی برابر یک خواهد شد.



شکل(۲-۲):گیتOR.

۳- گیت XOR :

گیت XOR با عملیات ریاضی زیر مشخص می شود.

$$aXORb = a \oplus b \qquad (۳-۲)$$

بنابراین خروجی برابر یک خواهد شد، اگر تنها یکی از ورودی ها صفر و دیگری یک باشد یعنی ورودی ها متفاوت باشند. در غیر این صورت خروجی صفر خواهد شد.

گیت های دو ورودی را می‌توان توسط جدول زیر نمایش داد:

جدول ۲-۱: نمایش گیت ورودی.

a	b	AND	OR	XOR
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

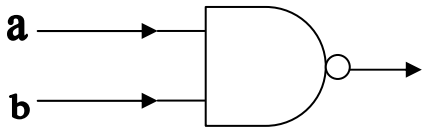
با استفاده از جدول فوق براحتی می‌توان نشان داد که:

$$aORb = (aANDb)XOR(aXORb) \qquad (۴-۲)$$

یعنی گیت OR به صورت ترکیبی از گیت های AND و XOR ساخته شود.

۴- گیت NAND:

این گیت شامل دو ورودی و یک خروجی است که عمل آن درست برعکس عمل گیت AND می باشد.

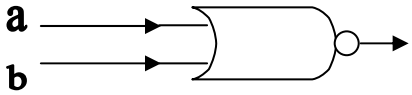


a NAND b= NOT(aANDb)

شکل (۲-۳):گیت NAND.

۵- گیت NOR:

این گیت هم برعکس گیت OR عمل می کند.



a NOR b= NOT(a OR b)

شکل (۲-۴):گیت NOR.

محاسبات کلاسیکی با استفاده از گیت های فوق انجام می شود اما جالب این جاست که بدانیم که برای محاسبات به همه گیت های فوق نیاز نداریم، چون می توان گیت های دیگر را از گیت های ERASE و FANOUT و NAND بدست آورد.

۲-۳ – محاسبات برگشت پذیر[1]

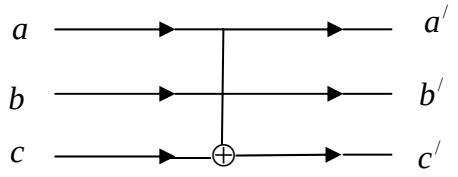
می توان ورودی گیت های FANOUT و NOT را از خروجی های گیت بدست آورد. در حالی که این عمل برای سایر گیت های کلاسیک امکان پذیر نمی باشد. می توان گفت که گیت های NOT و FANOUT برگشت پذیرند و تنها گیت های کلاسیکی برگشت پذیر می باشند. در گیت های برگشت ناپذیر کلاسیکی خروجی یک بیت کمتر از ورودی دارد.

در مقایسه گیت های کلاسیکی با گیت های کوانتومی بایدگفت که همه گیت های کوانتومی برگشت پذیر هستند. می توانیم گیت های کلاسیکی برگشت پذیر بسازیم که ایده اصلی این کار، کپی کردن تعدادی از بیت های ورودی به بیت های خروجی است.

با گیت Toffoli می توان گیت های برگشت پذیر کلاسیکی را شبیه سازی کرد.

۲-۳-۱ – گیت Toffoli :

این گیت شامل سه ورودی و سه خروجی است.



که $a' = a, b' = b, c' = c \oplus ab$.

چون $a = a', b = b'$, $c = c' \oplus a'b'$ بیت ورودی ممکن است با عقب برگشتن از بیت های خروجی ساخته شوند.

[1]- reversible

برای $c^{/}=0,b=c=0$ یک گیت Toffoli مانند گیت برگشت پذیر ERASE عمل می کند.

به ازاء $c^{/}=0,c=0,b=1$ مشابه گیت FANOUT عمل می کند.

و اگر b=1 و c=1 و $c^{/}=1\oplus a=NOTa$ که معادل با گیت NOT است.

به ازاء b=1 و $c^{/}=c\oplus a=aXORc$ یک گیت برگشت پذیر XOR را داریم.

و نهایتاً به ازا c=0 به $c^{/}=ab=aANDb$ مشابه گیت برگشت پذیرAND عمل می کند.

۲-۴ – گیت های کوانتومی

گیت های کوانتومی تبدیل کننده بیت های کوانتومی هستند درست مشابه گیت های کلاسیکی که بیت های کلاسیکی را تغییر می دهند.

مستلزم این عمل تحول زمانی سیستم کوانتومی است که برطبق قوانین مکانیک کوانتومی این عمل با عملگر یکانی توصیف می شوند. بنابراین هر گیت کوانتومی با یک عملگر یکانی U متناظر است.

چنانچه یک گیت کوانتومی روی یک حالت چند کیوبیتی اختیاری اثر کند ، داریم:

$$\left|\psi_{in}\right\rangle \rightarrow \left|\psi_{out}\right\rangle = U\left|\psi_{in}\right\rangle \qquad (۵-۲)$$

گیت های کوانتومی همیشه برگشت پذیر هستند و حالت های ورودی را می‌توان از حالت های خروجی بازسازی کرد.

هر تحول یکانی برگشت پذیر است بنابراین:

$$\left|\psi_{in}\right\rangle \rightarrow U^{\dagger}\left|\psi_{out}\right\rangle \qquad (۶-۲)$$

U عملگر یکانی است یعنی بزرگی و طول حالت را تغییر نمی دهد. بنابراین عملگر خطی و یکانی U به صورت یک گیت کوانتومی توصیف می شود که می تواند بر پایه های اصلی کیوبیت های منفرد $\left|0\right\rangle, \left|1\right\rangle$اعمال شود.

۲-۴-۱ – گیت های کوانتومی منفرد:

۱- گیت کوانتومی NOT (X):

مشابه گیت کلاسیکی NOT ، برای گیت کوانتومی NOT داریم:

$$|0\rangle \to |1\rangle, |1\rangle \to |0\rangle \qquad (۷-۲)$$

که ماتریس یکانی X را برای آن تعریف می کنیم:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (۸-۲)$$

که به صورت زیر عمل می کند:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad (۹-۲)$$

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

۲- گیت Z :

برای گیت Z در پایه های محاسباتی داریم:

$$|0\rangle \to |0\rangle \quad , \quad |1\rangle \to -|1\rangle \qquad (۱۰-۲)$$

که ماتریس یکانی آن به شکل زیر است:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad (۱۱-۲)$$

۳- گیت هادامارد[1] :

پایه های محاسباتی توسط عملگر گیت هادامارد به صورت زیر تعریف می شود :

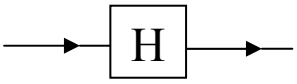
[1] . Hadamard gate

$$|0\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \qquad (۱۲-۲)$$

ماتریس متناظر یکانی آن به صورت زیر است :

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad (۱۳-۲)$$

عموماً گیت هادامارد را با نماد زیر نمایش می دهیم :

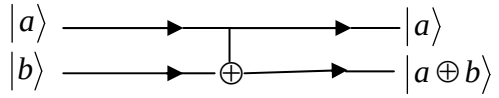


گیت Z و گیت H هیچ گونه مشابه کلاسیکی ندارند.

۲-۴-۲ – گیت های کوانتومی دوتایی:

۱- گیت CONTROLLED NOT (C-NOT):

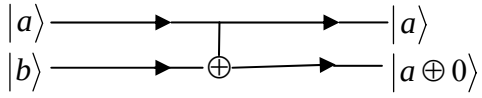
این گیت شامل دو کیوبیت ورودی است، کیوبیت ورودی بالایی را کیوبیت کنترل و کیوبیت ورودی پایین را کیوبیت هدف می نامند و نماد این گیت به شکل زیر است :



توجه شود که $a,b \in \{0,1\}$ هستند.

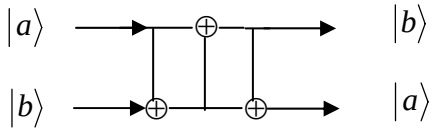
عمل ریاضی این گیت روی مدار فوق بیان شده است. ورودی هدف در صورتی که کنترل صفر باشد (a=0) تغییر نمی‌کند. اما اگر a=1 باشد، هدف تغییر می‌کند.

C-NOT یک گیت کوانتومی بسیار مهم است، اگر b=0 باشد گیت C-NOT به مانند کپی عمل می کند.



$$|a,o\rangle = |a\rangle|0\rangle = |a\rangle \otimes |0\rangle \xrightarrow{C-NOT} |a\rangle|a\rangle = |a,a\rangle \qquad (۱۴-۲)$$

یک نمونه از کاربردهای گیت C-NOT در زیر نشان داده شده است که یک جفت از بیت های کوانتومی را در پایه محاسباتی، عوض می کند.



عمل ریاضی این نمودار به صورت زیر انجام می شود.

$$|a,b\rangle \rightarrow |a,a \oplus b\rangle \rightarrow |(a \oplus b) \oplus a, a \oplus b\rangle$$

$$= |b,(a+b)\rangle = \rightarrow |b,b+(a+b)\rangle = |b,a\rangle \qquad (۱۵-۲)$$

بنابراین مکان a , b با هم عوض می شود.

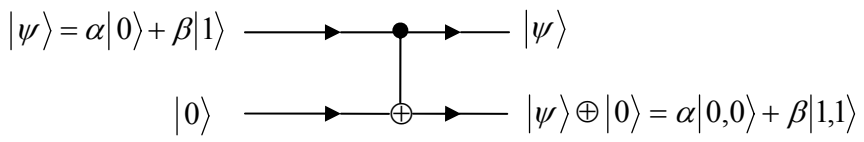
ماتریس یکانی متناظر با عملگر گیت C-NOT به صورت زیر بیان می شود.

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad (۱۶-۲)$$

اگر کیوبیت کنترل یک حالت کوانتومی کلی باشد به طوری که:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad , \quad \alpha^2 + \beta^2 = 1 \qquad (۱۷-۲)$$

و کیوبیت هدف $|0\rangle$ باشد طبق تعریف گیت C-NOT و با توجه به مدار زیر خواهیم داشت :



$$|\psi\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|0,0\rangle + \beta|1,0\rangle \xrightarrow{C-NOT(gate)} \alpha|0,0\rangle + \beta|1,1\rangle \qquad (۱۸-۲)$$

حال اگر کیوبیت هدف هم یک حالت کلی مانند $|\psi\rangle$ باشد :

$$|\psi\rangle|\psi\rangle = \alpha^2|0,0\rangle + \beta^2|1,1\rangle + \alpha\beta|0,1\rangle + \beta\alpha|1,0\rangle \qquad (۱۹-۲)$$

این در صورتی مشابه حالت پیش است که $\alpha = 0$ یا $\beta = 0$ باشد، یعنی اگر کیوبیت های ورودی، حالت های پایه محاسباتی باشد.

با این وجود نمی توان مدارها و گیت های پیچیده تر را برای کپی کردن یک حالت کوانتومی دلخواه به کار ببریم که این نتیجه به عنوان قضیه No-cloning مطرح می شود.

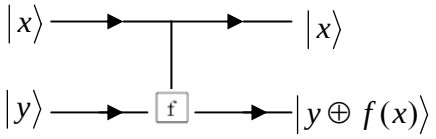
بنابراین قضیه کپی شدن برای حالت های پایه راست هنجار امکان پذیر است نه برای هر حالت کوانتومی دلخواه.

مثال:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|\psi\rangle = |0\rangle_x \qquad (۲۰-۲)$$

۲- گیت Function (f-gate)

گیت کوانتومی دوتایی مهمی دیگر است که شامل دو ورودی و دو خروجی است.



تعمیمی از گیت C-NOT است و مانند آن عمل می کند با این تفاوت که کیوبیت هـدف بـا تـابعی از کیوبیت کنترل ، مدول ۲ می شود.

$$f : \{0,1\} \to \{0,1\}$$
$$|x, y\rangle \to |x, y \oplus f(x)\rangle \qquad (۲۱-۲)$$

اگر f(x)= x باشد با گیت C-NOT متناظر است.

به ازای y= 0 خواهیم داشت:

$$|x,0\rangle \xrightarrow{f-gate} |x, f(x)\rangle \qquad (۲۲-۲)$$

اگر کیوبیت کنترل در حالت دلخواه $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$باشد نتیجه به صورت زیر است:

$$|\psi\rangle|10\rangle = \alpha|0,0\rangle + \beta|1,0\rangle \to \alpha|0, f(0)\rangle + \beta|1, f(1)\rangle \qquad (۲۳-۲)$$

هر کسی ممکن است فکر کند که گیت های کوانتومی شبیه گیت های کلاسیکی هستند. برای مثـال گیت هادامارد حالت $|0\rangle$را به $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ تبدیل می کند. که اندازه گیری این حالت هـر کـدام از مقادیر ۰ و ۱ را با احتمال $\frac{1}{2}$ مشخص می کند. این درست شبیه یک گیت کلاسیکی است که نتیجـه ۰ و ۱ را هر کدام با احتمال $\frac{1}{2}$ تولید می کند. به هر حال این تصور بـا بـه کـار بـردن دومـین گیـت هادامارد که حالت گذشته را با اطمینان به $|0\rangle$ تغییر خواهد داد، برطرف می شود.

عموماً حالت هادامارد $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ یک حالت خالص است که به وسیله ماتریس دانسیته $\frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$ در پایه محاسبات بیان می شود، چون خروجی گیت احتمال کلاسیک یک حالت آمیختـه بـا مـاتریس دانسیته $\frac{1}{2}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ است.

۲- ۵ – قضیه NO-Cloning

یکی از ویژگی های حالت های کوانتومی که مفاهیم تعمیمی را در محاسات کوانتومی به همراه دارد

قضیه No- Cloning می باشد. به این معنی که نمی‌توان از یک حالت کوانتومی E نشناخته، کپی گرفت و یا به عبارتی همانندسازی انجام داد که از نتایج خطی بودن مکانیک کوانتومی بدست می آید. برای اثبات آن کافی است که فرض کنیم که یک حالت را روی خودش نگاشت بدهیم در این صورت برای حالت دلخواه $|\psi\rangle$ داریم:

$$|\psi\rangle \to |\psi\rangle \otimes |\psi\rangle \qquad (۲۴-۲)$$

و همین طور برای حالت دلخواه $|\varphi\rangle$ هم بدست خواهیم آورد:

$$|\varphi\rangle \to |\varphi\rangle \otimes |\varphi\rangle \qquad (۲۵-۲)$$

چون تبدیل باید خطی باشد بنابراین به راحتی نشان داده می‌شود که:

$$|\psi\rangle \oplus |\varphi\rangle \to |\psi\rangle \otimes |\psi\rangle + |\varphi\rangle \otimes |\varphi\rangle \qquad (۲۶-۲)$$

از طرفی $|\psi\rangle + |\varphi\rangle$ را می شود معادل یک حالت کلی $|\chi\rangle$در نظر گرفت که طبق آن داریم:

$$\begin{aligned} &|\chi\rangle = |\psi\rangle + |\varphi\rangle \\ &\to |\chi\rangle \to |\chi\rangle \otimes |\chi\rangle = \big(|\psi\rangle + |\varphi\rangle\big) \otimes \big(|\psi\rangle + \varphi|\big) \end{aligned} \qquad (۲۷-۲)$$

با توجه به دو فرمول فوق داریم:

$$|\psi\rangle \otimes |\psi\rangle + |\psi\rangle \otimes |\varphi\rangle \neq \big(|\psi\rangle + |\varphi\rangle\big) \otimes \big(|\psi\rangle + |\varphi\rangle\big) \qquad (۲۸-۲)$$

بنابراین کپی کردن از $|\psi\rangle + |\varphi\rangle$ مردود اعلام می شود. درکل حالت های متعامد را جدا می کنیم ، می‌توان از حالت های پایه کپی بدست بیاوریم اما از بر هم نهی حالت های پایه نمی توان کپی برداشت.

در این صورت یا روی سیتم اولیه اندازه‌گیری خواهیم داشت که در این صورت برهم نهی از بین خواهد رفت، یا این که حالتی را تولید کنیم که حالت اولیه و کپی در هم تنیده می شود. [3, 4]

فصل سوم:

معرفی محاسبات کوانتومی

معرفی محاسبات کوانتومی

۳-۱- تعریف

همان طور که می دانیم می توانیم اعداد صحیح را بر حسب کیوبیت ها نمـایش دهـیم. فـرض کنیـد می‌خواهیم یک عدد صحیح بین صفر و ۷ را در یک رجیستر از کیوبیت ها بنویسیم. اگر این رجیـستر کلاسیکی باشد برای نوشتن این اعداد به سه بیت احتیاج داریم. در یک سیستم بر مبنای ۲ یک عـدد بین صفر و ۷ می تواند در نمایش در مبنای دو به صورت یک رشـته از سـه رقـم شـامل صـفر و یـک نمایش داده شود. یک رجیستر کلاسیکی که این اعداد را نشان می دهد یکی از ۸ پیکر بنـدی زیـر را در خود ذخیره خواهد کرد:

$$0=\{000\},1=\{001\},2=\{010\},...,7=\{111\} \qquad (۱-۳)$$

ولی دریک سیستم کوانتومی سـه کیـوبیتی یکـی از اعـداد صـفرتا ۷ بـه صـورت یـک حالـت ذخیـره می‌شوند.

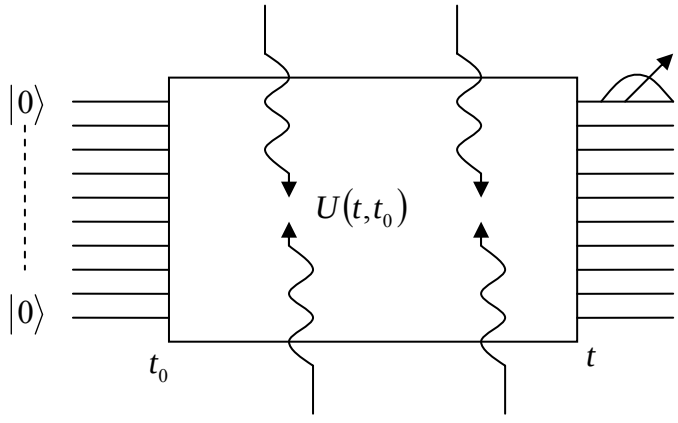
برای مثال: این اعداد به صورت ۸ حالت سه کیوبیتی زیر نشان داده می شوند.

$$0\equiv|000\rangle,1=|001\rangle,2=|010\rangle,3=|011\rangle,4=|100\rangle,5=|101\rangle,6=|110\rangle,7=|111\rangle \qquad (۲-۳)$$

در نمایش فوق نمایش ضرب تانسوری را حذف کرده‌ایم. برای مثال حالت $|101\rangle$ نمـایش سـاده شـده $|1_A\otimes 0_B\otimes 1_C\rangle$ است. که کیوبیتهای A، B و C به صورت یک بردار در فضای هیلبـرت $H_C, H_B. H_A$ هستند. از $|x\rangle$ که x =0, 1 , … , 7 است برای مشخص کردن یکـی از هـشت حالـت (۳-۲) اسـتفاده می‌کنیم. برای مثال $|101\rangle=|5\rangle$. تعمیم این نمایش به n کیو بیت سخت نیـست. نمـایش یـک عـدد کوچکتر از $N=2^n$ به n کیوبیـت نیـاز دارد و $|x\rangle$ یـک بـردار حالـت را بـا $0\le X\le 2^n-1$ مـشخص می‌کند.

پایه‌هایی از فضای هیلبرت $H^{\otimes n}$ که با استفاده از بردارهای $|x\rangle$ عمود بر هم ساخته شده اند، پایه‌های محاسباتی نامیده می شوند. چون ما می توانیم یک ترکیب خطی از هشت حالت (۳-۲)بسازیم، پس می‌توانیم نتیجه بگیریم که در یک زمان حالت‌های برداری یک سیستم سه اسپینی به ما اجازه می دهد $2^3=8$ عدد را ذخیره کنیم، در حالی که اگر n اسپین در فضای هیلبرت n بعدی استفاده شوند می توانیم 2^n عدد را در یک زمان ذخیره کنیم. اما اگر برای مثال اسپین های $\frac{1}{2}$ برای پشتیبانی فیزیکی از کیوبیت ها استفاده شده باشند، یک اندازه‌گیری از سه اسپین در طول محور O_Z لزوماً یکی از هشت حالت (۳-۲)را می دهد. اطلاعات مهمی را در دسترس داریم، اما وقتی که سعی می‌کنیم که آنها را عملی کنیم، نمی‌توانیم در یک اندازه‌گیری در یک سیستم کلاسیکی به بهترین شکل عمل کنیم. چون اندازه گیری فقط یکی از هشت حالت را به ما می دهد و همه را در یک زمان نمی دهد. بنابراین ضروری است که بیشتر کار کنیم تا احتمالات یک کامپیوتر کوانتومی را نتیجه بگیریم و الگوریتم هایی که برای آن مؤثر هستند را پیدا کنیم. حال ما توضیح طرح واری از اصول تابع کامپیوتر کوانتومی بیان می کنیم.

محاسبات انجام شده بر روی یک کامپیوتر کوانتومی به صورت طرح در شکل (۳-۱) نشان داده شده است.



شکل (۳-۱): طرح عمده از محاسبات کوانتومی . n کیوبیتی در حالت $|0\rangle$ فراهم شده اند. آنها تحت یک تحول یکانی در فضای $H^{\otimes n}$ از زمان $t=t_0$ تا زمان t بوسیله یک عملگر یکانی $u(t,t_0)$ در $H^{\otimes n}$ مشخص می شوند.

که n کیوبیت در زمان $t=t_0$ در حالت $|0\rangle$ تهیه شده‌اند. این مرحله آماده سازی سیستم کوانتومی است، و بردار حالت اولیه وابسته به یک فضای هیلبرت 2^n بعدی $H^{\otimes n}$ می باشد. این مرحله اولیه یک عملیات یونیتاری نیست. اما یک اندازه‌گیری تصویری و یک فرآیند اتلاف کننده است. کیوبیت‌ها تحت یک تحول کوانتومی یکانی بیان شده توسط یک عملگر یکانی $u(t,t_0)$ در فضای هیلبرت $H^{\otimes n}$ عمل می‌کنند که عملیات توضیح داده شده را انجام می دهد. برای مثال در یک تابع، مشکلات تجربی باعث دوری کردن از هر بر هم کنش با محیط می باشد، زیرا پدیده ناهمدوسی تحول یکانی را می‌سازد. همانطور که از قبل می‌دانیم، اگر یک بر هم کنش با محیط وجود داشته باشد، تحول یکانی در فضای هیلبرت اتفاق می افتد که از $H^{\otimes n}$ بزرگتر است، زیرا این شامل درجه آزادی محیط اطراف کیوبیت‌ها است. برهم کنش‌ها با میدان کلاسیکی خارجی با تحول یکانی سازگار هستند و آنها نیازمند این هستند که کیوبیت‌ها را با مهارت به وسیله نوسان Rabi اداره کنند. اولین تحول کوانتومی کامل شده یک اندازه‌گیری برروی کیوبیت‌ها (یا روی یک دسته از کیوبیت‌ها) درزمان t در مرتبه‌ای که محاسبات بدست می‌آیند می باشد. یک نکته مهم این است که حالت محاسبات نمی‌تواند در فاصله زمانی t_0 و t مشاهده شود، چون هر اندازه‌گیری ممکن است تحول یکانی را تغییر دهد: جعبه $u(t,t_0)$ ازشکل (۳-۱) یک جعبه سیاه است که نباید با آن مداخله کرد. کیوبیت‌ها در ورودی و خروجی اندازه‌گیری شده‌اند، اما داخل جعبه اندازه‌گیری نشده‌اند. نکته ضروری دیگر این است که تحول یکانی برگشت پذیر است؛ اگر ما بردار حالت را در زمان t بدانیم، ما می‌توانیم دوباره بردار حالت را در زمان t_0 با استفاده از $u^{-1}(t,t_0)=u(t_0,t)$ بدست بیاوریم.

۳-۲- محاسبات برگشت پذیر

عبور از حالت کیوبیت اولیه در $t=t_0$ به حالت کیوبیت نهایی در t توسط یک عملیات برگشت پذیر اتفاق می افتد، و الگوریتم های کامپیوتر کوانتومی حتماً باید برگشت پذیر باشند. این حالتی با الگوریتم های استفاده شده بر روی کامپیوترهای کلاسیکی که برگشت ناپذیرند نیست، و بنابراین بعداً نمی‌توانند مستقیماً باکامپیوترهای کوانتومی جابجا شوند. بیشتر گیتهای منطقی معمولی برگشت

ناپذیرند. زیرا آنها مربوط به یک تبدیل (۲ بیت ← ۱ بیت) هستند، و حالت نهایی یک حالت تک‌بیتی اجازه نمی دهد تا نمونه مطابق اصل از حالت دوبیتی اولیه انجام شود. برای مثال، گیت NAND

$$X \uparrow Y = 1 \oplus XY \qquad (۳-۳)$$

که $\oplus$ باقیمانده تقسیم بر ۲ است. نتیجه می دهد که:

$$(00) \to 1, (01) \to 1, (10) \to 1, (11) \to 0$$

و دانستن حالت نهایی اجازه نمی دهد که حالت ورودی دوباره ساخته شود. همانطور که می دانیم گیتهای NAND و COPY برای ساختن هر مدار منطقی مناسب هستند. یک سوال جالب این است که به هر حال همه عملیات های منطقی معمولی می توانند بر روی کامپیوترهای کلاسیکی به طور برگشت پذیر انجام شوند.

این سوال که در ابتدا فقط از لحاظ نظری جالب بود، در ابتدا توسط لانداور[۱] و بنت[۲] دو تن از دانشمندانی که بر روی این مسأله کار می‌کردند مطرح شد. آنها شگفت‌زده بودند که چگونه می‌توان یک محاسبه را بدون اتلاف انرژی انجام داد؟ در حقیقت، اطلاعات لزوماً به وسیله تعدادی پشتیبان فیزیکی حمل می شوند. بنت با استفاده از این تحقیق بعد از چند قرن سرانجام توانست یک حل رضایت‌بخش از پارادوکس ماکسول بدست بیاورد.

مطابق لانداور، یک عملیات شامل عملیات‌های برگشت ناپذیر شبیه اتلاف یک بیت اطلاعات در یک عملیات NAND، حداقل به اندازه‌ی یک آنتروپی ترمودینامیکی $K_B \ln 2$ بر بیت هزینه دارد. که K_B ثابت بولتزمان است $K_B = 1.38 \times 10^{-23} J/K$ و بنابراین منجر به اتلاف انرژی $\Delta E = K_B \ln 2$ در محیط می شود که T دمای مطلق کامپیوتر است. در حال حاضر این یک مسئله آکادمیک است. زیرا برای یک PC واقعی انرژی پراکنده شده به انرژی تولید شده، تقریباً $\Delta E \approx 500 K_B T$ است که واقعاً به علت مصرف الکتریکی است. و بنابراین ما هیچ کجا نزدک $K_B T$ نیستیم. اما، ممکن است که این پرسش از نظر اهمیت کاربردی بعضی وقتها در آینده پیش بیاید. انرژی پراکنده شده بر مبنای عملیات

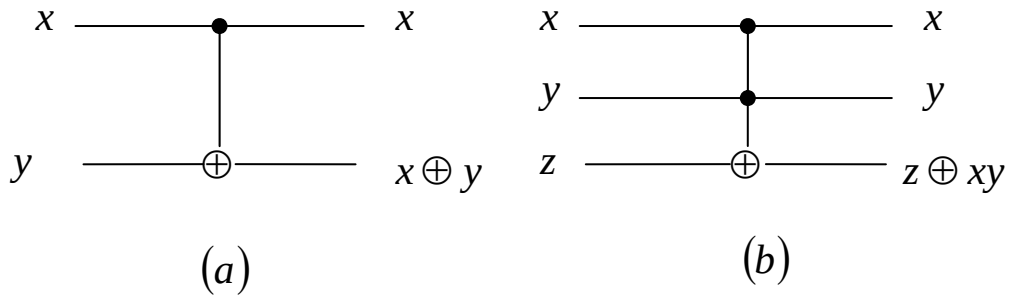
---

[1] .Landauer
[2] .Bennett

منطقی از نظربزرگی در طی ۵۰ سال به اندازه ده مرتبه کاهش داشته است، بنابراین ممکن است که K_BT محدود شده به ۱۰ یا ۱۵ سال مربوط باشد.

دلیل حقیقی برای جذابیت محاسبات برگشت پذیر امکان جابجایی الگوریتم های کلاسیکی، بامحاسبات کوانتومی است. به طوری که اشاره کردیم، جابجا کردن مستقیم امکان پذیر است، زیرا محاسبه کوانتومی برگشت پذیر است، و بنابراین عملیات NAND باید به وسیله یک عملیات برگشت پذیر معادل جایگزین شود.

همچنین ضروری است که معادل عملیات COPY بدون اینکه تضادی با قضیه no-cloning داشته باشد، وقتی که جابجایی نسخه کوانتومی گیتها را می سازد پیدا شود. این می تواند با استفاده از دو گیت اصلی انجام شود. گیت CNOT و گیت TOFFOLI (شکل (۳-۲)). اگر بیت هایی که به گیت Control-NOT (C-NOT) وارد می شوند (x,y) باشند، که x بیت کنترل و y بیت هدف[1] است. عمل گیت C-NOT روی بیت هدف به حالت بیت کنترل بر طبق طرح زیر وابسته است:



شکل (۳-۲): (a) گیت C-NOT . (b) گیت Toffoli نقطه سیاه بیتهای کنترل و دایره ها بیتهای هدف را نشان می دهند.

$$CNOT:(x,y)\rightarrow(x,x\oplus y) \qquad (۳-۳)$$

گیت C-NOT بیت x راکپی می کند اگر y=0 و اگر y=1 باشد به $\neg X$ می برد، و به طور برگشت پذیر معادل به عملیات copy است. این عمل برگشت پذیراست، چون یک رابطه یک به یک بین حالت اولیه و نهایی وجود دارد. عملیات C-NOT یک جایگشت ساده از بردارهای پایه است. (بخش۳-۴ را ببینید). این عمل می تواند بااستفاده از یک گیت تک بیتی نشان داده شود.

[1] . target

$$X \to 1 \oplus X \qquad \text{یا} \qquad X \to \neg X \qquad (۴-۳)$$

و گیت C-NOT، ممکن است فقط تابعهای خطی را ایجاد کند اگر ما خودمان را به عملیات های کلاسیکی محدود کنیم. اگر (x,y) و $(x^{/}, y^{/})$ بیتهای اولیه و نهایی باشند می‌توان نشان داد که:

$$\begin{pmatrix} x^{/} \\ y^{/} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \lambda \\ \mu \end{pmatrix} \qquad (۵-۳)$$

که $\alpha, \beta, ..., \mu$ ضرایب عددی هستند. ضروری است که یک گیت جمعی به نام گیت Toffoli معرفی کنیم که یک گیت با سه بیت ورودی و سه بیت خروجی است. دو تا از آنها بیتهای کنترل (x,y) ودیگری یک بیت هدف z است:

$$Toffoli : (x, y, z) \to (x, y, z \oplus xy) \qquad (۶-۳)$$

غیر خطی بودن گیت از عامل xy آشکار است. اگر z=1 باشد، گیت Toffoli عملیات NAND رابه طور برگشت پذیر انجام می دهد. گیت Toffoli می تواند با دوباره برگشت پذیر ساختن همه مدارهای منطقی کلاسیکی استفاده شود. گیت Toffoli یک گیت جهانی برای همه عملیات های منطق بولین است.

۳-۳- گیت‌های منطق کوانتومی

عموماً تحول کوانتومی یک تبدیل یکانی در فضای هیلبرت 2^n بعدی $H^{\otimes n}$ از n کیوبیت است. عموماً گیت منطق کوانتومی یک ماتریس $2^n \times 2^n$ یکانی است که در فضای هیلبرت $H^{\otimes n}$ عمل می کند. یک قضیه از جبر خطی که ما بدون اثبات آن را شرح می دهیم به ما اجازه می دهد که خودمان را به عملیات بر روی یک و دو کیوبیت محدود کنیم.

قضیه: هر تبدیل یکانی در $H^{\otimes n}$ می‌تواند به یک حاصلضرب ازگیتهای CNOT و تبدیلات یکانی بر روی یک کیو بیت تجزیه شود.

همان طور که قبلاً توضیح داده شد، یک عملیات بر روی کیوبیت منفرد نمی‌تواند یک تبدیل یکانی عمومی از $H^{\otimes n}$ تولید کند زیرا هر عملیات یک شکلی از حاصلضرب تا نسوری دارد.

$$U = U^{(1)} \otimes U^{(2)} \otimes ... \otimes U^{(n)} \qquad (۷-۳)$$

ضروری است که عملیات غیر بدیهی بر روی حداقل دو کیوبیت انجام دهیم تا یک تبدیل یکانی عمومی بدست آوریم. قضیه فوق تضمین می‌کند که این کار مناسب است. این قضیه یک قضیه حیاتی است. و عموما راه آسانتر این است که گیتهای منطق کوانتومی برای یک مسئله داده شده، بدون استفاده از این قضیه آشکارا تولید شوند. نمایش گیت C-NOT به صورت ماتریس 4×4 مفید است. عملیات C-NOT بر حسب کیوبیت‌ها مربوط می شود به تبدیل:

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle$$

در پایه های $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ نمایش ماتریسی به صورت زیراست:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix} \qquad (۸-۳)$$

دراین شکل واضح است که C-NOT نمی تواند یک حاصلضرب تا نسوری باشد. تعمیم یافته گیت C-NOT گیت Control –U(CU) است. که ماتریس σ_x به وسیله یک ماتریس U یکانی 2×2 جایگزین می شود.

$$CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} \qquad (۹-۳)$$

گیت CU بیت هدف را اگر x=0 بدون تغییر رها می کند و اگر x=1 باشد. آن را به صورت

$$|y\rangle = U|y\rangle \qquad (۱۰-۳)$$

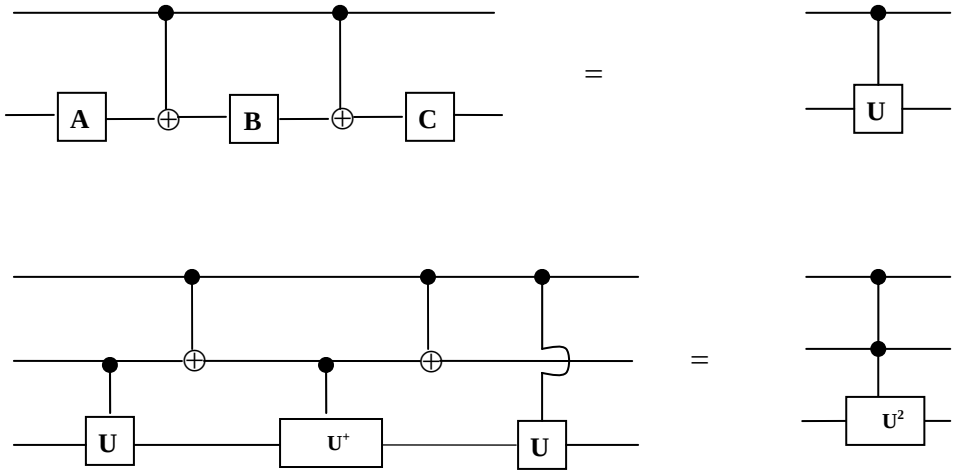
تغییر می دهد. گیت CU می‌تواند با شروع از گیت C-NOT تولید شود (شکل (۳-۳)).

ضروری است که سه عملگر A، B و C یکانی را به شکل زیر پیدا کنیم:

$$\text{CBA=I} \quad , \qquad C\sigma_x B\sigma_x A = U \qquad (۱۱-۳)$$

در فیزیک کوانتومی گیت Toffoli ممکن است از گیتهای CU و گیتهای CNOT (شکل (۳-۳) با $(U = \sqrt{\sigma_x})$ و معادله زیر تولید شود:

$$\sqrt{\sigma_x} = \frac{1}{1+i}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

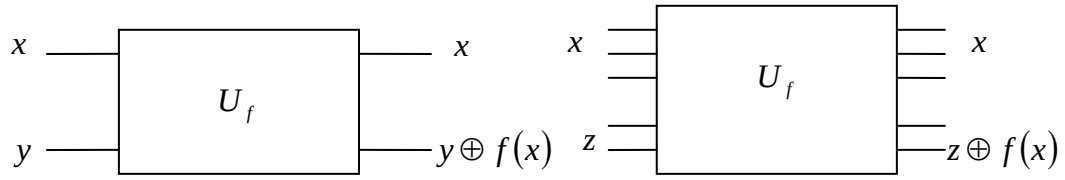


شکل (۳-۳): ساختن گیت CUو گیت Toffoli. نمودارها از چپ به راست خوانده می شوند و حاصلضرب عملگرها از راست به چپ عمل می کند.

که درفیزیک کلاسیک ممکن نیست، چرا که عملیات $\sqrt{\sigma_x}$ وجود ندارد. در مقابل حالت کلاسیکی ضروری نیست که گیت Toffoli رابه طور آشکار با تولید کردن آنسامبلی از مدارهای منطقی برگشت پذیر معرفی می کنیم. از نتیجه بخش ۳-۲ می بینیم که اگر یک مدار منطقی کلاسیکی در دسترس داشته باشیم اجازه می دهد که یک تابع f(x) محاسبه شود. پس می‌توانیم بر حسب نیاز یک مدار کوانتومی به تعداد گیت‌ها تولید کنیم.

حال می‌دانیم که یک مدار منطقی کوانتومی وجود دارد که می‌تواند یک تابع f(x) را ارزیابی کند، برای مثال، با جابجا کردن یک الگوریتم کلاسیکی، می توانیم ایده های اساسی هم ارزی کوانتومی (توازی کوانتومی) را قرار دهیم. از دو رجیستر استفاده خواهیم کرد. یک رجیستر ورودی که بیتهای مورد نیازX را ذخیره می کند و یک رجیستر خروجی که بیتهای مورد نیاز f(x) را ذخیره می کند. برای ساده شدن بحث، با حالتی که رجیستر ورودی یک رجیستر تک بیتی است شروع می کنیم، به طوری که رجیستر خروجی هم تک بیتی است. یک تبدیل U_f (شکل (۳-۴)) می سازیم که عملیات زیر را انجام دهد.

$$(x,y)\overset{U_f}{\rightarrow}(x,y\oplus f(x)) \qquad (۱۲-۳)$$



شکل (۳-۴): ساخت U_f : (a) 2 کیو بیتی. (b) (n+m) کیوبیتی.

اگر مقدار اولیه y=0 باشد. به طور خلاصه داریم:

$$(x,0)\xrightarrow{U_f}(x, f(x))$$

یک سوال وجود دارد که چرا به سادگی تبدیل $x \to f(x)$ را انجام نمی‌دهیم. پاسخ این است که اگر رابطه بین x و f(x) یک به یک نباشد، تبدیل نظیر نمی تواند یکانی باشد. و بنابراین برای یک الگوریتم کوانتومی مناسب نیست. برعکس این آسان است که خودمان را قانع کنیم که U_f یکانی است, زیرا یک اتحاد مربع است.

$$\left(x,[y \oplus f(x)]\right)\xrightarrow{U_f}\left(x,[y \oplus f(x)] \oplus f(x)\right) = (x,y) \qquad (۱۳-۳)$$

به علت اینکه برای هر $f(x) \oplus f(x) = 0, f(x)$ است. عملیات U_f یک بردار پایه را به دیگری تبدیل می کند. چون $U_f^2 = I$ این ارتباط فقط می تواند یک تغییر جایگشت چهار بردار پایه باشد، و بنابراین یک تبدیل یکانی است. در نماد گذاری عملگری:

$$U_f|x \otimes 0\rangle = |x \otimes f(x)\rangle, U_f|x \otimes y\rangle = |x \otimes [y \oplus f(x)]\rangle \qquad (۱۴-۳)$$

اجازه دهید تا حالت $|0\rangle_x$ را با یک گیت هادامارد H به کار بریم.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad (۱۵-۳)$$

یا

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

حال اگر کیوبیت دوم در حالت $|0\rangle$اولیه باشد بردار حالت نهایی دو کیوبیت، حالت جفت شده زیراست:

$$|\psi\rangle = U_f |H0 \otimes 0\rangle = U_f \frac{1}{\sqrt{2}}\left(|0 \otimes 0\rangle + |1 \otimes 0\rangle\right) = \frac{1}{\sqrt{2}}\left(|0 \otimes f(0)\rangle + |1 \otimes f(1)\rangle\right) \quad (۱۶-۳)$$

بردار حالت $|\psi\rangle$ اطلاعات بر روی f(0) و f(1) را همزمان در بردارد، و محاسبات بردار $|\psi\rangle$ نیازمند تعدادی عملیات به صورت $U_f|0 \otimes 0\rangle$ یا $U_f|1 \otimes 0\rangle$ به طور جداگانه است: U_f یک عملگر یکانی است که به حالت برداری به کار رفته وابسته نیست.

۳-۴- الگوریتم دوچ[1]

همانطورکه گفتیم $|\psi\rangle$ در معادله (۳-۱۶) اطلاعات بر روی f(0) و f(1) را همزمان دربر دارد، اما اگر بخواهیم یک جدول از مقادیر معلوم f(x) بسازیم، این کاربر روی یک کامپیوتر کلاسیکی هیچ فایده‌ای ندارد. اما ممکن است این اتفاق بیافتد که فقط به اطلاعاتی احتیاج داشته باشیم که نیاز به ساختن جدول مورد نظر نباشد. پس ممکن است که یک الگوریتم کوانتومی بتواند طوری رفتار کند که اطلاعات موجود در $|\psi\rangle$ نتایج را با استفاده از عملیات کمتری از یک الگوریتم کلاسیکی بدست آورد. چگونگی این کار را توضیح خواهیم داد.

برای مثال: الگوریتم دوچ می تواند با استفاده از مدار شکل (۳-۵) با رجیسترهای ورودی و خروجی یک کیوبیتی درک شود. تابع نامعلوم f(x) دو مقدار 0 یا 1 را می گیرد و می توانیم سوال زیر را مطرح کنیم. آیا f(0)=f(1) راداریم (یک تابع ثابت) یا $f(0) \neq f(1)$ (یک تابع بالانس شده)را داریم؟ اگر از یک الگوریتم کلاسیکی استفاده می کردیم، باید f(0) و f(1) را محاسبه می کردیم و دو مقدار را با هم مقالیسه کنیم. اما اگر از یک کامپیوتر کوانتومی استفاده کنیم، این سوال می تواند در یک تک عملیات پاسخ داده شود. یک مسئله معادل این بررسی سکه است: آیا دو طرف متفاوتند یا آنها یکسان هستند؟ کامپیوتر کوانتومی اجازه می‌دهد که این مقایسه را بدون نگاه کردن به دو طرف سکه در تکرار انجام دهیم. این مثال البته برای هر کاربرد مقدماتی جالب است، اما ساده ترین مثال توازی کوانتومی است.

[1] .Deutch

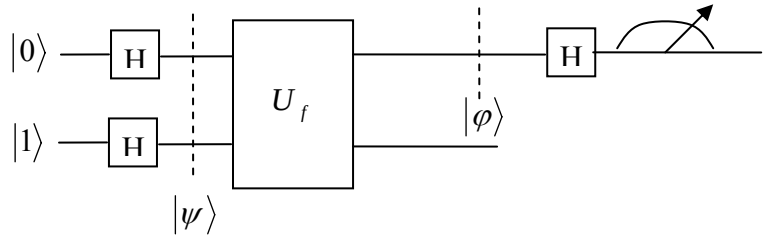
مدار شکل (۳-۵) حالت $|\psi\rangle$را در ورودی جعبه U_f دارد، رجیستر ورودی در ابتدا در حالت $|0\rangle$ و رجیستر خروجی در حالت $|1\rangle$ قرار دارند.

$$|\psi\rangle=(H|0\rangle)\otimes(H|1\rangle)=\frac{1}{2}(|0\rangle+|1\rangle)\otimes(|0\rangle-|1\rangle)=\frac{1}{2}\left(\sum_{x=0}^{1}|x\rangle\right)\otimes(|0\rangle-|1\rangle) \qquad (۱۷-۳)$$

U_f در (۳-۱۶)را در این حالت به کار می بریم که نتیجه زیر رامی دهد:

۱. اگر $f(x)=0\Rightarrow(|0\rangle-|1\rangle)\rightarrow(|0\rangle-|1\rangle)$

۲. اگر $f(x)=1\Rightarrow(|0\rangle-|1\rangle)=(|1\rangle-|0\rangle)\rightarrow(|0\rangle-|1\rangle)$



شکل (۳-۵):الگوریتم دوچ

یا به طور خلاصه:

$$(|0\rangle-|1\rangle)\rightarrow(-1)^{f(x)}(|0\rangle-|1\rangle) \qquad (۱۸-۳)$$

حالت $U_f|\psi\rangle$ حاصلضرب تانسوری زیر است:

$$U_f|\psi\rangle=\frac{1}{2}\left(\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle\right)\otimes(|0\rangle-|1\rangle) \qquad (۱۹-۳)$$

نتیجه خالص برای رجیستر ورودی به صورت زیر است:

$$|x\rangle\xrightarrow{U_f}(-1)^{f(x)}|x\rangle \qquad (۲۰-۳)$$

در این حالت خاص جعبه U_f یک پیشگو[1] نامیده می شود. توجه شود که رجیسترهای ورودی و خروجی بعد از پیشگویی غیر جفت شده هستند. حالتی از کیوبیت رجیستر ورودی به صورت زیراست:

$$|\Phi\rangle=\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle\right) \qquad (۲۱-۳)$$

[1] . oracle

قبل از اندازه‌گیری رجیستر ورودی، یک گیت هادامارد رابه کار می بریم (شکل (۳-۵) را ببینید):

$$H|\varphi\rangle = \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)\right] = \\ = \frac{1}{2}\left[(-1)^{f(0)} + (-1)^{f(1)}\right]0\rangle + \frac{1}{2}\left[(-1)^{f(0)} - (-1)^{f(1)}\right]1\rangle \qquad (۲۲-۳)$$

اگر اندازه‌گیری کیوبیت $|0\rangle$ را بدهد، پس f(0)=f(1) ، یعنی تابع در ابتدا ثابت است. اگر $|1\rangle$ را بدهد، پس $f(0) \neq f(1)$ و تابع در ابتدا بالانس شده است. یک نکته مهم این است که توازی کوانتومی اجازه می دهد که محاسبات صریح تابع f(x) راکنار بگذاریم و اندازه‌گیری یک تک کیوبیت دو نتیجه ممکن را در بردارد. این روش را می‌توان به چند کیوبیت تعمیم داد.

۳-۵- تعمیم به n+m کیوبیت

بحث فوق می‌تواند به یک رجیستر ورودی n کیوبیتی و یک رجیستر خروجی m کیوبیتی تعمیم داده شود که m تعداد بیتهای مورد نیاز برای نوشتن f(x) است. برای مثال برای رجیستر ورودی n=3 قرارمی دهیم. با استفاده از نماد گذاری $|x\rangle$ که x یکی از هشت عدد (در مبنای دو) زیر است:

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle. |101\rangle, |110\rangle, |111\rangle \qquad (۲۳-۳)$$

ترفند خاص یک کامپیوتر کوانتومی این است که می‌توان یک ترکیب خطی از بردارهای پایه محاسباتی با استفاده از اپراتور H ساخت که در حالت خاص n=3 داریم:

$$|\Psi\rangle = H^{\otimes 3}|000\rangle = \frac{1}{\sqrt{8}}\sum_{x=0}^{7}|x\rangle \qquad (۲۴-۳)$$

که $H^{\otimes 3}$ ضرب تانسوری سه اپراتور H را مشخص می کند. به طور عمومی

$$H^{\otimes n}\left|0^{\otimes n}\right\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}x \qquad (۲۵-۳)$$

که x نماد فشرده برای نمایش در مبنای دو عدد x و بردار حالت پایه محاسباتی $|x\rangle = |x_{n-1}...x_1x_0\rangle$ است، که $x_{n-1},...,x_1,x_0$ مقادیر 0 یا 1 را می‌گیرند. اپراتور U_f با استفاده از تعمیم رابطه (۳-۱۴) به

صورت شکل (۳-۴)(b) تعریف می‌شود:

$$U_f \left| x \otimes z \right\rangle = \left| x \otimes \left[z \oplus f\left(x\right) \right] \right\rangle \qquad (۲۶-۳)$$

که $\oplus$ باقیمانده بر ۲ بدون انتقال به صفحه بعد است، برای مثال:

$1101 \oplus 0111 = 1010$

به یاد داریم که:

$$\left| x \right\rangle = \left| x_{n-1} \ldots x_1 x_0 \right\rangle$$

$$\left| z \right\rangle = \left| z_{n-1} \ldots z_1 z_0 \right\rangle$$

با 1 یا $x_i, z_i = 0$ با این اطمینان که $U_f{}^2 = I$ و U_f، که یک جایگشت ساده از 2^{n+m} بردار پایه، یکانی است. اگر ما $\left| 0^{\otimes m} \right\rangle$ رابه صورت حالت اولیه رجیستر خروجی قرار دهیم. پس:

$$U_f \left| x \otimes 0^{\otimes m} \right\rangle = \left| x \otimes f\left(x\right) \right\rangle \qquad (۲۷-۳)$$

اگر درنهایت H را با رجیستر ورودی در حالت $\left| 0^{\otimes n} \right\rangle$ قبل از U_f به کار بریم. بردار حالت حالت نهایی به صورت خطی زیر خواهد شد:

$$\left| \Psi_{fin} \right\rangle = U_f \left| \left(H^{\otimes n} 0^{\otimes n} \right) \otimes 0^{\otimes m} \right\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n - 1} \left| x \otimes f\left(x\right) \right\rangle \qquad (۲۸-۳)$$

این بردار حالت در اصل شامل 2^n مقدار از تابع f(x) است (همه آنها با هم متفاوت نیستند).

برای مثال اگر n=100 باشد، آن شامل تقریباً 10^{30} مقدار از f(x) است که یک رشد نمایی حالت‌ها است که به واقعه شگفت انگیز توازی کوانتومی منجر می شود. البته یک اندازه گیری فقط می تواند یکی از این مقادیر را بدهد. به طوری که در الگوریتم دوچ دیده ایم این، این هرگز ممکن نیست که اطلاعات مفید درباره رابطه بین مقادیر f(x) برای یک آنسامبل از مقادیر مختلف x را خارج کند، یک کامپیوتر کلاسیکی باید f(x) را برای همه این مقادیر x وابسته ارزیابی کند. [3, 4, 5]

فصل چهارم:

تبدیل فوریه کوانتومی و کاربردهای آن

تبدیل فوریه کوانتومی و کاربردهای آن

۴-۱-تعریف:

امروزه مهترین کشف در محاسبات کوانتومی این است که کامپیوترهای کوانتومی می توانند کارهایی که در کامپیوتر های کلاسیکی ممکن نیستند را به طور موثر انجام دهند. برای مثال پیدا کردن عوامل اول یک عدد n بیتی در بهترین الگوریتم‌های کلاسیکی شناخته شده به نام غربال میدان عددی نیازمند $\exp\left(\Theta\left(n^{\frac{1}{3}}\log^{\frac{2}{3}} n\right)\right)$ عملیات در زمان نوشتن می باشد که Θ مرتبه بزرگی عبارت است. این عدد تجزیه شده در ابتدا به صورت نمایی است. بنابراین تجزیه عموماً به عنوان یک مسئله سخت بر روی یک کامپیوتر کلاسیکی مطرح شده است. در مقابل، یک الگوریتم کوانتومی می تواند کار مشابه را با استفاده از $O\left(n^2 \log n \log\log n\right)$ عملیات انجام دهد. بنابراین یک کامپیوتر کوانتومی می تواند یک عدد نمایی را سریعتر از بهترین الگوریتم های کلاسیکی شناخته شده تجزیه کند. این نتیجه خود در حقیقت مهم است، اما شاید در مهمترین جنبه جالب در این مسئله، این سوال مطرح شود: چگونه مسائل دیگر که بر روی کامپیوتر کلاسیکی غیر عملی هستند، می توانند به طور مؤثر بر روی یک کامپیوتر کوانتومی انجام شوند؟

دراین بخش تبدیل فوریه کوانتومی را بسط می دهیم، که از عوامل اصلی برای تجزیه کوانتومی و بسیاری از الگوریتم های کوانتومی جالب دیگراست. تبدیل فوریه کوانتومی، که شروع می کنیم، یک الگوریتم کوانتومی موثر برای انجام یک تبدیل فوریه از دامنه های مکانیک کوانتومی است. استفاده از

تبدیل فوریه بر روی داده های کلاسیکی سرعت کار کلاسیکی را بالا نمی برد. اما یک کارمهم که قادر است انجام دهد، تخمین فاز می باشد. تخمین ویژه مقادیر یک اپراتور یکانی تحت شرایط معین، در این بخش توضیح داده می شود. این مسئله اجازه می دهد تا چندین مسئله جالب دیگر شامل مسئله پیدا کردن مرتبه و مسئله تجزیه را حل کنیم. که دربخش ۴-۳ تو ضیح داده شده‌اند.

تخمین فاز همچنین می تواند با الگوریتم جستجوی کوانتومی ترکیب شود تا مسئله حل شمردن[1] را با یک مسئله جستجو حل کند. تبدیل فوریه کوانتومی ممکن است استفاده شود تا مسئله زیر گروه مخفی را حل کند.

دیگر مسائل گفته شده بر روی یک کامپیوتر کلاسیکی سخت هستند.

۴-۲-تبدیل فوریه کوانتومی[2]

یکی از مفید ترین راه حل‌های یک مسئله در علم ریاضی یا کامپیوتر تبدیل آن به چند مسئله دیگر که حل آن را می دانیم است. چند تبدیل از این نوع وجود دارد که اغلب پیدا می شوند و بنابراین در خیلی مفاهیم سخت تبدیلات برای منظور خاص خودشان یاد گرفته می شوند. بزرگترین کشف از محاسبات کوانتومی چند تبدیل دارد که خیلی سریعتر بر روی یک کامپیوتر کوانتومی ازیک کامپیوتر کلاسیکی می توانند محاسبه شوند. این کشف قادر می باشد که الگوریتم های سریعتر برای کامپیوترهای کوانتومی بسازد. یکی از این تبدیلات، تبدیل فوریه گسسته است. در زبان ریاضی معمولی، تبدیل فوریه گسسته بر روی یک بردار از اعداد مختلط به عنوان ورودی عمل می کند. $x_0, x_1, ..., x_{N-1}$ که طول N از بردار پارامتر ثابتی است. در خروجی داده های تبدیل یافته، یک بردار از اعداد مختلط $y_0, ..., y_{N-1}$ هستند، تبدیل فوریه با رابطه زیرتعریف می شود :

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j \frac{k}{N}} |k\rangle \qquad (۱-۴)$$

[1] . counting solutions
[2] .quantum fourier transform

تبدیل فوریه کوانتومی دقیقاً نظیر این تبدیل است، اگر چه نماد قراردادی برای تبدیل فوریه کوانتومی تا حدودی متفاوت است. تبدیل فوریه کوانتومی بر روی پایه‌های متعامد $|0\rangle$ و... و $|N-1\rangle$ تعریف می‌شود و به صورت یک اپراتور خطی است که در زیر بر روی حالت های پایه عمل می کند:

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \frac{k}{N}} |k\rangle \qquad (۲-۴)$$

به صورت مشابه عملیات بر روی یک حالت دلخواه ممکن است به صورت زیر نوشته شود:

$$\sum_{j=0}^{N-1} x_j |j\rangle \to \sum_{k=0}^{N-1} y_k |k\rangle \qquad (۳-۴)$$

که دامنه های y_k تبدیل فوریه گسسته از دامنه های x_j هستند. این یک شکل واضح از تعریف نیست، اما این تبدیل یک تبدیل یکانی است و بدین معناست که طول بردار ثابت است و بنابراین می تواند به صورت دینامیکی برای یک کامپیوتر کوانتومی انجام شود. یکانی بودن تبدیل فوریه را به وسیله ساختن یک مدار کوانتومی یکانی که تبدیل فوریه را محاسبه می کند اثبات خواهیم کرد. همچنین به‌آسانی می‌توانیم به طور مستقیم ثابت کنیم تبدیل فوریه یکانی است.

درزیر، $N=2^n$ قرار می دهیم، که n تعداد اعداد صحیح است، و پایه های $|0\rangle,...,|2^n-1\rangle$ پایه های محاسباتی برای یک کامپیوتر کوانتومی n بیتی هستند.

مفید است که حالت $|j\rangle$ را با استفاده از نمایش در مبنای دو به صورت $j = j_1 j_2 ... j_n$ بنویسیم که به صورت فرمولی $j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0$ است. همچنین مفید است که نماد $0.j_l j_{l+1} ... j_m$ را به عنوان نمایش اعشاردرمبنای۲، $\frac{j_l}{2} + \frac{j_{l+1}}{4} + ... + \frac{j_m}{2^{m-l+1}}$ قبول کنیم.

با یک محاسبات جبری کوچک تبدیل فوریه کوانتومی می تواند به صورت نمایش حاصلضرب مفید زیر بدست بیاید:

$$|j_1,..., j_n\rangle \to \frac{\left(|0\rangle + e^{2\pi i 0 \cdot j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n}|1\rangle\right)..\left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 ... j_n}|1\rangle\right)}{2^{\frac{n}{2}}} \qquad (۴-۴)$$

این نمایش ضربی مفید است، چون حتی ممکن است این تعریف را تعریفی از تبدیل فوریه کوانتـومی در نظر بگیرید. همان طور که به طور کوتاه بدست آوردیم با این نمایش می‌توان یـک مـدار کوانتـومی مناسب ساخت که تبدیل فوریه را محاسبه کند. یک اثبات وجود دارد که تبدیل فوریه کوانتومی یکانی است، و بینشی با الگوریتم های بناشده بر روی تبدیل فوریه کوانتومی فراهم می کند. به صـورت یـک نتیجه وابسته تبدیل فوریه سریع کلاسیکی را بدست می آوریم. معادل نمایش ضربی (۴-۴) و تعریف (۴-۲) در زیر از تعدادی عملیات جبری مقدماتی نشان داده می شود که:

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle \qquad \text{که} \qquad N = 2^n$$

$$|j\rangle \to \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} |k\rangle \qquad (۵-۴)$$

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_{n-1} 2^1 + j_n 2^0$$

$$j = j_1 j_2 \ldots j_n$$

$$0 \cdot j_l j_{l+1} \ldots j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \ldots + \frac{j_m}{j^{m-l+1}}$$

چون تمام k ها یا صفر ند یا یک پس داریم:

$$\sum_{k=0}^{2^n-1} = \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \ldots \sum_{k_n=0}^{1}$$

$$2 \times 2 \times \ldots \times 2 = 2^n$$

$$|j\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \ldots \sum_{k_n=0}^{1} e^{2\pi i j \frac{k}{2^n}} |k\rangle$$

$$|k\rangle = |k_1 k_2 \ldots k_n\rangle = |k_1\rangle |k_2\rangle \ldots |k_n\rangle \Rightarrow$$

$$\Rightarrow |j\rangle \to \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} e^{2\pi i j (k_1 k_2 \ldots k_n) 2^{-n}} |k_1 k_2 \ldots k_n\rangle$$

$$|j\rangle \to \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l} \right) 2^{-n}} |k_1 k_2 \dots k_n\rangle$$

$$|j\rangle \to \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \left[e^{2\pi i j \left[k_1 2^{-1} + k_2 2^{-2} + \dots + k_n 2^{-n} \right]} \right] k_1\rangle |k_2\rangle \dots |k_n\rangle \qquad (۶-۴)$$

$$|j\rangle \to \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \left[\left(e^{2\pi i j k_1 2^{-1}} |1\rangle \right) \left(e^{2\pi i j k_2 2^{-2}} |k_2\rangle \right) \dots \left(e^{2\pi i j k_n 2^{-n}} |k_n\rangle \right) \right]$$

$$|j\rangle \to \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \qquad (۷-۴)$$

$$|j\rangle \to \frac{1}{2^{\frac{n}{2}}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \qquad (۸-۴)$$

$$= \frac{1}{2^{\frac{n}{2}}} \bigotimes_{l=1}^{n} \left[e^{2\pi i j 02^{-l}} |0\rangle + e^{2\pi i j 12^{-l}} |1\rangle \right]$$

$$= \frac{1}{2^{\frac{n}{2}}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right] \qquad (۹-۴)$$

اگر به جای L مقدار قرار دهیم داریم:

$$l = 1 \to \left[|0\rangle + e^{2\pi i j 2^{-1}} |1\rangle \right]$$

$$l = 2 \to \left[|0\rangle + e^{2\pi i j 2^{-2}} |1\rangle \right]$$

از طرفی داریم:

$$l = 1 \to e^{2\pi i j_n 2^{-1}} = e^{2\pi i \frac{j_n}{2}} = e^{2\pi i 0.j_n} \qquad (۱)$$

$$l = 2 \to e^{2\pi i j_{n-1} 2^{-1}} e^{2\pi i j_n 2^{-2}} = e^{2\pi i (j_{n-1} 2^{-1} + j_n 2^{-2})} = e^{2\pi i \left(\frac{j_{n-1}}{2} + \frac{j_n}{4} \right)} = e^{2\pi i 0.j_{n-1} j_n} \qquad (۲)$$

$$l = 3 \to e^{2\pi i j_{n-2} 2^{-1}} e^{2\pi i j_{n-1} 2^{-2}} e^{2\pi i j_n 2^{-3}} = e^{2\pi i (j_{n-2} 2^{-1} + j_{n-1} 2^{-2} + j_n 2^{-3})} =$$

$$= e^{2\pi i\left(\frac{j_{n-2}}{2}+\frac{j_{n-1}}{4}+\frac{j_n}{8}\right)} = e^{2\pi i 0.j_{n-2}j_{n-1}j_n} \qquad (۳)$$

اگراین کارراتا n بارانجام دهیم داریم:

$$l=n \rightarrow e^{2\pi i j_1 2^{-1}} e^{2\pi i j_2 2^{-2}} \ldots e^{2\pi i j_{n-1} 2^{-n+1}} e^{2\pi i j_n 2^{-n}} = e^{2\pi i\left(j_1 2^{-1}+j_2 2^{-2}+\ldots+j_{n-1}2^{-n+1}+j_n 2^{-n}\right)}$$

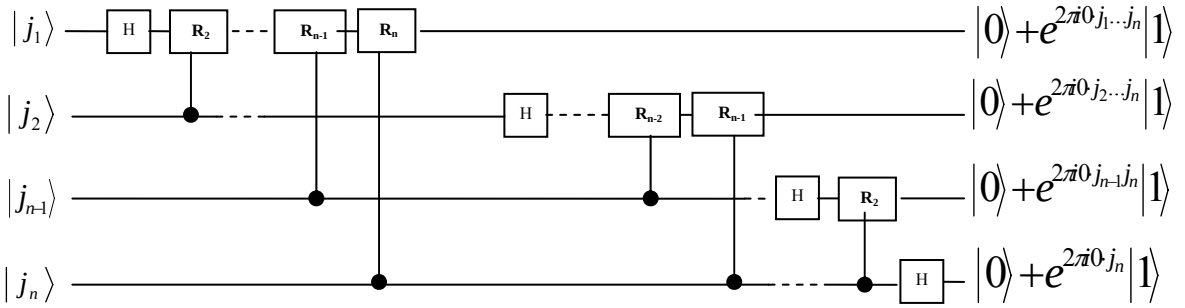
$$= e^{2\pi i\left(\frac{j_1}{2}+\frac{j_2}{4}+\ldots+\frac{j_{n-1}}{2^{n-1}}+\frac{j_n}{2^n}\right)} = e^{2\pi i 0.j_1 j_2 \ldots j_{n-1} j_n} \qquad (n)$$

از معادله (۴-۶) و (۱) و (۲) و (۳) و... و (n) داریم:

$$|j\rangle \rightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right)}{2^{\frac{n}{2}}} \qquad (۱۰-۴)$$

نمایش حاصلضرب (۴-۴) به راحتی درست می شود و به راحتی یک مدار موثر برای تبدیل فوریه کوانتومی را نتیجه می دهد. نظیر مدار نشان داده شده درشکل (۴-۱) گیت R_k تبدیل یکانی را مشخص می کند.

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \qquad (۱۱-۴)$$



شکل (۴-۱): مدار تبدیل فوریه کوانتومی.

با مشاهده مدار ترسیم شده تبدیل فوریه کوانتومی محاسبه می شود. در نظر بگیرید چه اتفاقی می افتد وقتی که حالت $|j_1...j_n\rangle$ به عنوان ورودی است. با به کار بردن گیت هادامارد با بیت اول، حالت زیر نتیجه می شود:

$$n=1 \rightarrow \frac{1}{2^{\frac{n}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_1}|1\rangle\right)|j_2...j_n\rangle \qquad (۱۲-۴)$$

چون $e^{2\pi i 0\cdot j_1} = -1$ وقتی که $j_1 = 1$ است و در غیر اینصورت برابر $+1$ است. به کار بردن گیت کنترلی R_2 حالت زیررا نتیجه می دهد:

$$R_2\left[\frac{1}{2^{\frac{n}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_1}\right)|j_2...j_n\rangle\right] =$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i \frac{j_2}{2^2}} \end{bmatrix}\left[\frac{1}{2^{\frac{1}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_1}|1\rangle\right)|j_2...j_n\rangle\right] =$$

$$= \frac{1}{2^{\frac{1}{2}}}\begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i \frac{j_2}{2^2}} \end{bmatrix}\left[\begin{pmatrix}1\\0\end{pmatrix} + e^{2\pi i 0\cdot j_1}\begin{pmatrix}0\\1\end{pmatrix}\right]|j_2...j_n\rangle =$$

$$= \frac{1}{2^{\frac{1}{2}}}\left[\begin{pmatrix}1\\0\end{pmatrix} + e^{2\pi i 0\cdot j_1}\begin{pmatrix}0\\e^{2\pi i \frac{j_2}{4}}\end{pmatrix}\right]|j_2...j_n\rangle =$$

$$= \frac{1}{2^{\frac{1}{2}}}\left[\begin{pmatrix}1\\0\end{pmatrix} + e^{2\pi i 0\cdot j_1}e^{2\pi i \frac{j_2}{4}}\begin{pmatrix}0\\1\end{pmatrix}\right]|j_2...j_n\rangle =$$

$$= \frac{1}{2^{\frac{1}{2}}}\left[|0\rangle + e^{2\pi i\left(0\cdot j_1 + \frac{j_2}{4}\right)}|1\rangle\right]|j_2...j_n\rangle =$$

$$= \frac{1}{2^{\frac{1}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_1 j_2}|1\rangle\right)|j_2...j_n\rangle$$

(۱۳-۴)

با استفاده از گیتهای کنترلی R_3، R_4 الی R_n ادامه می دهیم، هرکدام با بیت اضافی در فاز ضریب $|1\rangle$ اول جمع می شود درنهایت در این روش حالت زیر راداریم:

$$\frac{1}{2^{\frac{1}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_1 j_2 \cdots j_n}\right)|j_2 \cdots j_n\rangle \qquad (۱۴-۴)$$

حال یک روش مشابه را به روی کیو بیت دوم انجام می دهیم. گیت هـا دامـارد حالـت زیـر را نتیجـه می دهد:

$$n=2 \rightarrow \frac{1}{2^{\frac{2}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_1 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0\cdot j_2}|1\rangle\right)|j_3 \cdots j_n\rangle \qquad (۱۵-۴)$$

و گیتهای کنترلی R_2 تا R_{n-1} حالت زیر را نتیجه می دهند.

$$\frac{1}{2^{\frac{2}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_1 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0\cdot j_2 \cdots j_n}|1\rangle\right)|j_3 \cdots j_n\rangle \qquad (۱۶-۴)$$

به این روش برای هرکیوبیت ادامه می دهیم، حالت نهایی بدست می آید:

$$\frac{1}{2^{\frac{n}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_1 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0\cdot j_2 \cdots j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0\cdot j_n}|1\rangle\right) \qquad (۱۷-۴)$$

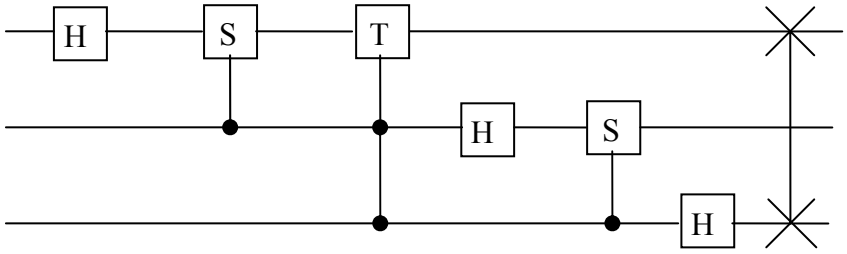
بعد از عوض کردن جای عملها، حالت کیوبیت به صورت زیراست:

$$\frac{1}{2^{\frac{n}{2}}}\left(|0\rangle + e^{2\pi i 0\cdot j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0\cdot j_{n-1} j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0\cdot j_1 \cdots j_n}|1\rangle\right) \qquad (۱۸-۴)$$

در مقایسه با معادله (۴-۴) می بینیم که این نتیجه دلخواه از تبدیل فوریه کوانتومی است. این ساختار همچنین ثابت می کند که تبدیل فوریه کوانتومی یکانی است، چون هرگیت درمدار یکانی اسـت. یـک مثال واضح نشان دهنده یک مدار برای تبدیل فوریه کوانتومی بر روی سه کیوبیت در زیـر نـشان داده شده است.

۴-۲-۱-مثال تبدیل فوریه کوانتومی سه کیوبیتی

مدار مشخص شده زیر برای تبدیل فوریه کوانتومی سه کیوبیتی است:



شکل (۴-۲): مدار تبدیل فوریه کوانتومی سه کیوبیتی

S و T که به ترتیب گیتهای فازو $\frac{\pi}{8}$ هستند را داریم. به صورت یک ماتریس تبدیل فوریه کوانتومی

در این مثال با استفاده از $\omega = e^{\frac{2\pi i}{8}} = \sqrt{i}$ و ماتریس های S وT که در زیر نشان داده شده‌اند:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

ماتریس این تبدیل به صورت زیر بدست می آید:

$$\frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}$$

با انجام یک گیت هادامارد و n-1 چرخش مقید (وابسته) به کیوبیت اول شروع می کنیم، در مجموع n گیت. این به وسیله یک گیت هادامارد و n-2 چرخش وابسته به کیوبیت دوم نشان داده می شود، در مجموع n-1 گیت. با ادامه این روش می بینیم که $n+(n-1)+(n-2)+...+1=\frac{n(n+1)}{2}$ گیت مورد نیاز است، به علاوه گیتها دراین مبادله درگیر هستند. به بیش از $\frac{n}{2}$ جانشین ها نیاز است. و هر جانشین می تواند با استفاده از سه گیت کنترلی NoT انجام شود. بنابراین این مدار $\Theta(n^2)$ الگوریتم برای انجام تبدیل فوریه کوانتومی فراهم می کند.

درمقابل، بهترین الگوریتم های کلاسیکی برای محاسبه تبدیل فوریه گسسته بر روی 2^n عنصر، الگوریتم هایی به صورت تبدیل فوریه سریع هستند (FFT)، که تبدیل فوریه گسسته را با استفاده از $\Theta(n2^n)$ گیت محاسبه می کنند، که برای اینکه تبدیل فوریه رابر روی یک کامپیوتر کلاسیکی محاسبه کند به طور نمایی نیازمند عملهای بیشتری است، بنابراین تبدیل فوریه کوانتومی را بر روی یک کامپیوتر کوانتومی انجام می دهد.

بدین ترتیب تبدیل فوریه کوانتومی ارزشمند است چون تبدیل فوریه در خیلی از جستجوهای کاربردی داده‌های جهان واقعی نقش دارد. برای مثال، درکامپیوتر تشخیص صدا، مرحله اول در تشخیص صوت این است که تبدیل فوریه مدار به صورت عددی تبدیل می کند. آیا می توانیم از تبدیل فوریه کوانتومی استفاده کنیم تاسرعت محاسبه را بالا ببرد؟ متأسفانه جواب این است که هیچ روشی شناخته شده نیست که این را انجام دهد. مسئله این است که دامنه ها در یک کامپیوتر کوانتومی نمی‌توانند مستقیماً با اندازه‌گیری در دسترس باشند. بنابراین روشی از تعیین دامنه‌های تبدیل فوریه از حالت اصلی وجود ندارد. بدتر اینکه در صورت کلی روشی وجود ندارد تا به طور موثر حالت اصلی تبدیل فوریه یافته را تهیه کند. بنابراین درک استفاده برای تبدیل کوانتومی خیلی دقیق‌تر از آنچه که امید داشتیم است. دراین فصل چندین الگوریتم پایه بر روی یک کاربرد خیلی دقیق از تبدیل فوریه کوانتومی را توسعه می دهیم.

۴-۳- تخمین فاز[1]

تبدیل فوریه کلیدی با یک روش عمومی شناخته شده بـه صـورت تخمـین فـاز اسـت، کـه در شـروع کلیدی برای بسیاری الگوهای کوانتومی است. فرض کنید که یـک اپراتـور یکـانی U دارای یـک ویـژه بردار $|u\rangle$ با ویژه مقدار $e^{2\pi i\varphi}$است، که مقدار φنامعلوم است. هدف نهایی الگوریتم تخمین فاز این اسـت که φرا تخمین بزند. با انجام تخمین فرض می کنیم که یک جعبه سیاه در دسـترس داریـم (بعـضی اوقـات بـه صـورت یـک پیـشگویی مـی شناسـیم) کـه قـادر اسـت حالـت $|u\rangle$ را تهیـه کنـد و عمـل کنترلی U^{2^j}را برای اعداد صحیح نامنفی j مناسب انجام دهد. استفاده از جعبه سیاه نشان می دهد که در حقیقت روش تخمین فاز خود یک الگوریتم کوانتومی کامل نیست. بلکه، باید درباره تخمین فاز بـه صورت یک نوع پیمانه فکر کرد، که وقتی که با دیگر پیمانه ها ترکیب می شود، می تـوان از آن بـرای انجام کارهای محاسباتی جالب استفاده کرد. در کاربردهای خـاص از روش تخمـین فـاز ایـن را کـاملا انجام خواهیم داد، توضیح اینکه چگونه عملهای جعبه سـیاه انجـام شـده‌انـد، و ترکیـب آنهـا بـا روش تخمین فاز واقعا کار مفیدی است. گرچه ما به تصور آنها به صورت یک جعبه سیاه ادامه خواهیم داد.

روش تخمین فاز کوانتومی از دو رجیستر استفاده می کنـد. رجیـستر اول شـامل t کیوبیـت اولیـه در حالت $|0\rangle$ است. اینکه چگونه t را انتخاب می کنیم به دو چیز بستگی دارد: عدد ارقام در دسترس کـه برای تخمین φ می‌خواهیم داشته باشیم، و بـا چـه احتمـالی روش تخمـین فـاز موفـق خواهـد بـود. وابستگی t به این کمیات به طور طبیعی از آنالیز زیر پدیدار می شود.

رجیستر دوم در حالت $|u\rangle$ شروع می شود و شامل کیوبیت های زیـادی بـه انـدازه ذخیـره $|u\rangle$ اسـت. تخمین فاز در دو مرحله انجام می شود. ابتدا، مدار نشان داده شده در شکل (۴-۳) را به کار می بریم. مدار با استفاده از یک تبدیل هادامارد بر روی رجیستر اول شروع می شود و با به کار بردن عمل هـای

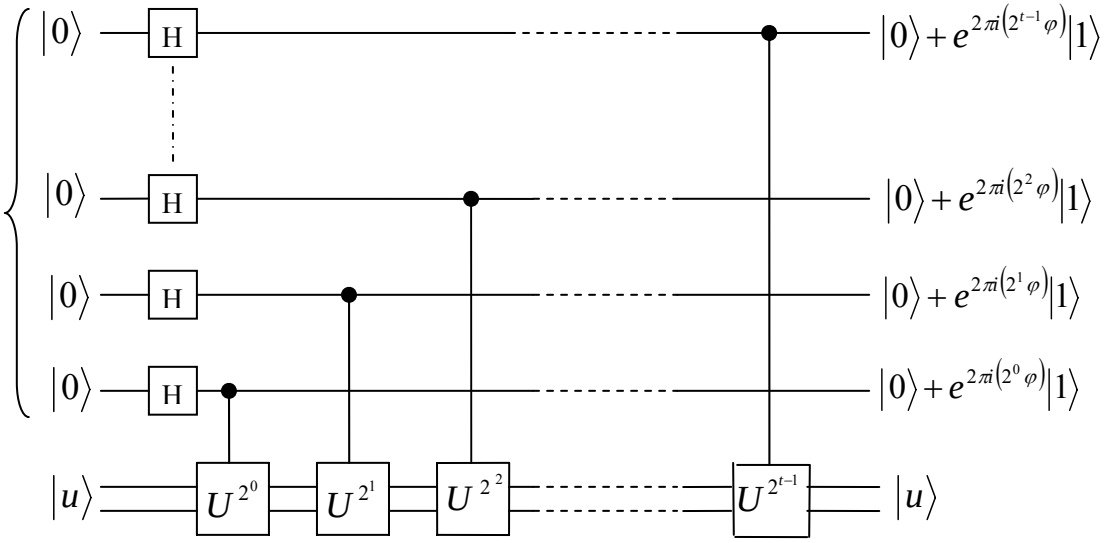
[1] .phase estimation

کنترلی U بر روی رجیستر دوم با U تولیدشده از توانهای دوم متوالی ادامه پیدا می کند. حالت نهـایی رجیستر اول به راحتی دیده می شود به صورت :

$$\frac{1}{2^{\frac{t}{2}}}\left(\left|0\right\rangle+e^{2\pi i2^{t-1}\varphi}\left|1\right\rangle\right)\left(\left|0\right\rangle+e^{2\pi i2^{t-2}\varphi}\left|1\right\rangle\right)..\left(\left|0\right\rangle+e^{2\pi i2^{0}\varphi}\left|1\right\rangle\right)=$$

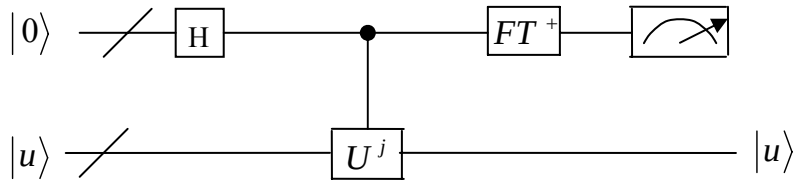
$$=\frac{1}{2^{\frac{t}{2}}}\sum_{k=0}^{2^t-1}e^{2\pi i\varphi k}\left|k\right\rangle \qquad (۱۹-۴)$$

رجیستر دوم را ازاین توصیف حذف می کنیم زیرا در طول محاسبات در حالت $\left|u\right\rangle$ باقی می ماند.



شکل (۴-۳): مرحله اول روش تخمین فاز. عامل نرمال $\frac{1}{\sqrt{2}}$ در سمت راست حذف شده است.

مرحله دوم تخمین فاز به کار بردن تبدیل فوریه کوانتومی معکوس بر روی رجیستر اول است. این کار به وسیله معکوس کردن مدار برای تبدیل فوریه کوانتومی در بخش قبل بدست مـی آیـد، و در $\Theta(t^2)$ مرحله می تواند انجام شود. سومین و آخرین مرحله از تخمـین فـاز خوانـدن حالـت رجیـستر اول بـه وسیله انجام یک اندازه گیری در پایه های محاسباتی است. نشان خواهیم داد که این کار یک تخمـین خیلی خوب از φ فراهم کند. یک طرح سرتاسر کلی در شکل (۴-۴) نشان داده شده است.



شکل (۴-۴) : طرح کلی از روش تخمین فاز. t کیوبیت بالایی رجیستر اول هستند. و کیوبیتهای پایینی رجیستر دوم هستند. (/ معمولا برای نمایش سیمها به کار می رود). $|u\rangle$ یک ویژه حالت از U با ویژه مقدار $e^{2\pi i\varphi}$ است. خروجی بعد از اندازه گیری یک تقریب دقیق از φ با $t-\left\lceil \log(2+\frac{1}{2\epsilon}) \right\rceil$ بیت، با احتمال ϵ -1 است.

با دقیق کردن بینشمان به طوری که چرا تخمین فاز کار می کند، فرض می کنیم که φ دقیقا در t بیت به صورت زیربیان شده باشد:

$$\varphi = 0.\varphi_1\varphi_2\ldots\varphi_t$$

پس حالت (۴-۱۹) نتیجه شده از مرحله اول تخمین فاز می تواند به صورت زیر نوشته شود:

$$\frac{1}{2^{\frac{t}{2}}}\left(|0\rangle+e^{2\pi i 0.\varphi_t}|1\rangle\right)\left(|0\rangle+e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle\right)\ldots\left(|0\rangle+e^{2\pi i 0.\varphi_1\varphi_2\ldots\varphi_t}|1\rangle\right) \qquad (۲۰-۴)$$

مرحله دوم ازتخمین فازبه کار بردن فوریه کوانتومی معکوس است. اما در مقایسه بخش قبل با نتیجه‌ی حاصل از تبدیل فوریه، معادله (۴-۴) می بینیم که حالت خروجی مرحله دوم حالت حاصلضرب $|\varphi_1\ldots\varphi_t\rangle$ است. یک اندازه گیری در پایه های محاسباتی دقیقاً φ را می دهد.

خلاصه، الگوریتم تخمین فاز اجازه می دهد تا یکبار فاز φ از یک ویژه مقدار اپراتور یکانی U متناظر با ویژه بردار $|u\rangle$ داده شده را تخمین بزنیم. یک رفتار ذاتی در دل این روش ، توانایی انجام تبدیل فوریه معکوس به انجام تبدیل زیر است:

$$\frac{1}{2^{\frac{t}{2}}}\sum_{j=0}^{2^t-1}e^{2\pi i\varphi j}|j\rangle|u\rangle\rightarrow|\tilde{\varphi}\rangle|u\rangle \qquad (۲۱-۴)$$

که $|\tilde{\varphi}\rangle$ یک حالت را مشخص می کند که یک تخمین خوب برای φ وقتی که اندازه‌گیری می شود، است.

۴-۳-۱- کارآیی و نیازها:

آنالیز فوق برای حالت ایده آل به کار می رود. که φ دقیقاً می تواند با یک بسط در مبنـای دو t بیتـی نوشته شود. حال وقتی که این حالت نباشد چه اتفاقی می افتد؟ نتیجه مـی‌گیـریم، روشـی کـه شـرح دادیم یک تقریب خیلی خوب برای φ با احتمال بالا تولید خواهد کرد.

به طور کلی همان‌طور که از قبل، از نمادگذاری استفاده شده در (۴-۲۱) حاکی بود. این نیازها بعـضی کاربردهای دقیق را نشان می دهند.

b را عدد صحیح در بازه صفرتا 2^t-1 قرار دهید به طوری که $\frac{b}{2^t} = 0.b_1 \ldots b_t$، بهترین تقریب t بیتی به φ است که از φ کوچکتر است. که $\delta = \varphi - \frac{b}{2^t}$ تفاضل بین φ و $\frac{b}{2^t}$ شرط $0 \le \delta \le 2^{-t}$ را برآورده می کند. قصد داریم نشان دهیم که مشاهده انتهای روش تخمین فاز یک نتیجه تولید خواهد کرد کـه به b وابسته است، و ما را قادر می سازد تا φ را دقیقا با احتمال بالا تخمین بزنیم. به کار بردن تبدیل فوریه کوانتومی معکوس با حالت (۴-۱۹) حالت زیر را تولید می کند:

$$\frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{\frac{-2\pi i k l}{2^t}} e^{2\pi i \varphi k} \left| l \right\rangle \qquad (۲۲-۴)$$

α_lرا دامنه $\left| (b+l) (\mathrm{mod}\ 2^t) \right\rangle$ قرار دهید.

$$\alpha_l = \frac{1}{2^t} \sum_{k=0}^{2^t-1} \left(e^{2\pi i \left(\varphi - (b+l)/2^t \right)} \right)^k \qquad (۲۳-۴)$$

این رابطه یک جمع سری هندسی است. بنابراین:

$$\alpha_l = \frac{1}{2^t} \left(\frac{1 - e^{2\pi i \left(2^t \varphi - (b+l) \right)}}{1 - e^{2\pi i \left(\varphi - \frac{(b+l)}{2^t} \right)}} \right) = \qquad (۲۴-۴)$$

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i\left[2^t\left(\varphi-\frac{b}{2^t}-\frac{l}{2^t}\right)\right]}}{1-e^{2\pi i\left(\varphi-\frac{b}{2^t}-\frac{l}{2^t}\right)}}\right) =$$

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i\left[2^t\left(\varphi-\frac{b}{2^t}\right)-l\right]}}{1-e^{2\pi i\left[\left(\varphi-\frac{b}{2^t}\right)-\frac{l}{2^t}\right]}}\right) =$$

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i\left[2^t\delta-l\right]}}{1-e^{2\pi i\left[\delta-\frac{l}{2^t}\right]}}\right) \qquad (۲۵-۴)$$

فرض می کنیم که این نتیجه‌ی اندازه‌گیری نهایی برای m است. قصد داریم تا احتمال به دست آوردن یک مقدار از m به صورت $|m-b|>e$ را تعیین کنیم، که e یک عدد صحیح مثبت است که چشم پوشی از خطا را مشخص می‌کند. احتمال مشاهده یک m نظیر به وسیله رابطه زیر داده می‌شود:

$$P\left(|m-b|>e\right)=\sum_{-2^{t-1}<l\le-(e+1)}|\alpha_l|^2+\sum_{e+1\le l\le 2^{t-1}}|\alpha_l|^2 \qquad (۲۶-۴)$$

اما برای هر θ حقیقی $|1-\exp(i\theta)|\le 2$، بنابراین با استفاده از رابطه (۴-۲۵) :

$$|\alpha_l|\le\frac{2}{2^t\left|1-e^{2\pi i\left(\delta-\frac{l}{2^t}\right)}\right|} \qquad (۲۷-۴)$$

با حساب دیفرانسیل و یا هندسه مقدماتی وقتی که $-\pi\le\theta\le\pi$ باشد رابطه $|1-\exp(i\theta)|\ge 2\frac{|\theta|}{\pi}$ را داریم. اما وقتی که $-2^{t-1}<l\le 2^{t-1}$ داریم $-\pi\le 2\pi\left(\delta-\frac{l}{2^t}\right)\le\pi$ بنابراین:

$$|\alpha_l|\le\frac{2}{2^t\left[\frac{2\left(2\pi\left(\delta-\frac{l}{2^t}\right)\right)}{\pi}\right]}$$

$$\Rightarrow |\alpha_l| \le \frac{1}{2^{t+1}\left(\delta - \frac{l}{2^t}\right)} \qquad (۲۸-۴)$$

ترکیب (۴-۲۶) و (۴-۲۸) نتیجه‌ی زیر را می دهد:

$$P\left(|m-b| \succ e\right) \le \left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \left[\frac{1}{2^{t+1}\left(\delta - \frac{l}{2^t}\right)}\right]^2 + \sum_{l=e+1}^{2^t+1} \left[\frac{1}{2^{t+1}\left(\delta - \frac{l}{2^t}\right)}\right]^2\right] \le$$

$$\le \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{\left(l - 2^t\delta\right)^2} + \sum_{l=e+1}^{2^t-1} \frac{1}{\left(l - 2^t\delta\right)^2}\right] \qquad (۲۹-۴)$$

به خاطر بیاورید که $0 \le 2^t\delta \le 1$ ، در نتیجه به دست می‌آوریم:

$$P\left(|m-b| \succ e\right) \le \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{l^2} + \sum_{l=e+1}^{2^t-1} \frac{1}{(l-1)^2}\right] \qquad (۳۰-۴)$$

$$\le \frac{1}{2}\sum_{l-e}^{2^{t-1}} \frac{1}{l^2} \qquad (۳۱-۴)$$

$$\le \frac{1}{2}\int_{e-1}^{2^{t-1}-1} \frac{1}{l^2}\,dl \qquad (۳۲-۴)$$

$$= \frac{1}{2(e-1)} \qquad (۳۳-۴)$$

فرض کنید می خواهیم φ را با یک دقت 2^{-n} تقریب بزنیم. برای این کار $e = 2^{t-n} - 1$ انتخاب می کنیم. با استفاده از t=n+p کیوبیت در الگوریتم تخمین فاز از (۴-۳۳) می بینیم که احتمال به دست آوردن یک تقریب صحیح با این دقت دقیقاً $1 - 1/2(2^p - 2)$است. بنابراین برای موفقیت در به دست آوردن φ دقیق با n بیت با احتمال حداقل $1-\varepsilon$ انتخاب می کنیم:

$$t = n + \left[\log\left(2 + \frac{1}{2\varepsilon} \right) \right] \qquad (۳۴-۴)$$

درمواردی برای استفاده از الگوریتم تخمین فاز، احتیاج داریم تا بتوانیم یک ویژه حالت $|u\rangle$ از U را فراهم کنیم. اما اگر ندانیم چگونه یک ویژه حالت نظیر را فراهم کنیم چه می شود؟ فرض کنید که چند حالت $|\psi\rangle$ دیگر را به جای $|u\rangle$ فراهم کرده ایم. بسط این حالت برحسب ویژه حالت های $|u\rangle$ از U، $|\psi\rangle = \sum_u C_u |u\rangle$ است. فرض کنید که ویژه حالت $|u\rangle$ ویژه مقدار $e^{2\pi i \varphi_u}$ دارد. با درک مستقیم نتیجه الگوریتم تخمین فاز مداوم یک حالت خروجی نهایی با $|\widetilde{\varphi}_u\rangle$ خواهد بود، که $\widetilde{\varphi}_u$ یک تقریب خیلی خوب به فاز φ_u است. بنابراین انتظار داریم که خواندن رجیستر اول در خروجی یک تقریب خوب به φ_u خواهد داد، که u تصادفی با احتمال $|C_u|^2$ انتخاب می شود. این روش اجازه می دهد تا از فراهم کردن یک ویژه حالت ناشناخته‌ی ممکن اجتناب کنیم.

چرا تخمین فاز جالب است؟ برای این دلیل که تخمین فاز مسئله‌ای که ازنظرفیزیکی هم غیر بدیهی و هم جالب است را حل می‌کند. به طورمثال، چگونه یک ویژه مقدار مربوط به یک ویژه بردار یک اپراتور یکانی داده شده تخمین زده می شود؟ این استفاده‌ی صحیح است که، به هر حال، از مشاهدات برمی‌آید که دیگر مسائل جالب می توانند به تخمین فاز تبدیل شوند، به طوری که در بخش بعدی نشان داده شده است. الگوریتم تخمین فاز در زیر خلاصه شده است.

۴-۳-۲- الگوریتم تخمین فاز کوانتومی

ورودی ها:

۱. یک جعبه سیاه که یک عمل کنترل U^j را برای عدد صحیح j انجام می دهد.

۲. یک ویژه حالت $|u\rangle$ از U با ویژه مقدار $e^{2\pi i \varphi_u}$.

۳. $t = n + \left[\log\left(2 + \frac{1}{2\varepsilon}\right)\right]$ کیوبیت اولیه درحالت $|0\rangle$.

خروجی:

یک تقریب n بیتی $\widetilde{\varphi}_u$ به φ_u.

تعداد مراحل الگوریتم:

شامل $O(t^2)$ عملیات و یک عمل که عملیات U^j کنترلی جعبه سیاه نامیده می‌شود است. احتمال موفقیت حداقل $1-\varepsilon$ است.

روش الگوریتم:

۱. حالت اولیه $|0\rangle|u\rangle$

۲. ایجاد ترکیب $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$

۳. به کار بردن جعبه سیاه $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle U^j|u\rangle$

نتیجه جعبه سیاه $= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi i\varphi_u}|j\rangle|u\rangle$

۴ . به کار بردن تبدیل فوریه معکوس $\rightarrow |\widetilde{\varphi}_u\rangle|u\rangle$

۵ . اندازه گیری رجیستر اول $\rightarrow \widetilde{\varphi}_u$

۴-۴- پیدا کردن مرتبه وتجزیه

با استفاده از تخمین فاز می توان مسائل جالب دیگر را حل کرد. اکنون به شرح دو نمونه از جالبترین مسائل مربوط به آن می پردازیم: مسئله پیداکردن مرتبه ومسئله تجزیه. این دو مسئله در حقیقت هم ارز با یکدیگر هستند، بنابراین دراین بخش یک الگوریتم کوانتومی را برای حل مسئله پیداکردن مرتبه شرح می دهیم و توضیح می دهیم که چگونه مسئله پیداکردن مرتبه به توانایی تجزیه به خوبی اشاره می کند.

برای فهم الگوریتم های کوانتومی تجزیه وپیداکردن مرتبه به یک زمینه کوچک در تئوری عددی نیـاز داریم. در سرتاسر این بخش به جنبه های کوانتومی مسئله می پردازیم.

الگوریتم های سریع کوانتومی برای فهمیدن مرتبـه و تجزیـه بـه سـه دلیـل جالـب هـستند. اولـین و مهمترین دلیل، این است که کامپیوترهای کوانتومی ممکـن اسـت قـویتر از کامپیوترهـای کلاسـیکی باشند. دومین دلیل اینکه هر دو مسئله دارای ارزش ذاتی کافی برای توجیه هر دو ا لگوریتم کلاسیکی یا کوانتومی هستند. سومین دلیل و مهمترین از دیدگاه عملی این است که الگوریتم هـای مـوثر بـرای پیداکردن مرتبه و تجزیه می توانند برای شکستن سیستم های کلید مخفی عمومی بکار روند.

۴-۴-۱- پیداکردن مرتبه:

برای اعداد صحیح مثبت x و N به طوری که x<N : بـدون عوامـل مـشترک مرتبـه x modulo N بـا کوچکترین عدد صحیح مثبت r به طوری کـه $x^r =1(\text{mod } N)$ تعریـف مـی شـود. مـسئله پیـداکردن مرتبه تعیین مرتبه r برای بعضی x و N های مشخص است. باید باور کـرد کـه پیـدا کـردن مرتبـه بـا استفاده از کامپیوترهای کلاسیکی یک مسئله سخت است، با این احساس که هیچ الگـوریتم شـناخته شده‌ای که مسئله را با استفاده از منبع چند جمله ای در O(L) بیت مورد نیاز حل کنـد وجـود نـدارد که مسئله را مشخص کند که در آن L = [Log (N)] تعداد بیتهای مورد نیاز است تا N مشخص شود. در این بخش شرح می دهیم که چگونه تخمـین فـاز ممکـن اسـت اسـتفاده شـود تـا یـک الگـوریتم کوانتومی موثر برای پیداکردن مرتبه بدست بیاید.

الگوریتم کوانتومی برای پیداکردن مرتبه فقط الگوریتم تخمین فاز به کار رفته بـا یـک عملگـر یکـانی است.

$$U\left|y\right\rangle \equiv \left|xy\ (\text{mod}\ \ N\ )\right\rangle \qquad (۳۵-۴)$$

با $y\in\{0,1\}^L$. (توجـه کنیـد کـه اینجـا و در زیـر وقتـی $N\le y \le 2^L-1$، از قـرار داد $xy\ (\text{mod}\ \ N\ )$ استفاده می کنیم که U به طور غیر بدیهی وقتیکه $0 \le y \le N-1$ است عمل می کنـد). یـک محاسـبه ساده نشان می دهد که حالت به وسیله رابطه زیر تعریف می شود:

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi isk}{r}\right] |x^k \bmod N\rangle \qquad (۳۶-۴)$$

برای اعداد صحیح $0 \le S \le r\text{-}1$ ویژه حالت های U هستند، چون

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi isk}{r}\right] |x^{k+1} \bmod N\rangle \qquad (۳۷-۴)$$

$$= \exp\left[\frac{2\pi is}{r}\right] |u_s\rangle \qquad (۳۸-۴)$$

استفاده از روش تخمین فاز اجازه می دهد با دقت بالا مطابق ویـژه مقـادیر $\exp(2\pi is/r)$ مرتبـه r را بدست آوریم.

برای استفاده از روش تخمین فاز به دو چیز نیاز داریم: اولاً باید روش مناسبی داشـته باشـیم تـا یـک عمل کنترلی U^{2^j} را برای هر عدد صحیح j انجام دهیم، ثانیاً باید به طور موثر یک ویژه حالت $|u_s\rangle$ با یک ویژه مقدار غیر بدیهی یا تقریباً ترکیبی از این ویژه حالتها فراهم کنیم.

نیاز اول با استفاده از یک روش که به نام توان رسانی پیمانه ای[1] مـی شناسـیم بـرآورده مـی‌شـود و همچنان می‌توانیم تمام دنباله عملهای کنترلی U^{2^j} را بوسیله روش تخمین فاز بـا اسـتفاده از $O(L^3)$ گیت انجام دهیم.

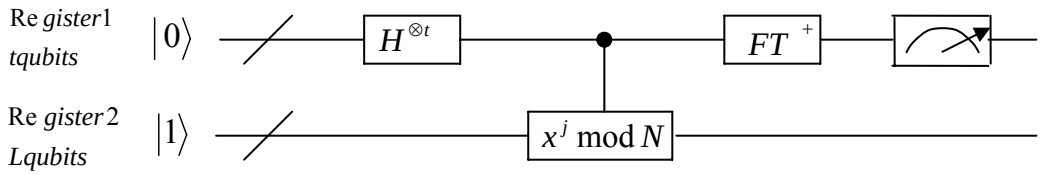
نیاز دوم یک حقه کوچک است. تهیه $|u_s\rangle$ نیازمند دانستن r است. بنابراین این خروجی مـسئله اسـت. خوشبختانه یک مشاهده زیرکانه وجود دارد که اجازه می دهد مسئله $|u_s\rangle$را حل کنیم که بـه صـورت زیر است:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \qquad (۳۹-۴)$$

در انجام روش تخمین فاز اگر از $t = 2L + 1 + \left\lceil \log(2 + \frac{1}{2\varepsilon}) \right\rceil$ کیوبیت در رجیستر اول استفاده کنیم (مربوط به شکل (۴-۴)) و رجیستر دوم را در حالت $|1\rangle$تهیه کنیم، نشان می دهد کـه بـرای هـر s در

[1] . modular

بـازه 0 تـا r-1 ، مـی‌خـواهیم یـک تخمـین از فـاز $\varphi \approx \frac{s}{r}$ دقیقـاً بـا 2L+1 بیـت بـا احتمـال تقریبـاً $\frac{(1-\varepsilon)}{r}$بدست بیاوریم. الگوریتم پیداکردن مرتبه به صورت طرح وار در شکل (۴-۵) نمایش داده شده است.



شکل (۴-۵): مدار کوانتومی برای الگوریتم پیداکردن مرتبه . رجیستر دوم همان طور که نشان داده شده است در ورودی $|1\rangle$ می باشد ولی می تواند در حالت $|0\rangle$نیز باشد.

۴-۴-۲- توان رسانی پیمانه ای:

حال می‌خواهیم ببینیم که چگونه می‌توانیم دنباله عملهای کنترلی U^{2^j} استفاده شده با روش تخمـین فاز را به صورت قسمتی از الگوریتم پیداکردن مرتبه محاسبه کنیم. به این ترتیب می خـواهیم تبـدیل زیر را محاسبه کنیم:

$$|z\rangle|y\rangle \to |z\rangle U^{z_t 2^{t-1}} \ldots U^{z_1 2^0}|y\rangle \qquad (۴۰-۴)$$

$$= |z\rangle\left|x^{z_t 2^{t-1}} \times \ldots \times x^{z_1 2^0} y \pmod N\right\rangle \qquad (۴۱-۴)$$

$$= |x\rangle\left|x^z y \pmod N\right\rangle \qquad (۴۲-۴)$$

بنابراین دنباله عملهای کنترلی U^{2^j} بکار رفته در تخمین فاز معادل ضرب کردن عناصر رجیـستر دوم با پیمانه نمایی $x^z \pmod N$ است که z عناصر رجیستر اول می باشد. این عمل ممکن است به آسـانی بـا اسـتفاده از تکنیـک محاسـبات معکـوس انجـام شـود. ایـده اساسـی در محاسـبات معکـوس تـابع $x^z \pmod N$ از z در سومین رجیستر است و سپس به طور معکوس عناصـر رجیـستر دوم بـه وسـیله $x^z \pmod N$ ضرب می شوند، استفاده از یک حقه بدون محاسبه، عناصـر رجیـسترسوم را بـه محـض تکمیل شدن پاک مـی کنـد. الگـوریتم بـرای محاسـبه دنبالـه نمـایی دو مرحلـه دارد. مرحلـه اول از

توان‌رسانی پیمانه‌ای استفاده می کند تا $x^2 (\text{mod } N)$ را به وسیله مربع کـردن x moduloN محاسـبه کند. سپس $x^4 (\text{mod } N)$ را به وسیله توان دوم $x^2 (\text{mod } N)$ محاسبه می‌کنـد و ایـن روش ادامـه پیـدا می‌کند تا $x^{2^j} (\text{mod})$ برای همه j ها تا t-1 محاسبه شود.

از $t = 2L + 1 + \left\lceil \log(2 + \frac{1}{2\varepsilon}) \right\rceil = O(L)$ بیت استفاده می کنیم، بنابراین تمام t-1=O(L) عمل مربـع در $O(L^2)$ عمل انجام می شود. بنابراین تعداد کل عملیات مرحله اول $O(L^3)$ است.

مرحله دوم الگوریتم بر روی مشاهده پایه‌ریزی شده است. به خاطر داریم که:

$$x^z (\text{mod } N) = \left(x^{z_t 2^{t-1}} (\text{mod } N)\right)\left(x^{z_{t-1} 2^{t-2}} (\text{mod } N)\right)..\left(x^{z_1 2^0} (\text{mod } N)\right) \qquad (۴۳-۴)$$

با انجام t-1 ضرب پیمانه ای که هر کدام $O(L^2)$ عمل دارد ، می بینیم که نتیجه می تواند بـا اسـتفاده از $O(L^3)$ گیت محاسبه شود. این عمل برای فرض ما مناسب است، اما بیشتر الگوریتم های مناسب بر پایه ضرب کردن الگوریتم ها هستند. حال می توان یک مدار معکوس با یـک رجیـستر t بیتـی و یـک رجیستر L بیتی ساخت که در ورودی حالت (z,y) را داراست و در خروجی $(z, x^z y \ (\text{mod}N))$ را بـا استفاده از $O(L^3)$ گیت می دهد. این مدار کوانتومی به این معنی است که با اسـتفاده از $O(L^3)$ گیـت تبدیل زیر را محاسبه می کند:

$$|z\rangle|y\rangle \rightarrow |z\rangle|x^z y \ (\text{mod} \quad N)\rangle \qquad (۴۴-۴)$$

۴-۴-۳- بسط کسرهای تکرار شونده:

تبدیل پیداکردن مرتبه با تخمین فاز با این توضیح کامل می شود که چگونه پاسخ خواسـته شـده r از نتیجه الگوریتم تخمین فاز یعنی $\varphi \approx \frac{s}{r}$ بدست می آید ؟ فقط می دانیم φ دارای 2L+1 بیـت اسـت، اما همچنین مقدمه‌ای درباره عددگویا (نسبت دوعدد صحیح معین) می دانیم. اگر بتـوانیم نزدیکتـرین کسر نظیر φ را محاسبه کنیم، می توانیم r را بدست بیاوریم.

یک الگوریتم به نام الگوریتم کسرهای تکرار شونده وجود دارد که به طور موثر این کار را انجام می دهد. دلیل اینکه این الگوریتم توانایی این کار را دارد در قضیه زیر آمده است.

قضیه: فرض کنید $\frac{s}{r}$ یک عدد گویا است به طوریکه:

$$\left|\frac{s}{r}-\varphi\right| \le \frac{1}{2r^2} \qquad (۴۵-۴)$$

پس $\frac{s}{r}$ یک سری همگرا از کسرهای تکرار شونده برای φ است وبنابراین می تواند در $O(L^3)$ عملیات با استفاده از الگوریتم کسرهای تکرار شونده محاسبه شود.

چون φ یک تقریب دقیق از φ با 2L+1 بیت است، از $\left|\frac{s}{r}-\varphi\right| \le 2^{-2L-1} \le \frac{1}{2r^2}$ پیروی می کند، چون $r \le N \le 2^L$. بنابراین قضیه کاربرد دارد.

به طور خلاصه φ مفروض الگوریتم کسرهای تکرار شونده به طور مناسب اعداد r', s' را بدون هیچ عامل مشترکی تولید می کند به طوریکه $\frac{s'}{r'} = \frac{s}{r}$. عدد r' یک کاندید برای مرتبه است. می توانیم با یک کنترل با محاسبه $x^{r'} \bmod N$ ببینیم که r' مرتبه مورد نظر است یا خیر. اگر نتیجه محاسبه ۱ باشد پس r' مرتبه x modulo N است و به نتیجه دلخواه رسیده‌ایم.

۴-۴-۴-کارآیی:

حال می خواهیم ببینیم چگونه الگوریتم پیداکردن مرتبه با شکست مواجه می شود. در دو صورت این اتفاق می افتد: اول وقتی که روش تخمین فاز یک تخمین بد از $\frac{s}{r}$ تولید کند. که این اتفاق با احتمال زیاد ε رخ می دهد و می تواند با چشم پوشی در اندازه مدار این احتمال کوچک می شود. وضعیت وخیم تر وقتی است که s وr عامل مشترک داشته باشند. در این حالت عدد r' به وسیله الگوریتم کسرهای تکرار شونده به یک عامل از r بر می گردد و به خود r برنمی گردد. خوشبختانه سه راه برای این مسئله وجود دارد.

شاید سرراست ترین راه این است که s به طور تصادفی در بازه 0 و r-1 انتخاب شود، که در این صورت با احتمال خیلی بالا s وr نسبت به هم اول هستند و عامل مشترکی ندارند. در این حالت الگوریتم کسرهای تکرار شونده به r برمی گردد. با دیدن این حالت توجه شود که تعداد اعداد اول کمتر از r تقریباً $\frac{r}{2}\log r$ است وبنابراین احتمال اینکه s عدد اول باشد (وبنابراین نسبت به r اول است) تقریباً $\frac{1}{2}\log(r) > \frac{1}{2}\log(N)$ است. بنابراین با تکرار الگوریتم در 2log (N) مرحله با احتمال خیلی زیاد یک فاز $\frac{s}{r}$ که در آن s وr نسبت به هم اول هستند را مشاهده خواهیم کرد و بنابراین کسرهای تکرار شونده (دنباله دار) r را همان طور که انتظار داریم تولید می کند.

روش دوم به این نکته توجه می کند که اگر r≠r′ باشد، پس مطمئناً r′ یک عامل (فاکتور) r است، مگر اینکه s=0 باشد که این اتفاق با احتمال $\frac{1}{r} \le \frac{1}{2}$ رخ می دهد و می‌تواند به وسیله چند تکرار کم شود. فرض کنید a را با $a' \equiv a^{r'} (\mathrm{mod}\, N)$ جایگزین می‌کنیم . پس مرتبه a′ در اینجا $\frac{r}{r'}$ است. اکنون می‌توانیم الگوریتم را تکرار کنیم، و سعی می کنیم مرتبه a′ را محاسبه کنیم، که اگر موفق شویم اجازه می دهد که مرتبه a را محاسبه کنیم، چون $r = r' \times \frac{r}{r'}$. اگر شکست بخوریم، پس r″ را که یک عامل از $\frac{r}{r'}$ است را بدست می‌آوریم. و اکنون سعی می کنیم که مرتبه $a'' \equiv (a')^{r''} (\mathrm{mod}\, N)$ را محاسبه کنیم. این روش را آنقدر تکرار می کنیم تا زمانیکه مرتبه a را تعیین کنیم. حداکثر تکرارهایی که نیاز داریم log (r)=O(L) است، از این رو هر تکرار مرتبه $a''' \cdots$ را به وسیله یک عامل حداقل دو کاهش می دهد.

روش سوم که از دو روش اول بهتر است، به طور کلی به تنها یک عدد ثابت از دنباله ها نسبت به O(L) تکرار نیاز دارد. طبق یک نظر با تکرار دوبار روش تخمین کسرهای تکرار شونده در مرحله اول r_1', s_1' و در مرحله دوم r_2', s_2' بدست می آیند. s_2', s_1' که تهیه شده‌اند بایدعامل مشترک نداشته

باشند، r ممکن است باگرفتن کوچکترین مضرب مشترک r_2, r_1 بدست بیاید. احتمال اینکه s_2', s_1' عامل مشترک نداشته باشند به وسیله رابطه زیر داده می شود:

$$1-\sum_q P(q|s_1')P(q|s_2') \qquad (۴۶-۴)$$

که جمع بر روی همه اعداد اول q است و P(x| y) در اینجا به معنی احتمال x تقسیم بر y است. اگر q ،s′ را تقسیم کند پس همچنین مقدار واقعی s و s_1 را در تکرار اول تقسیم می کند. بنابراین حد بالای P(q| s_1′) با حد بالای P(q| s_1) متناسب است که s_1 به شکل تصادفی از 0 تا r-1 انتخاب می شود. به آسانی می بینیم که $P(q|s_1) \le \frac{1}{q}$ وبنابراین $P(q|s_1') \le \frac{1}{q}$. به طور مشابه $P(q|s_2') \le \frac{1}{q}$ وبنابراین احتمال اینکه s_2', s_1' عامل مشترک نداشته باشند برآورده می شود با:

$$1-\sum_q P(q|s_1')P(q|s_2') \ge 1-\sum_q \frac{1}{q^2} \qquad (۴۷-۴)$$

در طرف راست حد بالا می‌تواند به چند روش محدود شود.

چون برای همه x≥2 ثابت می شود که $\int_x^{x+1} \frac{1}{y^2}dy \ge \frac{2}{3}x^2$ پس داریم:

$$\sum_q \frac{1}{q^2} \le \frac{3}{2}\int_2^{\infty} \frac{1}{y^2}dy = \frac{3}{4} \qquad (۴۸-۴)$$

پس نتیجه زیر حاصل می شود:

$$1-\sum_q P(q|s_1')P(q|s_2') \ge 1-\frac{3}{4} = \frac{1}{4} \qquad (۴۹-۴)$$

وبنابراین احتمال بدست آوردن r درست تقریباً $\frac{1}{4}$ است.

حال ببینیم این الگوریتم تحلیلی به چه منابعی نیاز دارد؟ تبدیل هادامارد به O(L) گیت نیاز دارد و تبدیل فوریه معکوس به $O(L^2)$ گیت نیاز دارد. که در مجموع به $O(L^3)$ گیت نیاز دارد. الگوریتم کسرهای تکرار شونده گیتهای بیشتر از $O(L^3)$ اضافه می کند تا r′ بدست بیاید. با استفاده از روش

سوم برای بدست آوردن r از r' نیاز داریم که فقط این روش را به یک تعداد ثابت تکرار کنیم تا مرتبه r بعد از همه مراحل $O(L^3)$ بدست بیاید. الگوریتم در زیر خلاصه شده است.

۴-۴-۵- الگوریتم پیداکردن مرتبه کوانتومی:

ورودی ها :

۱) یک جعبه سیاه $U_{x,N}$ که تبدیل $|j\rangle|k\rangle \to |j\rangle|x^j k \bmod N\rangle$ را برای یک x در L بیت که نسبت به N اول است انجام می دهد.

۲) $t = 2L+1+\left\lceil \log(2+\frac{1}{2\epsilon}) \right\rceil$ کیوبیت اولیه در حالت $|0\rangle$.

۳) L کیوبیت اولیه در حالت $|1\rangle$.

خروجی ها : یک لیست r>0 به طوریکه $x^r = 1 (\bmod N)$.

تعداد مراحل : $O(L^3)$ عملیات . احتمال موفقیت O(1).

روش :

۱. حالت اولیه $|0\rangle|1\rangle$

۲. ایجاد ترکیب $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t} |j\rangle|1\rangle$

۳. به کار بردن $U_{x,N}$ $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t} |j\rangle|x^j \bmod N\rangle$

$$\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j / r} |j\rangle|u_s\rangle$$

۴. به کار بردن تبدیل فوریه معکوس با رجیستر اول $\to \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\tilde{s/r}\rangle|u_s\rangle$

۵. اندازه گیری رجیستر اول $\to \tilde{s/r}$

۶. به کار بردن الگوریتم کسرهای تکرار شونده $\rightarrow r$

۴-۵- الگوریتم شر[1]

۴-۵-۱- تعریف

یک نمونه از مسائل دشوار در نظریه اعداد، مسئله تجزیه یک عدد به عاملهای اول آن است. هر گاه عددی مثل N داشته باشیم و بخواهیم یکی از عاملهای آنرا پیدا کنیم، بهترین الگوریتم های کلاسیکی این کار را در زمانی از مرتبه $O\left(\exp\left(\log N^{\frac{1}{3}}\right)\left(\log\log N^{\frac{2}{3}}\right)\right)$ انجام می دهند. شر نشان داد که با استفاده از الگوریتمهای کوانتومی می‌توان این مسئله را در زمان چند جمله‌ای حل کرد. حل این مسئله توسط شر علت اصلی توجه بسیار زیاد جامعه فیزیک، ریاضی و علوم کامپیوتر به کامپیوترهای کوانتومی در دهه اخیر بوده است. حال این الگوریتم را به دقت توضیح می دهیم.

۴-۵-۲- مبنای الگوریتم شر

در این بخش نشان می دهیم که مسئله یافتن یک عامل اول از یک عدد مثل N بامسئله یافتن دوره تناوب یک تابع معین یکسان است. فرض کنید که عددی غیر بدیهی مثل x را چنان بیابیم که در معادله زیر صدق کند:

$$x^2 = 1 \bmod N \qquad (۵۰-۴)$$

منظور از جواب غیر بدیهی این است که:

$$x \neq 1,-1 \bmod N \qquad \begin{cases} x - 1 \neq kN \\ x + 1 \neq kN \end{cases} \qquad (۵۱-۴)$$

در این صورت می توانیم بنویسیم:

$$x^2 - 1 = 0 \bmod N \Rightarrow (x-1)(x+1) = kN \qquad (۵۲-۴)$$

[1]. shor

این معادله به این معناست که حاصلضرب (x+1)(x-1) برN بخش پـذیر اسـت. امـا از آنجـا کـه بنـابر معادله (۴-۵۱) هیچ کدام از اعداد (x-1) یا (x+1) برN بخش پذیر نیستند، پس نتیجه می گیریم کـه N تنها می‌تواند فاکتورهای مشترکی با یکی یا هر دو عـدد داشـته باشـد. اکنـون بـرای درک بیـشتر موضوع چند مثال ذکر می‌کنیم.

مثال ۱: فرض کنید N=۱۵ و x =۴. در این صورت داریم:

$$x^2 = 4^2 = 16 = 1 \bmod 15 \qquad (۴-۵۳)$$

ضمنا x-1=3 و x+1=5 مضرب هایی از ۱۵ نیستند (یعنی۳ و ۵ بر۱۵ بخش پذیر نیستند ولی عدد ۳×۵ بر ۱۵ بخش پذیر است.) از رابطه (۴-۵۲) نتیجه می‌گیریم کـه ۱۵ مـضربی از ۳×۵ اسـت و ایـن تنها وقتی ممکن است که ۱۵ با ۳ یا ۵ عامل مشترکی داشته باشد.

در مثال قبل عدد x کوچکتر از N بود ولی x می تواند هر عدد دلخواه کـوچکتر یـابزرگتر از N باشـد. حال به مثال بعد توجه کنید.

مثال۲: فرض کنیدN=۱۵ و x =۱۳۹. در این صورت داریم:

$$x^2 = (139)^2 = 19321 = 1 \bmod 115 \qquad (۴-۵۴)$$

ضمناً x -۱=۱۳۸ و x +۱=۱۴۰ مضرب هایی از۱۱۵ نیستند و از رابطه فـوق نتیجـه مـی‌گیـریم کـه حاصلضرب ۱۳۸×۱۴۰ مضربی از ۱۱۵ است و این تنها وقتی ممکـن اسـت کـه ۱۱۵بـا ۱۳۸ یـا ۱۴۰ عامل مشترک داشته باشد.

پس ازاین به راحتی می توانیم عامل مشترک دوعدد N وx-1 یا x+1 را پیدا کنیم. یک الگـوریتم کـه به نام الگوریتم اقلیدس مشهور است بزرگترین مقسوم علیـه مـشترک ایـن دو عـدد را در زمـان چنـد جمله‌ای پیدا می کند.

پس مسئله پیدا کردن یک عامل از عدد N به مسئله یافتن عددی مثل x که در شرط زیرصـدق کنـد تبدیل می شود:

$$x^2 = 1 \bmod N \qquad (۴-۵۵)$$

برای حل این مسئله به ترتیب زیر اقدام می کنیم. عددی دلخواه مثل Yرا در نظر می گیریم به طوری که رتبه این عدد r باشد. هرگاه:

$$Y^r = 1 \bmod N \qquad (۵۶-۴)$$

در نظریه اعداد نشان می دهند که تقریباً نیمی از این گونه اعداد رتبه زوج و نیمی دیگر رتبه فرد دارند. بنابراین اگریک عدد تصادفی مثل Y اختیار کنیم و بتوانیم رتبه آن را پیدا کنیم به احتمال $\frac{1}{2}$ رتبه این عدد زوج خواهد بود. این رتبه را با r=2k نشان می دهیم. در نتیجه خواهیم داشت:

$$Y^r = Y^{2K} = 1 \bmod N \rightarrow X = Y^k, X^2 = 1 \bmod N \qquad (۵۷-۴)$$

بنابراین مشروط براینکه رتبه عدد Y را بتوانیم پیدا کنیم عدد X و درنتیجه یک عامل از N را پیدا خواهیم کرد. آنچه که شر انجام داده است ارایه یک الگوریتم برای پیدا کردن رتبه یک عدد دلخواه است. این کار چیزی جز یافتن پریود[1] نیست، زیرا هر گا ه تابعی به صورت زیر تعریف کنیم:

(۵۸-۴)

آنگاه: $f(x) = Y^X \bmod N$

$$f(x+r) = f(x) \rightarrow f(x+jr) = f(x) \quad ; \ j=1,2,3,... \qquad (۵۹-۴)$$

بنابراین مسئله یافتن مرتبه عدد Y عبارت است از پیدا کردن دوره تناوب تابع فوق و برای آن می توان یک الگوریتم به کار برد.

۴-۵-۳- مراحل الگوریتم شر

می توانیم مسئله را به شکل کلی تری طرح کنیم وآن اینکه هر گاه تابعی متناوب دلخواه مثل تابع $f : Z_N \rightarrow Z_N$ داشته باشیم، چگونه می توانیم دوره تناوب آنرا پیدا کنیم؟ اگردوره تناوب این تابع r باشد چند بار باید تابع را بخوانیم تا بتوانیم r را پیدا کنیم؟ کمی دقت نشان می‌دهد که تعداد دفعات خواندن تابع از مرتبه N است. می خواهیم با استفاده از توازی کوانتومی الگوریتمی بسازیم که

[1] . period finding

بتواند این دوره تناوب r را با کمترین تعداد ممکن از خواندن تابع پیدا کند. برای این کار الگـوریتم را به چند مرحله تقسیم می کنیم.

مرحله اول:

دو register بـه نـام هـای $|REG1\rangle, |REG2\rangle$ را در اختیـار داریـم. حالـت $|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$را تهیـه می کنیم که در آن $|0\rangle^{\otimes n} = |000...0\rangle$ و طول هر کدام از این حالتها چنان است که می‌توان یک عدد بسیار بزرگ مثل Q را در آن نوشت.

فرض می کنیم که این عدد ازN بزرگتر است. حالت $|\Psi_0\rangle$ را تشکیل می دهیم.

$$|\Psi_0\rangle = |REG1\rangle|REG2\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} = |00...0\rangle|00...0\rangle \qquad (۶۰-۴)$$

مرحله دوم:

با اعمال عملگرهای هادامارد H ، حالت اول را به یک ترکیب خطـی از همـه اعـداد 0 تـا Q-1 تبـدیل می کنیم. پس در پایان این مرحله حالت قبل به حالت زیر تبدیل می شود:

$$|\Psi_0\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} \xrightarrow{F} |\Psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} e^{\frac{2\pi i 0 \cdot l}{Q}} |l\rangle \otimes |0\rangle^{\otimes n}$$

$$\rightarrow |\Psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |0\rangle^{\otimes n} \qquad (۶۱-۴)$$

مرحله سوم:

حال با استفاده از تبـدیل یکـانی U_fکـه حالـت $|l\rangle \otimes |0\rangle^{\otimes n}$را بـه $|l\rangle \otimes |f(l)\rangle$ مـی بـرد بـر روی حالت $|\Psi 1\rangle$ اثر می دهیم داریم:

$$|\Psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |0\rangle^{\otimes n} \xrightarrow{U_f} |\Psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |f(l)\rangle$$

$$\rightarrow |\Psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |Y^l \bmod N\rangle \qquad (۶۲-۴)$$

مرحله چهارم:

روی register دوم یک اندازه گیری انجام می دهیم. فرض کنید که نتیجه اندازه‌گیری عدد $Y^{l_0} \bmod N$ باشد، در این صورت حالت register اول به حالت زیر تبدیل می شود:

$$\left|\Phi\right\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} \left|l_0 + jr\right\rangle \qquad (۶۳-۴)$$

در این جا A تعداد دوره های تناوبی است که در فاصله [0,Q-1]جا می شود. بدیهی است که با اندازه‌گیری این حالت نمی توان عدد A و در نتیجه دوره تناوب r را بدست آورد. هم چنین با اندازه‌گیری register اول تنها یکی از اعداد $...,l_0 - 2r, l_0 - r, l_0, l_0 + r, l_0 + 2r,...$ پیدا خواهند شدکه با توجه به اینکه مقدار l_0 را نمی دانیم، نمی توانیم از آن برای تعیین r کمک بگیریم. راهی که باقی می ماند این است که از تبدیل فوریه استفاده کنیم. حال تبدیل فوریه را روی Z_Q به کار می بریم. فرض می کنیم که $Q = 2^n$ و بنابراین تبدیل فوریه روی گروه Z_{2^n} تعریف می شود.

$$U\left|k\right\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} e^{\frac{2\pi i k l}{Q}} \left|l\right\rangle \qquad (۶۴-۴)$$

پس از انجام تبدیل فوریه حالت $\left|\Phi\right\rangle$ به حالت زیر تبدیل می شود:

$$\left|\Phi\right\rangle \xrightarrow{F} \left|\Phi'\right\rangle = \frac{1}{\sqrt{A}} \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \sum_{j=0}^{A-1} e^{\frac{2\pi i k (l_0 + jr)}{Q}} \left|k\right\rangle \qquad (۶۵-۴)$$

مرحله پنجم:

حال register اول را اندازه می گیریم. احتمال اینکه در این اندازه گیری مقدار **k** بدست آید برابر است با:

$$P(k) = \left\langle \Phi' \middle| \Phi' \right\rangle = \left(\frac{1}{\sqrt{A}} \frac{1}{\sqrt{Q}}\right)^2 \sum_{k=0}^{Q-1} \left| \sum_{j=0}^{A-1} e^{\frac{2\pi i k (l_0 + jr)}{Q}} \right|^2 \left\langle k \middle| k \right\rangle \qquad (۶۶-۴)$$

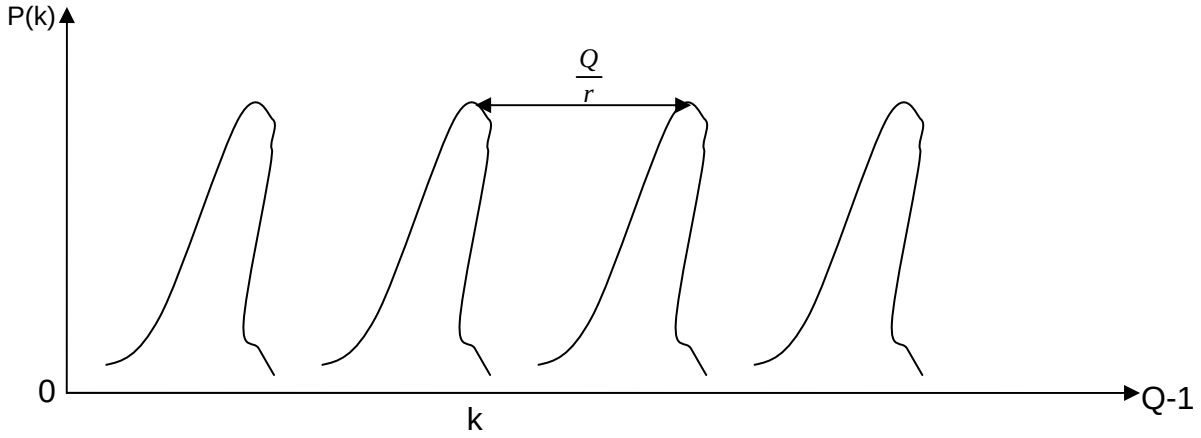
چون داریم:

$$\sum_{k=0}^{Q-1} \left\langle k \middle| k \right\rangle = 1$$

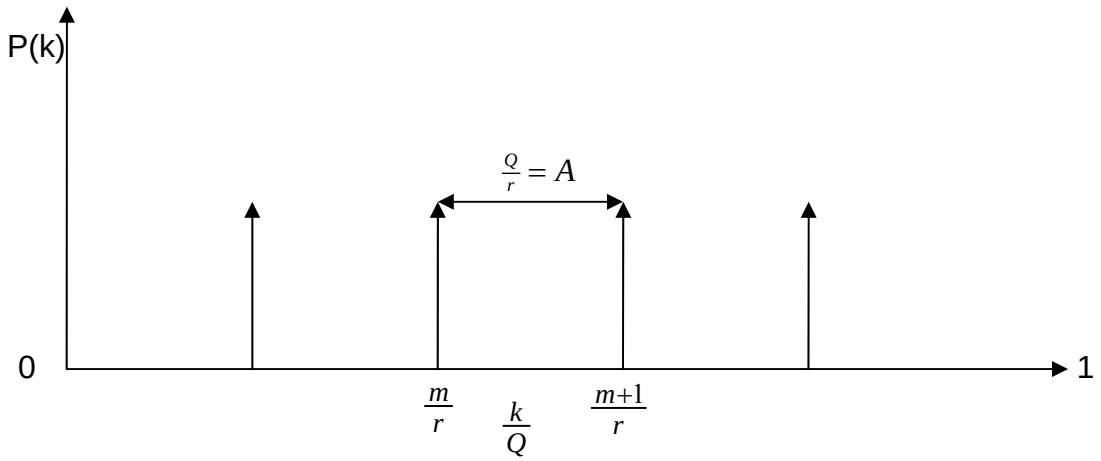
$$\Rightarrow P(k)=\frac{1}{QA}\left|\sum_{j=0}^{A-1}e^{\frac{2\pi ik(l_0+jr)}{Q}}\right|^2=\frac{1}{QA}\left|\sum_{j=0}^{A-1}e^{\frac{2\pi ikjr}{Q}}\right|^2$$

$$\Rightarrow P(k)=\frac{1}{QA}\left|\frac{1-e^{\frac{2\pi ikrA}{Q}}}{1-e^{\frac{2\pi ikr}{Q}}}\right|^2=\frac{1}{QA}\left|\frac{\sin\frac{\pi krA}{Q}}{\sin\frac{\pi kr}{Q}}\right|^2 \qquad (۶۷-۴)$$

این تابع تقریبا تناوبی است و دوره تناوب آن حدودا $A\cong\frac{Q}{r}$ است. بنـابراین در فـا صـله [0,Q -1] شکل این تابع به طور تقریبی A بار تکرار می شود (شکل (۴-۶)).



شکل (۴-۶): شکل تابع P(k) در حالت کلی وقتی که $\frac{Q}{r}$ عدد صحیحی نباشد.



شکل (۴-۷): شکل تابع P(k) در حالتی که $\frac{Q}{r}$عدد صحیحی باشد. این عدد صحیح همان A است.

مرحله ششم:

حال به تحلیل نتایج می پردازیم:

حالت اول:

نخست حالت ساده‌ای را در نظر می گیریم که Q مضرب صحیحی از دوره تناوب است. دراین صورت $A=\frac{Q}{r}$ و در نتیجه از رابطه (۴-۶۷) معلوم می شود که جمع سری هندسی برابر صفر است مگر در مواقعی که $\frac{kr}{Q}$ خود عدد صحیحی مثل m باشد که در این صورت جمع سری برابر با $\frac{1}{QA}A^2=\frac{1}{r}$ خواهد بود.

بنابراین در این حالت تابع احتمال برابر است با:

$$P(k)=\frac{1}{QA}\left|\frac{\sin\frac{\pi krA}{Q}}{\sin\frac{\pi kr}{Q}}\right|^2 \qquad \Rightarrow P(k)=\frac{1}{r}\delta_{\frac{k}{Q},\frac{m}{r}} \qquad (۴-۶۸)$$

$$if \quad m=\frac{kr}{Q}\rightarrow\frac{m}{r}=\frac{k}{Q}$$

تابع P(K) در این حالت مطابق شکل (۴-۷) است. این رابطه بیان می کند که در این حالت هر بار که register اول را اندازه بگیریم عددی بدست می آوریم که اگر آن را بر Q تقسیم کنیم کسری مثل $\frac{m}{r}$ بدست می‌آید. به عنوان مثال اگر r برابر ۱۰۰ باشد در اندازه‌گیری register اول یکی از اعداد زیر بدست خواهند آمد.

$$\left\{\frac{0}{100},\frac{1}{100},\frac{2}{100},\frac{3}{100},\cdots,\frac{99}{100}\right\}$$

مخرج این کسرها همان دوره تناوب r (در اینجا r=۱۰۰) است. البته باید توجه داشت که تعدادی از کسرهای فوق مثل $\frac{2}{100},\frac{4}{100},\frac{5}{100}$ و یا مثلا $\frac{50}{100}$ به ترتیب منجر به مخرج هایی مثل ۵۰،۲۵،۲۰ و یا ۲ می شوند که هیچکدام دوره تناوب واقعی نیستند. نکته این است که تعداد قابل ملاحظه ای از کسرهای دیگر وجود دارند که صورت و مخرج آنها نسبت به هم اول هستند و ساده نمی شوند مثل $\frac{19}{100},\frac{13}{100},\frac{11}{100},\frac{7}{100},\frac{3}{100}$ و نظایر آن.

در واقع برای اعداد بزرگ r تعداد اعداد کوچکتر از r که نسبت به آن اول هستند ازمرتبه $\frac{r}{\ln r}$است. و

این به این معناست که در هر ۱۰۰ بار اندازه گیری، حدودا $100\times\frac{1}{\ln r}$ دفعه آن به اعداد ساده نشدنی بر می‌خوریم که مخرج انها از همه مخرج های دیگر بزرگتر است. این مخرج ها همان دوره تناوب مورد نظر هستند.

حالت دوم:

تحلیل قبلی مربوط به یک حالت ایده آل بود که فرض کرده بودیم عدد Q مضرب صحیحی از دوره تناوب است و در نتیجه A دقیقاً برابر $\frac{Q}{r}$ است. ولی چون دوره تناوب را از قبل نمی دانیم این فرض صحیح نیست و تنها چیزی که می دانیم آن است که جز صحیح $\frac{Q}{r}$ یعنی $\left[\frac{Q}{r}\right]$ برابر A است.

در این حالت K هایی که اندازه می گیریم دیگر به صورت $Q\left(\frac{m}{r}\right)$ نخواهند بود و براحتی نمی توان از روی آنها r را تعیین کرد. تابع P(k) در این حالت مطابق شکل (۴-۷) دیگر مجموعه ای از توابع دلتای کرونکر در نقاط $\frac{m}{r}$ نخواهد بود. این تابع هنوز شکل تناوبی خود را حفظ می کند ولی هر تابع دلتای کرونکر کمی پهن می شود، به این معنا که بجز مقادیر $\frac{m}{r}$ مقادیر نزدیک آن نیز بدست می آیند. برا ی جلو رفتن دو کار انجام می دهیم.

الف) k های مناسب را k هایی تعریف می کنیم که در شرط زیر صدق کنند.

$$\left|\frac{k}{Q}-\frac{m}{r}\right|\le\frac{1}{2Q} \qquad (۶۹-۴)$$

به عبارت دقیق تر اختلاف K ها با $Q\left(\frac{m}{r}\right)$ از $\frac{1}{2}$ کمتر است.

نشان خواهیم داد که چرا این K ها مناسب هستند. و نشان خواهیم داد که باز هم می توان از این K ها دوره تناوب r را پیدا کرد. این امر در قضیه زیر بیان شده است.

قضیه: اگر Q به اندازه کافی بزرگ باشد، کسر $\frac{k}{Q}$ را تنها به یک صورت می توان به صورت کسری با مخرج کوچکتر از N ساده کرد. اگر این کسر را به صورت $\frac{m}{r}$ بنویسیم، r همان دوره تناوب خواهد بود. (یاد آوری می کنیم که r از N کوچکتر است.)

اثبات: فرض کنید که علاوه بر کسر $\frac{m}{r}$، کسر $\frac{m'}{r'}$ نیز در شرط (۴-۶۹) صدق کند.

یعنی داریم:

$$\left|\frac{k}{Q}-\frac{m'}{r'}\right| \le \frac{1}{2Q} \qquad (۴-۷۰)$$

در این صورت با جمع دو نا مساوی فوق و استفاده از نامساوی مثلث به رابطه زیر می رسیم:

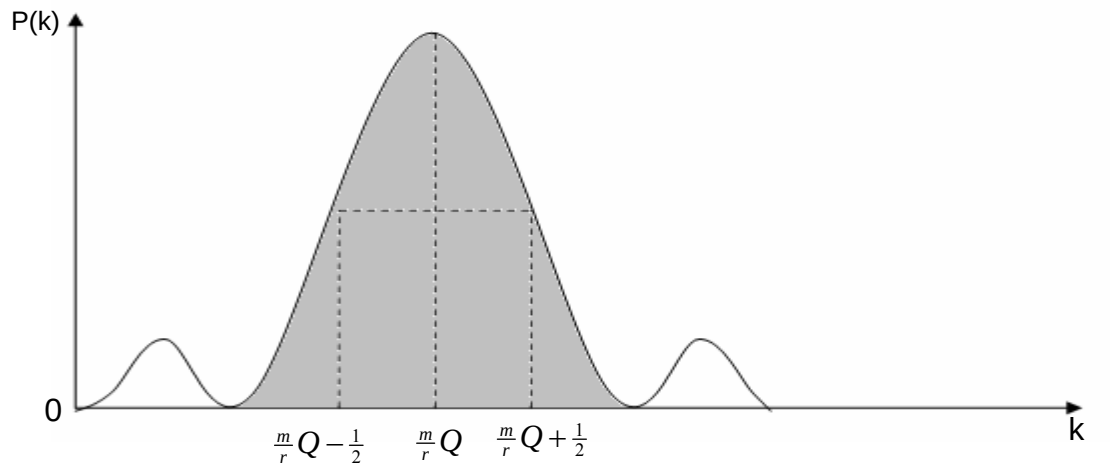
$$\left|\frac{m}{r}-\frac{m'}{r'}\right| \le \frac{1}{Q} \qquad (۴-۷۱)$$

ازطرفی می دانیم که:

$$\left|\frac{m}{r}-\frac{m'}{r'}\right| = \left|\frac{mr'-m'r}{rr'}\right| \ge \frac{1}{N^2} \qquad (۴-۷۲)$$

از (۴-۷۱) و (۴-۷۲) به این نتیجه می‌رسیم که اگر Q را از N^2 بزرگتر انتخاب کنیم وجود دو کسر با مخرج کوچکتر از N اتفاق نخواهد افتاد.

ب) نشان‌می دهیم که احتمال پیدا کردن یک K مناسب به اندازه کافی بالاست. به عبارت دقیق تر نشان خواهیم داد که احتمال یافتن چنین K هایی از $\frac{4}{\pi^2}$ بیشتر است. برای این کار به شکل تابع $P(k)=\frac{1}{QA}\left|\frac{\sin\frac{\pi krA}{Q}}{\sin\frac{\pi kr}{Q}}\right|^2$ در اطراف یکی از نقطه ها، مثلا نقطه $k=\frac{Q}{r}$ نگاه می‌کنیم. در شکل (۴-۸) تابع P(k) در نزدیکی یکی از نقطه ها رسم شده است. دقت کنید که این تابع را بر حسب $\frac{k}{Q}$ رسم کرده‌ایم و تنها یکی از دوره های تناوب تابع را نشان داده‌ایم.



شکل (۴-۸): شکل تابع p(K) در نزدیکی یکی از نقاط $\frac{k}{Q}=\frac{m}{r}$ ، شکل کامل تکراری از این منحنی است و تعداد تکرارها نیز r است.

سطح هاشورخورده احتمال پیدا کردن یک k مناسب در اطراف این نقطه را نشان می دهد که هنوز می توان با دانستن این k دوره تناوب r را پیدا کرد.

مساحت سطح هاشور خورده بیشتر از مساحت سطح مستطیل نشان داده شده است. مساحت مستطیل برابر است با:

$$S=\left[\left(\frac{m}{r}Q+\frac{1}{2}\right)-\left(\frac{m}{r}Q-\frac{1}{2}\right)\right]\times p\left(k=\frac{m}{r}Q+\frac{1}{2}\right)=2\times\frac{1}{2}\times p\left(k=\frac{1}{2}\right)$$

$$S=p(k=\tfrac{1}{2})=\frac{1}{QA}\left|\frac{\sin\frac{\pi rA}{2Q}}{\sin\frac{\pi r}{2Q}}\right|^2 \qquad (۷۳-۴)$$

اما می دانیم که $\frac{\pi r}{2Q}\langle\langle 1$ و $Q\approx Ar$، در نتیجه این عبارت تقریبا برابر است با:

$$S=\frac{4}{\pi^2}\frac{1}{r} \qquad (۷۴-۴)$$

بنابراین مساحت هاشورخورده از این مقدار بیشتر است و از آنجا که تعداد r تا پریود داریم احتمال پیدا کردن k های مناسب از $\frac{4}{\pi^2}$ بیشتر خواهد بود.

به طور خلاصه در حالت اول که Q مضرب صحیحی از یک دوره تناوب است در اندازه‌گیری register اول به طورقاطع اعدادی بدست می آوریم که هر گاه آنها را برQ تقسیم کنیم اعدادی به صورت $\frac{m}{r}$ بدست می آیند و درحالت دوم با احتمال بیشتر از $\frac{4}{\pi^2}$اعدادی بدست می آوریم که

می توان آنها را به صورت $\frac{m}{r}$ نوشت. در هر صورت می توان r را در زمان چند جمله ای پیدا کرد. تنها چیزی که از الگوریتم شر باقی مانده است آن است که نشان دهیم تبدیل فوریه کوانتومی را می توان به صورت یک مدار کوانتومی با تعداد کمتری عملگر ساخت. این کار را در بخش بعد انجام می دهیم.

۴-۵-۴- تبدیل فوریه کوانتومی در الگوریتم شر

تبدیل فوریه کوانتومی را به صورت یک نگاشت خطی به صورت زیر تعریف می کنیم. فرض کنید یک فضای هیلبرت N بعدی داریم که بردارهای پایه آن را با $\{|0\rangle,|1\rangle,|2\rangle,...,|N-1\rangle\}$ نشان می دهیم. در این صورت تبدیل فوریه کوانتومی (QFT) به صورت زیر تعریف می شود:

$$U|k\rangle = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}}|l\rangle \qquad (۷۵-۴)$$

هر گاه $|f\rangle$ یک بردار دلخواه در این فضا باشد، مولفه های این بردار تحت تبدیل فوریه به شکل زیر تبدیل خواهند شد:

$$\langle k|U|f\rangle = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}}\langle l|f\rangle \qquad (۷۶-۴)$$

ویا:

$$\tilde{f} = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}} f_l \qquad (۷۷-۴)$$

۴-۵-۵- یک مدار کوانتومی برای محاسبه تبدیل فوریه کوانتومی

برای سادگی فرض می کنیم که N عدد مثل $2^m - 1$ است می دانیم که تبدیل فوریه کوانتومی به شکل زیر است:

$$U|a\rangle = \frac{1}{\sqrt{N}}\sum_{b} e^{2\pi iab}|b\rangle \qquad ,a,b \in Z \qquad (۷۸-۴)$$

در یک کامپیوتر کوانتومی داریم:

$$a = \sum_{j=1}^{m} a_j 2^{m-j}$$
$$|a\rangle = |a_1 a_2 ... a_m\rangle = \bigotimes_{j=1}^{m-1}|a_j\rangle \qquad (۷۹-۴)$$

مثلا عدد ۲۳ در کامپیوتر کوانتومی به شکل زیر نشان داده می شود:

در n کیوبیت (qbit):
$$\left|23\right\rangle = \left|1011100...0\right\rangle$$

$$a = (a_1, a_2, ..., a_m) = a_1 \times 2^{m-1} + a_2 \times 2^{m-2} + ... + a_m \times 2^0 \qquad (۸۰\text{-}۴)$$

$$b = (b_1, b_2, ..., b_m) = b_1 \times 2^{m-1} + b_2 \times 2^{m-2} + ... + b_m \times 2^0 \qquad (۸۱\text{-}۴)$$

بنابراین:

$$U\left|a\right\rangle = \frac{1}{\sqrt{2^m}} \sum_b e^{\frac{2\pi i a}{2^m}\left[b_1 \times 2^{m-1} + b_2 \times 2^{m-2} + ... + b_m \times 2^0\right]} \left|b\right\rangle$$

$$= \left(\frac{1}{\sqrt{2}} \sum_{b_1} e^{\frac{2\pi i a b_1}{2}} \left|b_1\right\rangle\right)\left(\frac{1}{\sqrt{2}} \sum_{b_2} e^{\frac{2\pi i a b_2}{2^2}} \left|b_2\right\rangle\right)...\left(\frac{1}{\sqrt{2}} \sum_{b_m} e^{\frac{2\pi i a b_m}{2^m}} \left|b_m\right\rangle\right) \qquad (۸۲\text{-}۴)$$

عبارت سمت راست در رابطه فوق را می توان به صورت زیر نوشت:

$$U\left|a\right\rangle = \left(\frac{1}{\sqrt{2}} \sum_{b_1} e^{\frac{2\pi i a_m b_1}{2}} \left|b_1\right\rangle\right)\left(\frac{1}{\sqrt{2}} \sum_{b_2} e^{\frac{2\pi i (2a_{m-1} + a_m) b_2}{2^2}} \left|b_2\right\rangle\right)$$

$$...\left(\frac{1}{\sqrt{2}} \sum_{b_m} e^{\frac{2\pi i \left(2^{m-1} a_1 + ... + 2^0 a_m\right) b_m}{2^m}} \left|b_m\right\rangle\right) \qquad (۸۳\text{-}۴)$$

بنابراین می توانیم بنویسیم:

$$U\left|a\right\rangle = \left|\Phi_1\right\rangle\left|\Phi_2\right\rangle...\left|\Phi_m\right\rangle \qquad (۸۴\text{-}۴)$$

که در آن:

$$\left|\Phi_1\right\rangle = \frac{1}{\sqrt{2}}\left[\left|0\right\rangle + e^{\frac{2\pi i a_m}{2}} \left|1\right\rangle\right]$$

$$\left|\Phi_2\right\rangle = \frac{1}{\sqrt{2}}\left[\left|0\right\rangle + e^{\frac{2\pi i (2a_{m-1} + a_m)}{2^2}} \left|1\right\rangle\right], ... \qquad (۸۵\text{-}۴)$$

حال یک مدار کوانتومی معرفی می کنیم که تبدیل فوریه کوانتومی را انجام دهد.

ابتدا عملگر یک کیوبیتی زیر را معرفی می کنیم:

$$R_k(\alpha)=\begin{pmatrix}1 & 0\\ 0 & e^{\frac{2\pi i\alpha}{2^k}}\end{pmatrix} \qquad (۸۶-۴)$$

با استفاده از روابط فوق داریم:

$$\left|\Phi_1\right\rangle = H\left|a_m\right\rangle$$

$$\left|\Phi_2\right\rangle = R_2(a_m)H\left|a_{m-1}\right\rangle$$

$$\left|\Phi_3\right\rangle = R_2(a_{m-1})R_3(a_m)H\left|a_{m-2}\right\rangle$$

$$\left|\Phi_4\right\rangle = R_2(a_{m-2})R_3(a_{m-1})R_4(a_m)H\left|a_{m-3}\right\rangle,... \qquad (۸۷-۴)$$

هر کدام از عملگرهای $R_k(\alpha)$ در واقع به صورت یک عملگر کنترلی عمل می کند. اگر α مقدار برابر صفر باشد هیچ کاری انجام نمی دهند ولی اگر مقدار α برابر 1 باشد عمل R_k را انجام می دهند. بنابراین به سادگی مدار مربوط به عملگر تبدیل فوریه کوانتومی ساخته می شود.

۴-۵-۶- یک مثال از روند کار الگوریتم شر:

حال نشان می دهیم چگونه عدد $N=91(=7\times 13)$ می تواند با استفاده از الگوریتم شر تجزیه شود.

ابتدا عدد $Q=2^{14}=16384$ را انتخاب می کنیم چون داریم: $N^2\le Q\le 2N^2$

یک عدد تصادفی صحیح و مثبت مثل ۳=Y را انتخاب می کنیم. چون باید داشته باشیم:

$$\gcd(N,Y)=\gcd(91,3)=1 \qquad (۸۸-۴)$$

حال باید دوره تناوب تابع f را پیدا کنیم.

$$f(x)=Y^x \bmod N = 3^x \bmod 91 \qquad (۸۹-۴)$$

دوره تناوب تابع f را نمی دانیم اما از روی محاسبات بدست می آوریم:

جدول۴-۱:مقادیر f(x) بر حسب x برای تعیین دوره تناوب تابع.

x	0	1	2	3	4	5	6	7	…
F(x)	1	3	9	27	81	61	1	3	…

از روی جدول دوره تناوب r=۶ است حال باید آنرا بدست آوریم.

register اول و دوم را داریم:

$$\left|\Psi_0\right\rangle = \left|0\right\rangle \otimes \left|0\right\rangle \qquad (۹۰-۴)$$

حال تبدیل F را اعمال می کنیم:

$$F\left|k\right\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} e^{\frac{2\pi i 0 \cdot l}{Q}} \left|l\right\rangle = \frac{1}{\sqrt{16384}} \sum_{l=0}^{16383} e^{\frac{2\pi i 0 \cdot l}{16384}} \left|l\right\rangle \rightarrow$$

$$\rightarrow \left|\Psi_1\right\rangle = \frac{1}{\sqrt{16384}} \sum_{l=0}^{16383} \left|l\right\rangle \otimes \left|0\right\rangle =$$

$$= \frac{1}{\sqrt{16384}} \left(\left|0\right\rangle\left|0\right\rangle + \left|1\right\rangle\left|0\right\rangle + \left|2\right\rangle\left|0\right\rangle + \ldots + \left|16382\right\rangle\left|0\right\rangle + \left|16383\right\rangle\left|0\right\rangle \right) \qquad (۹۱-۴)$$

حال با استفاده از تبدیل یکانی U_f داریم:

$$U_f \left|x\right\rangle \otimes \left|\, f(x)\right\rangle = \left|x\right\rangle \otimes \left|3^x \bmod 91\right\rangle \qquad (۹۲-۴)$$

$$U_f \left|\Psi_1\right\rangle \rightarrow \left|\Psi_2\right\rangle = \frac{1}{\sqrt{16384}} \sum_{l=0}^{16383} \left|l\right\rangle \otimes \left|3^l \bmod 91\right\rangle =$$

$$= \frac{1}{\sqrt{16384}} \left[\left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|3\right\rangle + \left|2\right\rangle\left|9\right\rangle + \left|3\right\rangle\left|27\right\rangle + \ldots + \left|16382\right\rangle\left|9\right\rangle + \left|16383\right\rangle\left|27\right\rangle \right]$$

حال دوباره تبدیل فوریه را با $register \neq 1$ به کار می بریم. بنابراین حالت سیستم بدست می آید:

$$\left|\Psi_3\right\rangle = \frac{1}{\sqrt{16384}} \sum_{l=0}^{16383} \frac{1}{\sqrt{16384}} \sum_{k=0}^{16383} e^{\frac{2\pi i k l}{16384}} \left|k\right\rangle \left|3^l \bmod 91\right\rangle =$$

$$= \frac{1}{16384} \sum_{l=0}^{16383} \left|k\right\rangle \sum_{l=0}^{16383} e^{\frac{2\pi i k l}{16384}} \left|3^l \bmod 91\right\rangle = \frac{1}{16384} \sum_{l=0}^{16383} \left|k\right\rangle \left|\gamma(k)\right\rangle \qquad (۹۳-۴)$$

که در آن:

$$\left|\gamma(k)\right\rangle = \sum_{l=0}^{16383} e^{\frac{2\pi i k l}{16384}} \left|3^l \bmod 91\right\rangle$$

$$\left|\gamma(k)\right\rangle = \left|1\right\rangle + e^{\frac{2\pi i k}{16384}}\left|3\right\rangle + e^{\frac{2\pi i\, 2k}{16384}}\left|9\right\rangle + e^{\frac{2\pi i\, 3k}{16384}}\left|27\right\rangle + \ldots +$$

$$+ e^{\frac{2\pi i 16381\ k}{16384}}\left|3\right\rangle + e^{\frac{2\pi i 16382\ k}{16384}}\left|9\right\rangle + e^{\frac{2\pi i 16383\ k}{16384}}\left|27\right\rangle \qquad (۹۴-۴)$$

با اندازه گیری register اول داریم:

$$k = 13453 \qquad (۹۵-۴)$$

که احتمال بدست آوردن این k خاص برابر است با:

$$P(k) = 0.3189335551\times 10^{-6} \qquad (۹۶-۴)$$

حال از رابطه (۴-۶۹) داریم:

$$\left|\frac{k}{Q} - \frac{m}{r}\right| \le \frac{1}{2Q}$$

وبا استفاده از این رابطه داریم:

$$\left|\frac{13453}{16384} - \frac{m}{r}\right| \le \frac{1}{2\times 16384} \Rightarrow \frac{m}{r} = \frac{5}{6} \qquad (۹۷-۴)$$

حال به آنچه می خواستیم دست یافتیم.

یعنی دوره تناوب r در این مورد برابر ۶ است. پس داریم:

$$\gcd(r,m) = \gcd(6,5) = 1 \qquad (۹۸-۴)$$

حال با توجه به روابط (۴-۵۶) و (۴-۵۷) داریم:

$$X = Y^k \rightarrow X^2 = Y^{2K} = Y$$

$$Y^{2K} = 1 \bmod N \Rightarrow 3^6 = 1 \bmod 91 \Rightarrow \left(3^6 - 1\right) = 0 \bmod 91 \rightarrow$$

$$\left(\left(3^3\right)^2 - 1\right) = 0 \bmod 91 \rightarrow \left(3^3 - 1\right)\left(3^3 + 1\right) = 0 \bmod 91 \rightarrow$$

$$\Rightarrow 26\times 28 = 0 \bmod 91 \qquad (۹۹-۴)$$

بنابراین N=۹۱ باید با ۲۶ یا ۲۸ مضرب مشترک داشته باشد. حال با محاسبه رابطه زیر می بینیم کـه عدد ۹۱ با ۲۶ مضرب مشترک دارد.

$$\gcd\left(3^3-1,91\right)=\gcd\left(26,91\right)=13 \qquad (۱۰۰-۴)$$

یعنی ۱۳ یک مضرب مشترک ۹۱ و۲۶ است. به این ترتیب عدد N=۹۱ به دو عدد تجزیه مـی شـود و نتیجه حاصل است.

$$\frac{91}{13}=7 \Rightarrow N=91=\left(13\times 7\right) \qquad (۱۰۱-۴)$$

به این ترتیب نتیجه‌ای که انتظار داشتیم بدست می‌آید. [5, 6, 7, 8]

۴-۶- نتیجه‌گیری و پیشنهادات:

با استفاده از مواردی که گفته شد نتیجه می‌گیریم که تبدیل فوریه کوانتومی در بسیاری از کاربردها نقش بسزایی دارد و با استفاده از آن سرعت عملیات افزایش یافته و تعداد مراحل عملیات مورد نظر کاهش می‌یابد. آنچه که ما در این پژوهش استفاده کردیم اسپین $\frac{1}{2}$ بوده است که در آن S_z دو حالتی است، یعنی دو مقدار $\frac{1}{2}+$ و $\frac{1}{2}-$ را دارد. برای مثال در یک رجیستر چهار کیوبیتی، چون در هر کیوبیت دو حالت اسپین بالا و پایین قرار می‌گیرد بنابراین، $2^4=16$ حالت برای بیان رجیستر مورد نظر وجود دارد. حال اگر بخواهیم از اسپین 1 استفاده کنیم، چون S_z دارای سه حالت $1+$ و 0 و $1-$ است بنابراین در یک رجیستر چهار کیوبیتی $3^4=81$ حالت برای نشان دادن رجیستر وجود دارد. حال اگر تعداد کیوبیتها افزایش یابد تعداد حالات بطور نمایی زیاد می‌شود که نشان دادن حالتها به این صورت کار بسیار سخت و غیر ممکنی است. پس باید راهی پیدا کرد که بتوان تعداد مراحل را کاهش داد که این راه همان تبدیل فوریه است. بنابراین می‌توان تبدیل فوریه را توسعه داد تا سرعت عملیات در کامپیوترهای کوانتومی افزایش یابد.

[1] J. J. Sakurai, (revised edition 1999), "**Modern quantum mechanics**", Addison-Wesely, USA.

[2] J. Preskill, (1998), **"Lecture notes for physics 229: Quantum Information and Computation"** , California Institute of Technology.

[3] A. Chatterjee, (2003), **"Introduction to Quantum Computation"**, Saha Institute of Nuclear physics, Kolkata, India,e-print:quant-ph/0312111.

[4] A. Ekert, P. Hayden and H. Inamori, (2007), **"Basic consepts in quantum Computation "** ,University of Oxford, Oxford OX1 3PU, United Kingdom.

[5] M. Nielsen, I. Chuang, (2000), **"Quantum Computation and Quantum Information"** ,Cambridge, United Kingdom.

[6] M. Le Bllac, **"A short Introduction to Quantum Information and Quantum Computation"** , Cambridge Univrsity press, United Kingdom, pp75-105.

[7] S. J. Lomonaco, JR, (2000), **"Lecture on Shor's Quantum Factoring Algorithm version 1.1"** ,e-print: quant- ph/0010034v1.

[8] P. W. Shor, (2001),**"Introduction to Quantum Algorithms"** .e-print:quant-ph/0005003v2.

Abstract:

As we know, the quantum fourier transform has been investigated since 1958. the present research deals with entangled stats and superposition stats in the quantum theory and their features. And also it investigates the quick quantum fourier transform and optimization factoring speed by quantum fourier transform. The significance of the investigation and research about quantum fourier transform is because of its widely use in basic function of quantum computer. Quantum fourier transform is used in many problems of quantum computer such as; in factoring problem, order finding problem, counting solution problem, hidden subgroup problem and discrete logarithm problem. By investigating quantum fourier transform and the above mentioned points, especially factoring to prime numbers, by shor's algorithm which is the result of fourier transform, the numbers in quantum computers is factored with high speed.

Key words:

Quantum fourier transform, entanglement, superposition, factoring, quantum theory, density operator, qubit, gate, phase estimation, shor's algorithm.

*S*hahrood University of Technology

Faculty Physics

Quantum Fourier Transform

Reza Mokarrami Rostami

Supervisor: Hossein Movahhedian

Date: jul 2009