دانشکده علوم

گروه فیزیک

پایان نامه جهت اخذ درجه کارشناسی ارشد رشته فیزیک

گرایش نظری

عنوان پایان نامه

رمز نگاری کوانتومی

استاد راهنما:

دکتر شاهپور مرادی

نگارش:

افسانه امیری

تیرماه ۱۳۹۰

دانشکده علوم

گروه فیزیک

پایان نامه جهت اخذ درجه کارشناسی ارشد رشته فیزیک

گرایش نظری

نام دانشجو:

افسانه امیری

عنوان پایان نامه

رمز نگاری کوانتومی

در تاریخ توسط هیأت داوران زیر بررسی و با درجه به تصویب نهایی رسید.

۱- استاد/استادان راهنمای دکتر با مرتبه ی علمی امضاء

۲- استاد/استادان داور داخل گروه دکتر با مرتبه ی علمی امضاء

۳- استاد/استادان داور خارج از گروه دکتر با مرتبه ی علمی امضاء

چکیده :

رمز نگاری کوانتومی[1] با هدف امن ساختن پروتکل های رمز نگاری به کمک قوانین مکانیک کوانتومی مورد توجه جامعه رمزنگاری قرار گرفته است . امنیت این نوع رمزنگاری ،بر خلاف رمزنگاری کلاسیک ،بر اساس قوانین مکانیک کوانتومی قابل اثبات است .رمزنگاری کوانتومی با ایجاد پروتکل توزیع کلید کوانتومی[2] کاملاً امن مطرح شد. معادل کلاسیک کاملاً امن برای این پروتکل وجود ندارد . پس از این معرفی ، محققان به طراحی نسخه کوانتومی تعداد زیادی از پروتکل های رمزنگاری کلاسیک پرداختند . در این پایان نامه ابتدا در فصل اول مروری اجمالی بر اصول اطلاعات کلاسیکی واطلاعات کوانتومی خواهیم داشت . در فصل دوم به مطالعه رمزنگاری کلاسیکی[3] وبررسی ویژگی های آن می پردازیم . در فصل سوم با معرفی طرح توزیع کلید کوانتومی نشان خواهیم داد که به رمزنگاری کوانتومی تنها برای تولید وتوزیع کلید استفاده می شود ونه برای انتقال اطلاعات این کلید در مراحل بعدی می تواند همراه با هر الگوریتم رمز گذاری[4] (یا رمز گشایی) برای تبدیل پیام به رمز یا بر عکس استفاده شود . در این طرح پروتکل هایی معرفی خواهد شد. این پروتکل ها بر اساس یک کانال ارتباطی که دارای حامل های کوانتومی می باشد ایجاد شده است . همچنین منبع این حامل های کوانتومی فوتونهای موجود در امواج الکترو مغناطیسی هستند ،سپس یکی از این پروتکل ها را به صورت عملی معرفی می کنیم . چندین حمله کلی ،از جمله شنود مکالمات هنگام توزیع اطلاعات در حین اجرای پروتکل مد نظر قرار گرفته است ونشان می دهیم این پروتکل این حملات را شناسایی می کند . در فصل چهارم یک پروتکل را برای فاصله های طولانی به صورت عملی نشان خواهیم داد.

[1] Quantum cryptography
[2] Quantum Key Distribution
[3] Classical Crptography
[4] Encoding

فصل اول

اطلاعات کلاسیکی و کوانتومی

۱- کامپیوتر و فیزیک

کامپیوتر تنها بخشی از دنیایی است که ما آنرا دنیای دیجیتالی می نامیم. پردازش ماشینی اطلاعات، در هر شکلی، بر مبنای دیجیتال و محاسبات کلاسیک انجام میشود در طی نیمه دوم قرن بیستم توسعه علم کامپیوتر منجر به ایجاد یک روش جدید برای فهم فیزیک شد. همه اطلاعات اعم از حروف و اعداد یا وضعیت مودم و موس با مجموعه ای از بیت های متشکل از صفرها و یک ها به کامپیوتر داده می شود. درکامپیوترهای معمولی قوانین فیزیک کلاسیک حاکم است،بیت های اطلاعات، خیلی ساده تعریف می شوند؛ سوئیچ های الکتریکی می توانند روشن یا خاموش باشند. ولی کامپیوترهای کوانتومی با طبیعت دودویی های فیزیک کلاسیک محدود نمی شودکامپیوتر کوانتومی دستگاهی است که یک پدیده ی فیزیکی را بر اساس قوانین فیزیک کوانتومی به صورت منحصر به فردی در می آورد تا به صورت اساسی یک حالت جدیداز پردازش اطلاعات را تشخیص دهد. در واقع روش بهتر و قدرتمندتر برای پردازش اطلاعات پیش رویمان براساس فیزیک کوانتومی می باشد در شرایط کلی، سیستم های فیزیکی مانند پردازش اطلاعات کامپیوتری می توانند سنجیده شوند. حالت اولیه یک سیستم فیزیکی، یک ورودی برای کامپیوتر محسوب می شود و همچنین محاسبات علمی کامپیوتر برای حالت نهایی سیستم فیزیکی استنتاج می شود که خروجی کامپیوتر است. مطالعه علم فیزیک با چنین روشی نه تنها به ما اجازه می دهد که از ابزارهای تئوری علم کامپیوتر و نظریه اطلاعات برای فهم قوانین فیزیک استفاده کنیم، بلکه ما را با یک روش جدید کلی درمورد فیزیک آشنا می کند، ما می توانیم به این صورت فکر کنیم که مقادیر فیزیکی یک سیستم به صورت اطلاعات در آن سیستم نگاه داشته شده است. کامپیوترها سیستم هایی فیزیکی هستند و فیزیک در آینده این دانش نقش تعیین کننده ای خواهد داشت. البته وجود تفاوت بین این دو به معنای حذف یکی و جایگزینی دیگری نیست. بنابراین محاسبات کوانتومی را به عنوان یک زمینه و روش جدید و بسیار کارآمد مطرح می کنیم. وجود چند پدیده مهم که مختص فیزیک کوانتومی است، آن را از دنیای کلاسیک جدا می سازد. این پدیده ها عبارتند از: درهم تنیدگی ، نا جایگزیدگی

به عبارت دیگر فیزیک و محاسبه در بعضی موارد می توانند به صورت دو واژه مترادف باشند که در این حالت قوانین پردازش اطلاعات به طور کامل با قوانین فیزیک مرتبط است. بدین معنی که هرگاه که ما قوانین فیزیکی جدیدی را کشف کنیم محاسبات موجود محتملاً تحت تاثیر واقع خواهد شد.

۱-۲ اطلاعات کلاسیکی

در نظریه اطلاعات کلاسیکی فرض می شود که اطلاعات مطابق با قوانین فیزیک کلاسیکی پایه ریزی شده اند. روش های سنتی برای پردازش اطلاعات و محاسبات به اطلاعات کلاسیکی معروف است. کوچک ترین واحد تشکیل دهنده اطلاعات کلاسیکی بیت نامیده می شود. که به طور کلی به پاسخ های بله یا خیر اشاره دارد. یک بیت می تواند شامل دو مقدار صفر یا یک باشد.در حافظه کامپیوتر میلیونها ترانزیستور و خازن وجود دارد.خازن اطلاعات مربوط به بیت را که یک یا صفر است در خود نگهداری خواهد کرد. خازن مشابه یک ظرف بوده که قادر به نگهداری الکترونها است به منظور ذخیره سازی مقدار" یک" در حافظه، ظرف فوق می بایست از الکترونها پر گردد. برای ذخیره سازی مقدار صفر، می بایست ظرف فوق خالی گردد.مسئله مهم در رابطه با خازن، نشت اطلاعات است (وجود سوراخ در ظرف). بدین ترتیب پس از گذشت چندین میلی ثانیه یک ظرف مملو از الکترون تخلیه می گردد. بنابراین بمنظور اینکه حافظه بصورت پویا اطلاعات خود را نگهداری نماید ، می بایست پردازنده و یا " کنترل کننده حافظه " قبل از تخلیه شدن خازن، مکلف به شارژ مجدد آن بمنظور نگهداری مقدار "یک" باشد.بدین منظور کنترل کننده حافظه اطلاعات حافظه را خوانده و مجددا" اطلاعات را بازنویسی می نماید.عملیات فوق(refresh) ، هزاران مرتبه در یک ثانیه تکرار خواهد شد . رابطه بین تعداد بیت ها و محتوای اطلاعاتی به صورت زیر بیان می شوند:

$$۲^n \geq m \qquad (۱-۱)$$

که m حالت های مختلف برای محتوای اطلاعاتی می باشد وn تعداد بیت های موردنیاز است. اگر بخواهیم تعداد بیت های موردنیاز را برای نمایش اعداد $\{0,1,2,3\}$را به دست آوریم به دو بیت نیاز داریم.

$$m = ۴ \Rightarrow ۲^n = ۴ \quad \& \quad n = ۲$$

Decimal	Binary
0	00
1	01
2	10
3	11

شکل(۱-۱)

شکل(۱-۱) نشان می دهد که برای نمایش اعداد(3-0)به دو بیت نیاز داریم.

۱-۳ محتوای اطلاعاتی در یک پیام

باتوجه به بخش قبل، می توانیم درمورد اندازه گیری اطلاعات بحث کنیم. اگر یک پیام(m) داشته باشیم محتوای اطلاعاتی آن چیست؟ با توجه به معادله(۱-۱) بدست می آید:

$$2^n = m \,. \qquad (۱-۲)$$

این رابطه که توسط رالف هارتلی[1] در سال ۱۹۲۷ بدست آمد، بیان می کند که n بیت در m پیام مختلف ذخیره می شود. به طور مثال، $\log_2 ۱۶ = ۴$ نشان می دهد که ۴ بیت در ۱۶پیام ذخیره شده است.

۱-٤ آنتروپی و تئوری اطلاعات شانون[2]

آنتروپی میزان بی نظمی در فیزیک را بیان می کند. اما اطلاعات، با بی نظمی در تضاد است بنابراین ما خواهیم دید که آنتروپی چگونه محتوای اطلاعاتی یک پیام را بیان می کند. روش هارتلی یک اندازه گیری مقدماتی و پایه از محتوای اطلاعاتی دریک پیام را بیان می کند، اما دانشمند دیگری که شانون نام داشت، نشان داد که می توانیم تخمین درستی از محتوای اطلاعاتی یک پیام بدست آوریم.

1 -Ralph Hartly
2 - Shannon

مطالعات شانون براین اساس بود که اگر یک پیام، دارای احتمال وقوع بالایی باشد، آن گاه هیچ اطلاعات جدیدی از آن بدست نمی آید، در مقابل اگر یک پیام احتمال وقوع پایینی داشته باشد، آن گاه محتوای اطلاعاتی بالایی بدست می آوریم.

اندازه گیری شانون از طریق لگاریتم گرفتن در پایه ۲ از احتمال رخ دادن یک پیام صورت می گیرد ، اگرمحتوای اطلاعاتی را با I نشان دهیم و احتمال وقوع پیام رابا P نشان دهیم،آنگاه خواهیم داشت:

(۳-۱)

$$I = -\log_2 P$$

فرض کنید که X یک متغیر تصادفی باشد که با احتمال P نمایش داده شود و همچنین فرض می کنیم که یکی از مقادیر $x_1, x_2, x_3,\ldots,x_i$ با احتمال $p_1, p_2, p_3, \ldots,p_i$ شامل شود، آنگاه آنتروپی شانون به صورت زیر تعریف می شود:

(۴-۱)

$$H(X)=\sum_i p_i \log_2 p_i$$

مثال: فرض کنید X خروجی انداختن تاس باشد $X=\{1,2,3,4,5,6\}$ و
$P=\{1/6,1/6,1/6,1/6,1/6,1/6\}$ درنتیجه: $H(X)=\log6=2058$

فرض کنیم که پیامی تنها شامل عدد ۲ باشد که به صورت رشته ای از عدد۲ به شکل ۲...۲۲۲۲۲ نمایش داده می شود. آنتروپی به صورت زیر است:

$$H = -\log_2^1 = 0 \qquad (۵-۱)$$

در رابطه (۱-۵) آنتروپی پیام صفر می شود، به دلیل این که احتمال وقوع پیام عدد ۲ یک است.درنتیجه هرچه عدم قطعیت در پیام بیشتر باشد محتوای اطلاعاتی بیشتر است و درنتیجه آنتروپی شانون بیشتر است.

H(X)می تواند به عنوان معیار اندازه گیری موارد زیردر مورد X باشد:

۱) مقدار اطلاعاتی که از اندازه گیری X بدست می آید.

۲) عدم قطعیت در مورد X.

۳) ماهیت تصادفیX.

۱-۵ اندازه گیری اطلاعات

آنتروپی شانون می تواند برای اندازه گیری های دیگر اطلاعات که ارتباط بین دو متغیر تصادفی X, Y است استفاده شود. این اندازه گیری ها به صورت زیر تعریف می شوند:

- آنتروپی نسبی، همسانی بین دو متغیر تصادفی را اندازه گیری می کند.
- آنتروپی مشترک، اطلاعات ترکیب شده را در دو متغیر تصادفی اندازه گیری می کند.
- آنتروپی شرطی ،اطلاعات بدست آمده در یک متغیر تصادفی را به شرط آنکه حاصل متغیر تصادفی دیگر معلوم باشد.
- اطلاعات متقابل، ارتباط بین دو متغیر تصادفی، برحسب اختلاف اندازه گیری اطلاعات بدست آمده از یک متغیر تصادفی و اطلاعات بدست آمده از متغیر تصادفی با داشتن متغیر تصادفی دیگر را اندازه گیری می کند. این اندازه گیری ها ابزارهای خیلی مفیدی برای طرز تفکر درمورد اطلاعات و دارای ارتباط مشترکی به وسیله بعضی تساوی ها هستند. حال باید به صورت فرمولی این روابط توصیف شوند.

۱-۵-۱ آنتروپی نسبی[1]

آنتروپی نسبی دو متغیر تصادفی X,Y به صورت زیر طبق فرمول (۱-۴)تعریف می شوند:

(۱-۶)

$$H(X||Y) = \sum_{\substack{x\in X\\ y\in Y}} P_x \log P_y - H(x) = \sum_{x,y} P(x) \log \frac{P_x}{P_y}$$

آنتروپی نسبی بین دومتغیر تصادفی X,Y اختلاف بین اطلاعات بدست آمده از متغیر Y با توجه به توزیع نسبت به متغیر X و محتوای اطلاعاتی متغیرXاست. اگر X,Y باهم برابر باشندآنتروپی نسبی صفرمی شود. یعنی:

$$H(X||X) = -\sum_{x} P_x \log \frac{P_x}{P_x} \qquad (۱-۷)$$

آنتروپی نسبی،معیار ناکارمدی این فرض است که توزیع q_x است در صورتی که توزیع درست p_x باشد.

اگر Y بتواند یک مقدار اختیار کند یعنی $P(Y)=1$ دراین حالت:

1 - Relative Entropy

$$H(X||Y) = \sum_{x} P_x \log P_y = -H(x) \qquad (۸-۱)$$

یعنی در رابطه(۱-۸) آنتروپی نسبی تبدیل به آنتروپی شانون می شود.

۱-۵-۲ آنتروپی مشترک[1]

آنتروپی مشترک بین دو متغیر تصادفی Y,X به صورت زیر تعریف می شود:

$$H(X,Y) = -\sum_{x,y} p(x,y)\log p(x,y) \qquad (۹-۱)$$

$p(x,y)$ احتمال توام رخدادهای x,y است.

اگر Y,X مستقل از هم باشند رابطه به صورت زیر در می آید:

$$H(X,Y) = H(X) + H(Y) \qquad (۱۰-۱)$$

$$-\sum P(x,y)\log P(x,y) = -\sum_{x,y} P_x P_y \log(P_x P_y)$$
$$= -\sum_{x,y} P_x P_y \log P_x - \sum_{x,y} P_x P_y \log P_y$$
$$= -\sum_{x} P_x \log P_x \left(\sum_{y} P_y\right) - \sum_{y} P_y \log P_y \left(\sum_{x} P_x\right) = H(X) + H(y)$$

که $P(x,y) = P_x P_y$

بنابراین اگر دو آزمایش داشته باشیم که خروجیهای آنها مستقل باشد،اطلاعات بدست آمده از دو آزمایش برابر با مجموع اطلاعات بدست آمده از هر آزمایش است.

۱-۵-۳ آنتروپی شرطی۲

آنتروپی شرطی،اطلاعاتی را که از اندازه گیری X با دانستن Y بدست می آید، اندازه گیری می کند.

$$H(X \mid Y) = -\sum_{x,y} P(x \mid y)\log P(x \mid y) \qquad (۱۱-۱)$$

2-Joint Entropy
2 - Conditional Entropy

بطوریکه $P(x \mid y)=\frac{P(x,y)}{P(y)}$ احتمال رخ دادن x بشرطی که yرخ داده باشد.اگر دو رویداد مستقل باشندآنگاه P(x|y)=P(x)

رابطه بین آنتروپی مشترک و نسبی به صورت زیر است:

$$H(X,Y)=H(X)+H(Y \mid X) \qquad (۱۲-۱)$$

$$\begin{aligned} H(Y \mid X) &= \sum_x P_x H(y \mid x) = -\sum_x P_x \sum_y P(y \mid x)\log P(y \mid x) \\ &= -\sum_{x,y} P(x,y)\log \frac{P(y \mid x)}{\frac{P(x,y)}{P_x}} = -\sum P(x,y)\log(P(x,y)) + \sum P(x,y)\log P(x) \\ &= H(x,y) - H(X) \end{aligned}$$

مثال: اگر دوتای جوراب داشته باشیم اگر یک تای آن رنگش آبی باشد می توان با ندیدن تای دیگر حدس زد که آبی است با دانستن رنگ یک تای جوراب می توان رنگ تای دیگر را تشخیص داد یعنی آنتروپی شرطی بین رنگ های یک جفت جوراب صفر است یعنی اگر Y,X به هم وابسته باشند، H(X,Y)=0 یعنی با دانستن Y اطلاعات جدید از اندازه گیری بدست نمی آید.

۱-۵-٤ اطلاعات متقابل[1]

اطلاعات متقابل بین دو متغیر تصادفی، اختلاف بین اطلاعات بدست آمده از اندازه X و اطلاعات بدست آمده از اندازه گیری X با دانستن Y است که به صورت زیر تعریف می شوند:

$$I(X:Y)=H(X)-H(X \mid Y) \qquad (۱۳-۱)$$

بدیهی است که اگر X,Y مستقل از هم باشند I(X:Y)=0 زیرا وقتی که Y,X از هم مستقل هستند H(X)=H(X|Y)

$$I(X:Y)=H(X)-H(Y)-H(X,Y) \qquad (۱۴-۱)$$

$$I(X:Y)=I(Y:X) \qquad (۱۵-۱)$$

رابطه بالا نشان می دهد که اطلاعات متقابل دو رویداد جا به جایی پذیر هستند.

1 - Mutual information

(۱۶-۱)

$$I(X:Y)=H(X)$$

رابطه بالا نشان می دهد که اگر اطلاعاتی از اندازه گیری X با دانستن Y بدست نیاید،آنگاه اطلاعات متقابل برابر با آنتروپی رویداد X است.

۱-۵-۵ ارتباط بین آنتروپی ها

برای اینکه ارتباط بین آنتروپی ها را شرح دهیم مثالی می زنیم.

مثال:p(x,y) را به صورت زیر درنظر بگیرید:

X \ Y	0	۱
0	$\frac{۱}{۳}$	$\frac{۱}{۳}$
۱	0	$\frac{۱}{۳}$

بدست آورید:

a. $H(X),H(Y)$

b. $H(X\mid Y),\ H(Y\mid X).$

c. $H(X,Y)$

d. $H(Y)-H(Y\mid X)$

e. $I(X;Y).$

حـــل:

$$a.\ H(X)=\frac{۲}{۳}\log\frac{۳}{۲}+\frac{۱}{۳}\log۳=۰.۹۱۸bits=H(Y)$$

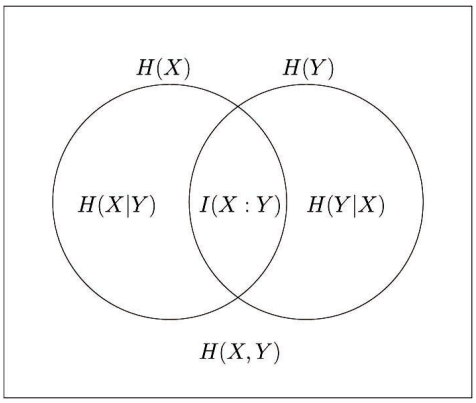
$$b.\ H(X\mid Y)=\frac{۱}{۳}H(Y\mid X=۰)+\frac{۲}{۳}H(X\mid Y=۱)=۰.۶۶۷bits=H(Y\mid X).$$

$$c.\ H(X,Y)=۳\times\frac{۱}{۳}\log۳=۱.۵۸۵bits$$

$$d.\ H(Y)-H(Y\mid X)=۰.۲۵۱bits$$

$$e.\ I(X;Y)=H(Y)=H(Y\mid X)=۰.۲۵۱bits.$$

ارتباط بین آنتروپی های شرح داده شده با توجه به شکل زیر معرفی می شود.



شکل(۱-۲)

از این شکل می توان دید که چگونه آنتروپی های متفاوت به وسیله جمع به هم مرتبط شده اند، برای مثال $H(X,Y)=H(X\mid Y)+I(X:Y)+H(Y\mid X)$

۱-٦ مکانیک کوانتومی

۱-٦-۱ مقدمه

بی شک بزرگ ترین دستاورد علمی قرن گذشته مکانیک کوانتومی است.مکانیک کوانتومی بزرگ ترین تغییرات را در شیوه تفکر کلاسیک و اصول فلسفی حاکم بر فیزیک نیوتنی بوجود آورد و گامی در جهت نیل به یک شیوه تفکر و زبان علمی جدید دربرداشت.مکانیک کوانتومی با کارپلانک(در ۱۹۰۰ میلادی)

روی توزیع انرژی جسم سیاه آغاز شد و با کار انیشتین درارتباط با مفهوم فوتون(۱۹۰۵) و بالاخره نظریه اتمی بور(۱۹۱۳) توسعه یافت. مکانیک کوانتومی نسبت به مکانیک کلاسیکی دقت بیشتری از جهان میکروسکوپ دارد.

۱-۶-۲ اپراتورهای یکانی[1]

یک اپراتور یکانی را به صورت زیر نمایش می دهند:

$$U = \sum_i |\psi_i >< \Phi_i| \qquad (۱-۱۷)$$

که $|\psi_i >, |\Phi_i >$هردوپایه های متعامد هستند یک نمونه ساده از یک اپراتور یکانی،اپراتور همانی[2] است که به صورت زیر است:

$$I = \sum_i |\psi_i >< \psi_i| \qquad (۱-۱۸)$$

که $|\psi_i >$یک پایه است. بنابراین بردار $|\psi >$ به صورت زیر است:

$$|\psi >= \sum_i \alpha_i |\psi_i > \qquad (۱-۱۹)$$

اثر اپراتور یکانی به صورت زیر بررسی می شود:

$$I|\psi >= I\sum_i \alpha_i |\psi_i > \qquad (۱-۲۰)$$

$$= \sum_i \alpha_i |\psi_i >< \psi_i|\psi_i\rangle = |\psi > \qquad (۱-۲۱)$$

اپراتور U یکانی است اگر دردو شرط زیر صدق کند:

$$U^+=U^{-1} \qquad (۱-۲۲)$$

$$UU^+=U^+U= \qquad (۱-۲۳)$$

می توان یکانی بودن این اپراتور را به صورت زیر نشان داد:

$$UU^+ = \sum_i |\psi_i >< \Phi_i| \sum_j |\Phi_j >< \psi_j| \qquad (۱-۲۴)$$

---

1 - Unitary operators
2 - Identity operator

$$= \sum_i |\langle \Phi_i || \Phi_j \rangle || \psi_i >< \psi_j | \qquad (۲۵-۱)$$

$$= \sum_i | \psi_i >< \psi_i | = ۱ \qquad (۲۶-۱)$$

۱-۶-۳ نماد گذاری دیراک

در مکانیک کوانتومی از نمادگذاری دیراک برای نمایش حالت های کوانتومی استفاده می شود. در این نماد گذاری یک بردار دوبعدی ستونی $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ توسط کت $< \psi |$ نمایش داده می شود که بردار سطری آن $(\alpha^* \ \beta^*)$ توسط برا $| \psi >$نمایش داده می شود. در این نوتاسیون ضرب داخلی دوبردار به صورت $\langle \phi | \psi >$نمایش داده می شوند.

هر کت $< \psi |$را می توان به فرم زیر نوشت:

$$| \psi >= \alpha \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} + \beta \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} = \alpha | x > + \beta | y > \qquad (۲۷-۱)$$

در رابطه بالا هر بردار دوبعدی را می توان برحسب این دوبردار پایه نوشت.ما می توانیم نماد گذاری برا و کت را با تعریف زیر انجام دهیم.

$$\begin{aligned} &< x | y >=< y | x >= 0 \\ &< x | x >=< y | y >= 1 \end{aligned} \qquad (۲۸-۱)$$

رابطه بالا بدین معنی است که حالت های y,x متعامد هستند. یعنی ضرب داخلی آنها صفر می شود و بهنجار شده هستند اگر ضرب داخلی آنها با خودشان یک باشد.

برای مثال اگر $| \psi >= \alpha | x > + \beta | y >$ پس ضرب داخلی آن در خودش به صورت زیر انجام می شود:

(۲۹-۱)

$$\begin{aligned} < \psi | \psi > &= \left(\alpha^* < x | + \beta^* \langle y | \right)\left(\alpha | x > + \beta | y >\right) \\ &= \alpha^* \alpha < x | x > + \alpha^* \beta < x | y > + \beta^* \alpha < y | x > + \beta^* \beta < y | y > \\ &= \alpha^* \alpha .1 + \alpha^* \beta .0 + \beta^* \alpha .0 + \beta^* \beta .1 \\ &= |\alpha|^2 + |\beta|^2 \end{aligned}$$

دررابطه بالا $|\alpha|^۲ , |\beta|^۲$ متناظر با احتمالاتی برای اندازه گیری $| \psi >$ می باشند همچنین برا و کت می تواند برای ماتریس زیر تعریف شود.

$$A=\begin{pmatrix} a_{xx} & a_{xy} \\ a_{yx} & a_{yy} \end{pmatrix} \qquad (۳۰-۱)$$

این ماتریس را می توان در نمادگذاری دیراک با کمک ضرب خارجی برا و کت $|o><o|$ انشان داد به صورت زیر:

$$A = a_{xx}|x><x|+a_{xy}|x><y|+a_{yx}|y><x|+a_{yy}|y><y| \qquad (۳۱-۱)$$

ضرب تانسوی دو کت به صورت $|\psi>\otimes|\phi>$ انمایش داده می شود.

این بردارها در مکانیک کوانتومی در فضایی به نام فضای هیلبرت معرفی میشوند. فضای هیلبرت یک فضای برداری مختلط است که تمام کت ها مانند $|\psi>$ متعلق به این فضا می باشند.

چهاراصل در مکانیک کوانتومی وجود دارد که درمورد سیستم کوانتومی لازم است که بدانیم.

۱- بردارهای حالت: حالت های یک سیستم فیزیکی توسط برداری در فضای هیلبرت توصیف می شود.

۲- مشاهده پذیرهای فیزیکی مانند مکان، اندازه حرکت، انرژی، توسط عملگرهای هرمیتی نمایش داده می شوند چون ویژه مقادیرشان حقیقی است.

۳- اندازه گیری: هرکمیتی که قابل اندازه گیری است عملگر[1] هرمیتی بدان وابسته است که ویژه بردارهای عملگرهای هرمیتی کامل اند. بدین ترتیب حالت سیستم را که توسط بردار $|\psi>$ در فضای هیلبرت توصیف می شود می توان برحسب ویژه کت های $\{|\Phi_i>\}$ نمایش داد.

$$|\psi>=\sum_i |\Phi_i><\Phi_i|\psi> \qquad (۳۲-۱)$$

از طرفی $|<\Phi_i|\psi>|^2$ احتمال آن است که سیستم پس از اندازه گیری در حالت $|\Phi_i>$ یافت شود.

۴- تحول سیستم: تحول[2] سیستم فیزیکی توسط یک عملگر یکانی[3] بیان می شود یعنی اگر حالت سیستم $|\psi(o)>$ انمایش داده شود در زمان t داریم:

$$|\psi(t)>=U(t)|\psi(0)>, \quad UU^+=1 \qquad (۳۳-۱)$$

1 - Operator
2 - Evolution
3 - unitary

۱-٦-٤ اندازه گیری تصویری و عملیات

به طور کلی یک اپراتور اندازه گیری یک حالت M است که به وسیله یک ضرب خارجی به صورت $|x><x|$ نشان داده می شود. این اپراتور هرمیتی است یعنی $M=M^{+}$.همچنین این اپراتور تصویرگر گفته می شود یعنی مربع خودش مساوی با خودش است. $|x><x||x\rangle<x|=|x><x|$ ،$M^2=M$ ،دو اپراتور تصویرگر M_1, M_2 متعامد هستند اگر ضرب داخلی آنها صفر باشد. برای هر حالت $|\psi>, M_1, M_2$ متعامد هستند اگر:

$$M_1 M_2 |\psi>=0 \qquad (۳۴-۱)$$

یک مجموعه کامل از اپراتورهای تصویرگر متعامد برابر با یک است.

$$\sum_i M_i = I \qquad (۳۵-۱)$$

برای حالت کوانتومی $|\psi>=\alpha|0>+\beta|1>$ ابعد فضایی ۲ است و اپراتورهای تصویری متناظر با $|0>, |1>$ به صورت زیراند:

$$M_o = |0><0| \quad , \quad M_1 = |1><1| \qquad (۳۶-۱)$$

اگر ما اپراتورهای تصویری $\{M_1, M_2, M_3, ...\}$ را داشته باشیم، ما می توانیم نشان دهیم که آنها دو بدو متعامد هستند.

$$M_i M_j = \delta_{ij} M_i \qquad (۳۷-۱)$$

فرض کنید بعد یک سیستم n است و یک مجموعه از اپراتورهای تصویری متعامد $\{M_1, M_2, M_3, ...\}$ را درنظر بگیرید. اگر سیستم در حالت $|\psi>$ قرار بگیرید، احتمال یافتن خروجی iام هنگامی که یک اندازه گیری انجام شود به صورت زیر است:

(۳۸-۱)

$$pr(i) = |M_i|\psi>|^2 = (M_i|\psi>)^{+}(M_i|\psi>) = <\psi|M_i^2|\psi> = <\psi|M_i|\psi>$$

یک مجموعه مشاهده پذیر از اپراتورهای تصویرگردرنظر بگیرید که با A مشخص می شوند و ویژه بردارهای A با $|u_i>$ با ویژه مقدار a_i مشخص می شوند.

$$A = \sum_{i=1}^{n} a_i |u_i><u_i| = \sum_{i=1}^{n} a_i M_i \qquad (۳۹-۱)$$

ما می توانیم حالت سیستم $|\psi>$ را برحسب ویژه بردارهای A بسط دهیم به صورت زیر:

$$|\psi>=\sum_{i=1}^{n}(<u_i|\psi\rangle)|u_i>=\sum_{i=1}^{n}c_i|u_i> \qquad (۴۰-۱)$$

که $c_i=\langle u_i|\psi>$ دامنه احتمال است (برای بدست آوردن نتیجه اندازه گیری a_i) که احتمال بدست آمده برای این سیستم برابر است با:

$$pr(i)=|<u_i|\psi>|^2 \qquad (۴۱-۱)$$

ما می توانیم حالت سیستم را بعد از اندازه گیری به صورت زیر شرح دهیم:

$$\text{که}|\psi'>=\frac{M_i|\psi>}{\sqrt{<\psi|M_i|\psi>}} \qquad (۴۲-۱)$$

حضور $<\psi|M_i|\psi>$ در مخرج نشان می دهد که $|\psi'>$ نرمالیزه است. مقدار چشم داشتی A نسبت به حالت $|\psi>$ به صورت زیر تعریف می شود:

$$<A>=\sum_i a_i<\psi|M_i|\psi> \qquad (۴۳-۱)$$

۱-۶-۵ پایه اصلی محاسبه کوانتومی

۱-۶-۵-۱ کیوبیت[1]

اطلاعات کلاسیکی دربیت ذخیره می شوند. هربیت می تواند با دو مقدار صفر و یک بیان شود. کیوبیت معادل کوانتومی بیت است[۱].کیوبیت یک بردار حالت کوانتومی درفضای هیلبرت H^2 می باشد. اگر بردارهای $|۰>,|۱>$ پایه های H^2 باشند آنگاه یک کیوبیت را می توان به صورت زیر نوشت:

$$|\psi>=C_o|0\rangle+C_1|1> \qquad (۴۴-۱)$$

که C_o , $C_۱$ اعداد مختلط هستند که شرط نرمالیزه را برآورد می کنند.

$$|C_o|^2+|C_۱|^2=۱ \qquad (۴۵-۱)$$

احتمال این که کیوبیت درحالت $|0>$ و حالت $|۱>$ باشد به ترتیب با $|C_o|^2$ و $|C_۱|^2$ نمایش داده می شود.

یک تفاوت اصلی بین بیت و کیوبیت وجود دارد. یک بیت می تواند درحالت صفر یا درحالت یک باشد در صورتی که یک کیوبیت می تواند ترکیب خطی از $|0>$ و $|۱>$ باشد یعنی در هرزمان می تواند بیانگر بیش از یک حالت باشد. کیوبیتی که در رابطه(۱-۴۴) اشاره شد به تک کیوبیت معروف است اما دو کیوبیت به

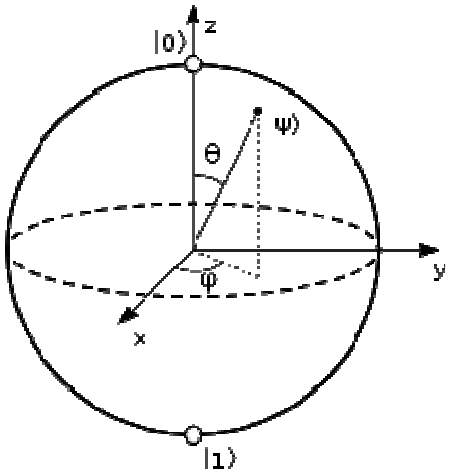
[1] Qubit

صورت ضرب تانسوری پایه های <۰| و <۱| بدست می آید. به وسیله این پایه ها، دو کیوبیت را می توان به صورت زیر نمایش داد:

$$|\psi>=C_o\,|۰۰>+C_۱\,|۰۱>+C_۲\,|۱۰>+C_۳\,|۱۱> \qquad (۴۶-۱)$$

که $|C_o|^۲+|C_۱|^۲+|C_۲|^۲+|C_۳|^۲=۱$، کامپیوترهای کوانتومی می توانند ازکیوبیت برای پردازش داده ها استفاده کنند. کارشناسان کامپیوتر چندین سال پیش دریافتند که نشان دادن همزمان چند مقدار عددی می تواند زمان لازم را برای حل مسائل عددی را از چندسال به چند دقیقه کاهش دهدکه کیوبیت برخلاف بیت این کار را انجام می دهد.

حالتهای ممکن برای یک تک کیوبیت می تواند با استفاده از کره Bloch تجسم شود در نمایش یک چنین کره ای،یک بیت کلاسیکی می تواند در قطب شمال و جنوب در محل $|0\rangle$، $|1>$ به ترتیب قرار بگیرد.سطح کره، خارج از دسترس برای بیت کلاسیکی است ولی یک حالت کیوبیت خالص می تواند در هر نقطه روی سطح نمایش داده شود برای مثال حالت کیوبیت خالص $|0\rangle + i\,|1>$ می تواند روی خط استوای کره در قسمت مثبت محور y قرار بگیرد.



شکل (۱-۳)

۱-۶-۵-۲ انواع کیوبیت ها

دانشمندان ایده های زیادی برای ساخت کامپیوترهای کوانتومی دارند. برخی، ازسطوح انرژی یون های به دام افتاده در میدان های الکتریکی به عنوان صفر و یک های کوانتومی استفاده کردند. برخی هم در قطبش فوتون به دنبال کیوبیت هاگشتند وبرخی هم اسپین های الکترونی محدودشده در یک نقطه کوانتومی راکیوبیت دانسته اند.