
بسم الله الرحمن الرحيم

دانشکده فیزیک

پایان‌نامه کارشناسی ارشد

فیزیک ذرات بنیادی

عنوان:

ارتباط میان کاتوره و ناموضعیت

دانشجو:

فاطمه عدالتخواه

استاد راهنما:

دکتر حسین موحدیان

پایان‌نامه ارشد جهت اخذ درجه کارشناسی ارشد

زمستان۹۲

تقدیم به وجود نازنین پدر و مادرم

همه ی آموخته هایم را تقدیم می کنم به آنان که مهر آسمانی شان آرام بخش آلام زمینی ام است، به استوارترین تکیه گاهم، دستان پرمهر پدرم به سبزترین نگاه زندگیم، چشمان پرمهر مادرم که هرچه آموختم در مکتب عشق شما آموختم و هرچه بکوشم قطره ای از دریای بی کران مهربانیتان را سپاس نتوانم بگویم. امروز هستی ام به امید شماست و فردا کلید باغ بهشتم رضای شما. ماحصلی گران سنگ تر از این نداشتم تا به خاک پایتان نثار کنم، باشد که حاصل تلاشم غبار از خستگیتان بزداید.

بوسه بر دستان پرمهرتان

سپاسگذاری:

سپاس بی کران پروردگاریکتارا که هستی مان بخشید و به طریق علم و دانش رهنمونمان شد. پروردگار بی همتایی که کسب علم و معرفت را روزیمان ساخت و درهای علم را برما گشود. سپاس آن خالق بینایی که فرصتی عطا فرمود تا بدان، بنده ضعیف خویش را در طریق علم و معرفت بیازماید.

از آنجایی که تجلیل از معلم، سپاس از انسانی است که هدف و غایت آفرینش را تامین می کند و سلامت امانت هایی را که به دستش سپرده اند، تضمین، بر حسب وظیفه و از باب "من لم یشکر المنعم من المخلوقین لم یشکر اللهَ عزّ و جلّ" :

از استاد فرزانه و دلسوز، جناب آقای دکتر حسین موحدیان که در کمال سعه صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه بر من دریغ ننمودند و زحمت راهنمایی این رساله را بر عهده گرفتند؛

و از اساتید با کمالات و شایسته، جناب آقای پروفسور علی اکبر رجبی و جناب آقای دکتر. مصطفی عنابستانی که زحمت داوری این رساله را متقبل شدند، کمال تشکر و قدردانی را دارم.

تعهد نامه

اینجانب فاطمه عدالتخواه دانشجوی دوره کارشناسی ارشد، رشته فیزیک ذرات بنیادی دانشکده فیزیک دانشگاه صنعتی شاهرود، نویسنده‌ی پایان نامهٔ **ارتباط میان کاتوره و ناموضعیت** تحت راهنمائی دکتر حسین موحدیان متعهد می‌شوم:

- تحقیقات در این پایان نامه 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 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 می‌باشد و مقالات مستخرج با نام « دانشگاه صنعتی شاهرود» و یا «Shahrood University of Technology» به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به‌دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده‌اند در مقالات مستخرج از پایان نامه رعایت می‌گردد.
- در کلیه مراحل انجام این پایان‌نامه، 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، 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**

چکیده

امروزه تولید اعداد تصادفی به‌خصوص در رمزنگاری از اهمیت فوق‌العاده‌ای برخوردار است. برای تولید اعداد تصادفی بسته به کاربرد آنها از روشهای تولید متفاوتی بهره می‌جوییم. امنیت پارامتر مهمی در رمز نگاری است. در این تحقیق علمی به‌دنبال تولید اعداد تصادفی هستیم که توسط جاسوس شناسایی نمی‌شود و از امنیت بالایی برخوردار است. در فیزیک نیوتنی، با داشتن آگاهی کاملی از شرایط اولیه و برهم‌کنشهای سیستم می‌توانیم آینده سیستم را به صورت قطعی پیش‌بینی کنیم. تولید اعداد تصادفی به روش کلاسیک، با توجه به قطعیتی که در سیستم وجود دارد امنیت لازمه را ندارد. چارچوب نظریه کوانتمی شامل یک نوعی از کاتورگی می‌باشد که همتای کلاسیکی ندارد. فیزیک کوانتمی ذاتا تصادفی است، لذا برای تولید اعداد تصادفی مناسب می‌باشد. در این تحقیق علمی میزان کاتورگی خروجی‌های یک آزمایش بل را تعیین می‌کنیم و بهترین سیستم را برای تولید اعداد کاملا تصادفی برمی‌گزینیم.

خروجی‌های یک حالت در هم‌تنیده که آزمایش بل را نقض می‌کنند، الزاما مقداری کاتورگی را نشان می‌دهند. در اینجا قصد داریم تا ارتباط میان ناموضعیت و کاتورگی را که در یک آزمایش بل وجود دارد بررسی کنیم. انتظار داریم ارتباط مستقیمی میان میزان ناموضعیت و کاتورگی تولید شده در یک آزمایش بل برقرار باشد یعنی برای مثال هرچه میزان ناموضعیت کمتر باشد میزان کاتورگی نیز کمتر است. نتایج نشان می‌دهد که این ارتباط مستقیم درست نمی‌باشد و ارتباط میان این دو مفهوم دقیقتر از آن است که انتظار داریم. میزان طبیعی ناموضعیت سیستم را، میزان کمّی نقص نامساوی بل در نظر می‌گیریم سپس میزان کمّی کاتورگی سیستم را بدست می‌آوریم. در این تحقیق علمی نشان می‌دهیم همبستگی‌های ناموضعی کم، که نامساوی CHSH را کم نقض می‌کنند، با این‌حال حداکثر کاتورگی را دارند. می‌دانیم که با انجام آزمایشهایی با خروجی‌های دوتایی بر روی دو زیر سیستم حداکثر دو بیت کاتورگی تولید می‌شود. ما نشان می‌دهیم که به ازای حالاتی که دارای درهم‌تنیدگی کمی هستند دارای دو بیت کاتورگی حداکثری هستیم.

واژگان کلیدی: ناموضعیت، کاتورگی، نامساوی CHSH، درهم‌تنیدگی، احتمال حدسی.

لیست مقالات مستخرج از پایان‌نامه

۱- عدالتخواه، فاطمه؛ موحدیان، حسین، (۱۳۹۲) "ارتباط میان ناموضعیت وکاتورگی"، کنفرانس فیزیک محاسباتی- دانشگاه تربیت دبیر شهید رجایی.

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها صفحه

فصل اول

مروری بر نظریه اطلاعات و مفاهیم مقدماتی

مقدمه

فرآیند پردازش اطلاعات در حوزه‌ی فیزیک کلاسیک و فیزیک کوانتمی علی‌رغم شباهت‌های فراوان دارای تفاوت‌هایی نیز می‌باشد. همانطور که حالت کلاسیک حاوی اطلاعات، تحت پردازش و انتقال قرار می‌گیرد در پروتکل‌های اطلاعات و محاسبات کوانتمی[1] حالت کوانتمی تحت نگاشت‌های کوانتمی مناسب قرار می‌گیرد. واحد اطلاعات در هر دوی این حوزه‌ها از یکدیگر متفاوت می‌باشند. با ورود به حوزه‌ی کوانتمی خیلی از مفاهیمی که در کلاسیک در نظر می‌گیریم نقض می‌شوند. و این یکی از دلایل مشکل بودن مکانیک کوانتمی می‌باشد.

استفاده از پردازنده‌های موازی، عدم امکان نسخه‌برداری[2]، و یا کاتوره‌ای بودن این سیستم‌ها سبب گرایش به سمت محاسبات کوانتمی و برتری محاسبات کوانتمی می‌شود. استفاده از ویژگی کاتورگی ذاتی این سیستم‌ها سبب تولید اعدادی با کیفیت بالا از لحاظ امنیتی می‌شود لذا برای تولید اعداد کاملا کاتوره‌ای بسیار مناسب می‌باشند. هدف این است که با استفاده از نقض نامساوی بل به میزان کمّی کاتورگی پی‌ببریم. و رابطه‌ی میان کاتورگی ذاتی و میزان نقض نامساوی بل را محاسبه کنیم.

[1] Quantum computing and information
[2] No cloning

۱-۱ نظریه پردازش کوانتمی اطلاعات

علوم اطلاعات و محاسبات کوانتمی عبارت است از فرآیندهای پردازش اطلاعاتی که در آنها از خاصیت کوانتمی مواد استفاده می‌شود. پردازش اطلاعات نیز شامل ذخیره‌سازی، فراخوانی، انتقال و تغییرات حساب شده در اطلاعات (از قبیل فشرده سازی، تصحیح خطا، محاسبه و رمز کردن) می‌باشد.

در علوم اطلاعات و محاسبات کوانتمی در مقایسه با پردازش اطلاعات کلاسیک، علاوه بر حالات کلاسیک (حالات همواره متمایز مانند بیت‌ها) از حالات کوانتمی نیز استفاده می‌شود، که در نهایت با انجام اندازه‌گیری بر روی آن حالت کوانتمی نتیجه‌ی پردازش بدست می‌آید. در واقع همانطور که درعلوم اطلاعات و محاسبات کلاسیک حالت کلاسیک حاوی اطلاعات، تحت پردازش و انتقال قرار می‌گیرد، در پروتکل‌های اطلاعات و محاسبات کوانتمی حالت کوانتمی تحت نگاشت‌های کوانتمی مناسب قرار می‌گیرد و یا می‌توان حالت کوانتمی را از نقطه‌ای از فضا به نقطه‌ای دیگر منتقل کرد. این کار را می‌توان با انتقال مستقیم سیستم کوانتمی و یا بدون انتقال سیستم و با فرآیندهایی نظیر دورنگاری[۳] یا معاوضه[۴] درهم‌تنیدگی حالت کوانتمی ورودی انجام داد.

همانطور که واحد اطلاعات در فیزیک کلاسیک بیت[۵] می‌باشد که یک واحد گسسته می‌باشد، در مکانیک کوانتمی واحد اطلاعات کیوبیت است که به‌صورت پیوسته می‌باشد.

برای اعمال یک نگاشت کوانتمی دلخواه از گیت‌های تک‌کیوبیتی (مانند σ_x و σ_y) و دو کیوبیتی (مانند C-Not) استفاده می‌شود. مشابه با بیت‌ها در فرآیند اطلاعات کلاسیکی ما کیوبیت‌ها را در فرآیند اطلاعات کوانتمی داریم، علاوه بر آن نیز تمامی مفاهیم مبنایی که در شاخه‌های اصلی

[3] Teleportation
[4] Entanglement swapping
[5] Bit

علوم و اطلاعات کلاسیک توسعه یافته‌اند، در علوم اطلاعات و محاسبات کوانتمی معادل‌سازی شده‌اند. با ورود به حوزه‌ی فیزیک کوانتمی از مفاهیمی استفاده می‌شود که معادل آن را در کلاسیک نداریم، و این یکی از دلایل مشکل بودن مفاهیم مکانیک کوانتمی می‌باشد.

۱-۲ استفاده از ویژگی‌های سیستم‌های کوانتمی در پردازش اطلاعات

با گذشت زمان و کوچکتر شدن ابعاد ترانزیستورها به جایی می‌رسیم که عناصر، از یک اتم بزرگتر نخواهند بود. در این ابعاد اتمی مشکل این است که نمی‌توان سیستم را با قوانین فیزیک کلاسیک توجیه کرد، بلکه باید از اصول مکانیک کوانتمی برای فهم چنین سیستم‌های میکروسکوپیکی استفاده کرد. لذا لزوم ساخت کامپیوترهای کوانتمی که اساس کارشان مکانیک کوانتمی است، توسط ریچارد فاینمن در اوایل دهه ۱۹۸۰ مطرح شد. در این کامپیوترها زمان لازم برای انجام یک محاسبه با افزایش پردازنده‌های موازی کاهش می‌یابد.

در طرف مقابل پردازنده‌های کلاسیک اطلاعات، پردازنده‌های کوانتمی قرار دارند. یک حالت کوانتمی از مجموعه‌ای از حالات متمایز تشکیل شده است. اطلاعات نهایی کسب شده از سیستم کوانتمی به‌وسیله‌ی اندازه‌گیری کلاسیک صورت می‌پذیرد. ارتباط ما با دنیای کوانتمی توسط اندازه‌گیری بوده، یعنی در اصل اطلاعات بدست آمده توسط ما کلاسیکی است.

در اینجا مثال ساده‌ای از حالت چند کیوبیتی را بررسی می‌کنیم. با در نظر گرفتن یک سیستم کوانتمی n کیوبیتی حداکثر تعداد حالات متمایز از یکدیگر 2^n خواهد بود. اگر حالت اولیه‌ی سیستم بدین صورت باشد:

$$|0\rangle_1 \otimes |0\rangle_2 \otimes ... \otimes |0\rangle_n \qquad (۱-۱)$$

آنگاه با اعمال n عمل یکانی موضعی به‌صورت زیر:

$$U^{(i)} = I^{(1)} \otimes I^{(2)} \otimes ... \otimes H^{(i)} ... \otimes I^{n} \qquad : \quad 1 \le i \le n \qquad (۲-۱)$$

بر روی n کیوبیت، که H به صورت زیر تعریف می‌شود:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \qquad (۳-۱)$$

خواهیم داشت:

(۴-۱)

$$|\psi\rangle = U^{(1)}U^{(2)}..U^{(j)}..U^{(n)} = (H^{(1)} \otimes H^{(2)} \otimes ... \otimes H^{(j)} ... \otimes H^{(n)})(|0\rangle_1 \otimes |0\rangle_2 \otimes ... \otimes |0\rangle_n)$$
$$= (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes ... \otimes (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) H = \frac{1}{2^{\frac{n}{2}}}(|000...0\rangle + |000...1\rangle + ... + |111...1\rangle)$$

در نتیجه تنها با n عمل موضعی، برهم‌نهی از 2^n حالت متمایز، و با احتمال یکسان تولید شد. که در یک بار پردازش چنین خروجی خواهد داشت [۱].

ویژگی دیگری که یک حالت کوانتمی دارد این است که در حالت کلی امکان تشخیص یک حالت مجهول وجود ندارد، و در صورت اندازه‌گیری در روی یک حالت کوانتمی مجهول آن حالت به اصطلاح ریزش[۶] می‌کند. علاوه بر این امکان نسخه‌برداری از یک حالت کوانتمی وجود ندارد. از یک نظر این نتیجه محدودیت ایجاد می‌کند زیرا که موجب می‌شود تا امکان معادل‌سازی آن‌دسته از پروتکل‌های اطلاعات کلاسیک، که مبتنی بر نسخه‌برداری از اطلاعات است، در پردازش اطلاعات کوانتمی از بین برود.

[6] Colaps

سیستم‌های کوانتمی به صورت ذاتی کاتوره‌ای هستند، بنابراین برای استفاده در الگوریتم‌های تصادفی بسیار مناسب می‌باشند. در سیستم‌های کلاسیک برای پیاده‌سازی الگوریتم‌های تصادفی باید بخش مستقلی را به روند کاتوره‌ای اختصاص دهند بنابراین عملا تولید اعداد تصادفی یکی از چالش‌های پروتکل‌های تصادفی محسوب می‌شود.

بی‌شک بزرگترین دستاورد علمی قرن گذشته مکانیک کوانتمی است. فرمولبندی نهایی مکانیک کوانتمی به شکل ماتریسی آن توسط هایزنبرگ و به‌صورت مکانیک موجی توسط شرودینگر به‌ترتیب در سال‌های (۱۹۲۵) و (۱۹۲۶) ارائه گردید. البته دو شکل موجی و ماتریسی ارائه شده برای مکانیک کوانتمی دو فرمولبندی متفاوت ریاضی برای نمایش یک دینامیک واحد بودند که در سال ۱۹۲۶ هم‌ارزی این دو تئوری توسط شرودینگر و دیراک نشان داده شد [۱].

۱-۳ کاتورگی ذاتی[۷]

همانطور که بیان شد یکی از ویژگی‌های مهم سیستم‌های کوانتمی کاتوره‌ای بودن این سیستم‌هاست. البته این کاتورگی که در مکانیک کوانتمی مطرح می‌شود متفاوت از کاتورگی مطرح شده در فیزیک کلاسیک است. در دنیای کلاسیک کاتورگی خالص وجود ندارد. در واقع می‌توان گفت در دنیای کلاسیک کاتورگی نتیجه‌ای از نقص موجود در آماده‌سازی دستگاه یا سیستم است، و یا از کمبود اطلاعات ما ناشی می‌شود. بنابراین این ویژگی ذاتی تصادفی سیستم‌های کوانتمی سبب می‌شود تا در تولید اعداد کاملا تصادفی از این سیستم‌ها استفاده کنیم. چرا که این سیستم‌ها می‌توانند غیر قابل پیش‌بینی‌ترین اعداد را برای ما تولید کنند. عبارات بل دسته عبارتهایی هستند که

[7] Intrinsic randomness

با تکیه بر مکانیک کلاسیک بوجود آمده‌اند. در واقع یک عبارت بل بر اساس نظریه متغیرهای پنهان[۸] تشکیل شده است. هر گاه یک نامساوی بل نقض شود آنگاه الزاما دارای کاتورگی هستیم. در ابتدای امر فکر می‌کنیم که رابطه‌ی مستقیمی میان ناموضعیت و کاتورگی برقرار است یعنی هر چه میزان نقض نامساوی بل بیشتر باشد آن‌گاه کاتورگی سیستم نیز بیشتر خواهد بود. با بررسی بیشتر به این نکته پی می‌بریم که رابطه‌ی میان نقض نامساوی بل و میزان کاتورگی به همین سادگی که اشاره شد نمی‌باشد و همواره رابطه‌ی مستقیمی میان اینها برقرار نیست. یعنی گاه پیش می‌آید که به ازای نقض ناچیزی از نامساوی بل میزان حداکثری کاتورگی داریم، و یا به ازای یک سیستم با درهم‌تنیدگی کم دارای حداکثر کاتورگی هستیم. البته میزان این حداکثر کاتورگی بستگی به تعداد طرفین سیستم و تعداد کیوبیت‌ها دارد.

[8] Hidden variable

فصل دوم

مروری بر مفاهیم ناموضعیت، درهم‌تنیدگی و آنتروپی

مقدمه

همبستگی‌ها[9] شامل سه دسته همبستگی‌های کوانتمی، همبستگی‌های کلاسیک، و همبستگی‌های عدم علامت‌دهی[10] تقسیم می‌شوند [۲]. در اینجا همبستگی‌های مد نظر ما، همبستگی‌های کوانتمی هستند. این دسته همبستگی‌ها ناموضع‌اند. یکی از عجیب‌ترین و کلیدی‌ترین ویژگی‌های همبستگی‌های کوانتمی، درهم‌تنیدگی است، که علی‌رغم تمرکز بسیار زیاد دانشمندان بر روی این ویژگی اسرارآمیز، شناخت کافی از آن حاصل نشده است. این ویژگی وسوسه‌های زیادی را برای ارسال آنی اطلاعات برانگیخت. تنها در صورت استفاده از حالت‌های درهم‌تنیده امکان برخی از مسائل که توسط محاسبه‌گر کلاسیک انجام پذیر نمی‌باشد وجود دارد.

پدیده شگفت‌انگیز درهم‌تنیدگی نتایجی را در رایانه‌های کوانتمی به دنبال داشته است. با استفاده از موادی که می‌توانند این خاصیت را در مقیاس‌های میکروسکوپی از خود نشان دهند می‌توان برای کار در فرآیند اطلاعات و پردازش کوانتمی استفاده کرد.

[9] Correlations
[10] No-signalling correlations

۲-۱ کیوبیت

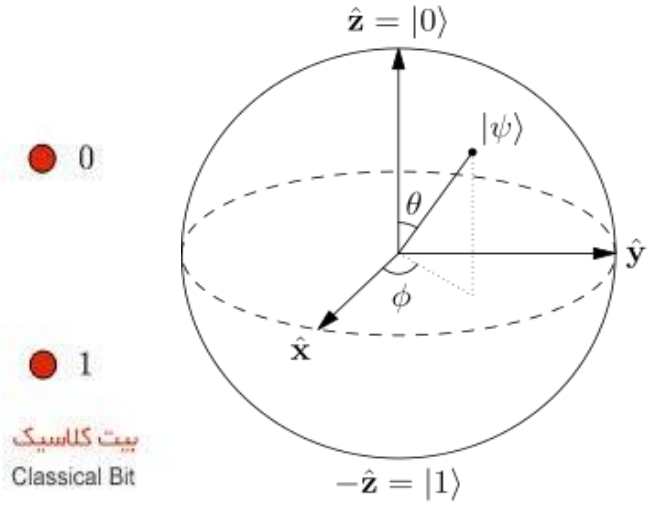
بیت یک مفهوم علمی در محاسبات و اطلاعات کلاسیکی است. همتای بیت کلاسیک در محاسبات کوانتمی، کیوبیت را داریم. کیوبیت‌ها اجسام ریاضی انتزاعی هستند، که دارای ویژگی‌های خاصی می‌باشند،که این ویژگی‌ها باعث می‌شوند تا یک نظریه کلی از محاسبات کوانتمی و اطلاعات کوانتمی را بر اساس آنها بسازیم. یک کیوبیت حالت برهم‌نهی است از 0 و 1 که در اینجا از نمادگذاری استاندارد دیراک (|⟩) برای نشان دادن این 0 و 1ها استفاده می‌شود. تفاوت میان بیت و کیوبیت این است که یک کیوبیت می‌تواند همزمان در حالت 0 و 1 باشد که اغلب به آن برهم‌نهی[11] می‌گوییم و به فرم کلی زیر آن را نشان می‌دهیم:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (۱-۲)$$

α و β اعداد مختلط می‌باشند. حالت یک کیوبیت یک بردار در یک فضای برداری مختلط دو بعدی است. حالت‌های مخصوص $|0\rangle$ و $|1\rangle$ حالت‌های پایه و عمود بر هم هستند.

زمانی که ما یک حالت را اندازه می‌گیریم با احتمال $|\alpha|^2$ آن را در $|0\rangle$ پیدا می‌کنیم و با احتمال $|\beta|^2$ آن را در $|1\rangle$ می‌یابیم. به‌صورت طبیعی $|\alpha|^2+|\beta|^2=1$ زیرا مجموع احتمالات باید 1 شود. در واقع می‌توان گفت کیوبیت به 1 بهنجار می‌باشد. برای مثال فرض کنید حالت سیستم را به صورت $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ داشته باشیم. بنابراین سیستم با احتمال $(\frac{1}{\sqrt{2}})^2$ در حالت $|1\rangle$ یافت می‌شود و با احتمال $(\frac{1}{\sqrt{2}})^2$ نیز در حالت $|0\rangle$ یافت می‌شود.

[11] Super position



شکل(۲-۱): تمایز میان بیت کلاسیک و بیت کوانتمی

عدم تطابق میان واقعیت با سیستم‌های کوانتمی بررسی سیستم‌های کوانتمی را دشوار نموده است. نتایج حاصله ازیک حالت کوانتمی به صورت آزمایشگاهی قابل بررسی است. یک بیت کلاسیک همانند یک سکه‌ی ایده‌آل است، که در پرتاب آن نتیجه یا شیر می‌آید یا خط. در حالی که یک کیوبیت می‌تواند در حالت پیوسته‌ای از $|0\rangle$ و $|1\rangle$ قرار بگیرد و بعد از اندازه‌گیری حالت کلی سیستم در یکی از دو حالت $|0\rangle$ یا $|1\rangle$ قرار خواهد گرفت. یک کیوبیت می‌تواند از راههای مختلفی ساخته شود، ممکن است جهت‌های مختلف قطبش یک فوتون باشد و یا حالات مختلف چرخش یک الکترون، و یا ممکن است حالت پایه و برانگیخته یک اتم باشد، که به‌ترتیب با $|0\rangle$ و $|1\rangle$ نشان داده می‌شود که در مورد اخیر اتم با ساطع کردن نور و یا دریافت انرژی در هر یک از حالات قرار می‌گیرد. ما می‌توانیم رابطه (۲-۱) را به صورت زیر نیز نمایش دهیم:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \qquad (۲-۲)$$

که این رابطه به نوعی نمایش هندسی حالتمان را نشان می‌دهد که رابطه‌ی بهنجارش را نیز رعایت می‌کند. اعداد θ و φ نیز به‌ترتیب زاویه قطبی و سمتی می‌باشند. این حالت یک نقطه را بر روی کره

سه بعدی واحد (که به آن کره بلاخ می‌گوییم) تعریف می‌کند. این شکل یک تصویر ریاضی دقیق از حالت یک کیوبیت تنهاست.

با توجه به رابطه(۲-۱) چون مقدار α و β می‌تواند هر مقدار پیوسته‌ای باشد بنابراین یک کیوبیت می‌تواند هر نقطه‌ای روی کره بلاخ باشد از این رو یک کیوبیت حاوی اطلاعات بسیار زیادی خواهد بود. لذا کاربرد کیوبیت‌ها در علم اطلاعات می‌تواند بسیار با اهمیت باشد [۳].

۲-۲ تعبیری از حالت سیستم

یک سیستم کوانتمی را تنها می‌توان بر اساس احتمال حضور در حالات متمایز نشان داد. و این حالات متمایز قبل از اندازه‌گیری واقعیت خارجی ندارند، بلکه همه‌ی آنها حالات متمایزی هستند که ممکن است نتیجه‌ی اندازه‌گیری بر روی سیستم باشند، که با احتمال متفاوت ممکن است اتفاق بیافتند. بنابراین متغیرهای کوانتمی وابسته به مشاهده هستند. و به این دلیل است که آنها را اغلب اوقات مشاهده پذیر[۱۲] می‌نامیم.

یک حالت کوانتمی یک مفهوم انتزاعی است که حقیقت فیزیکی ندارد. مگر آنکه بتوانیم نوعی شی فیزیکی را تصور کنیم که متفاوت از اشیا کلاسیک موج یا ذره باشد که تصور این امر غیر ممکن است. مکانیک موجی یک معادله موج بدون امواج واقعی ارائه می‌دهد و مکانیک کوانتم اجازه محاسبه گذارهای اتمی، بدون نمایش فضایی این گذارها (مسیرها) را به ما می‌دهد. تابع موج یا تابع حالت، که به عنوان توصیف حالت فیزیکی به کار گرفته می‌شود، نمی‌تواند به‌عنوان یک نمایش مستقیم از حالت فیزیکی در نظر گرفته شود. ارتباط تابع حالت با حالت فیزیکی، تنها به طور قراردادی می‌باشد، و مانند

[12] Observable

رابطه بین دامنه موج و خود موج است. گرچه معادله مشابهی برای هردو برقرار است، اما دارای معانی فیزیکی متفاوتی هستند.

بور عقیده داشت ریاضیات به کار رفته در فیزیک کلاسیک محدود به اعداد حقیقی است، در حالی که فیزیک کوانتمی ضرورتا از عدد موهومی خالص $i=\sqrt{-1}$ که در معادلات شرودینگر و نیز روابط عدم‌قطعیت هایزنبرگ بین کمیات مزدوج ظاهر می‌شود استفاده می‌کند.

هنگامی که مفاهیم جدیدی وارد فیزیک می‌شوند، در یک غالب ریاضی به کار گرفته می‌شوند. تفاوت عمده بین محدوده‌های فیزیک کلاسیک و فیزیک کوانتمی، در ماهیت فیزیکی ریاضیات به کار گرفته شده نیست، زیرا که آنها تنها یک ابزار هستند. مفاهیم ریاضی و ارتباط آنها در فیزیک کلاسیک به طور مستقیم به موجوداتی ارجاع داده می‌شوند که وجود فیزیکی و خواص فیزیکی دارند، در حالی که در بیان استاندارد مکانیک کوانتمی مفاهیم ریاضی تنها به صورت غیر مستقیم به فیزیک ارجاع داده می‌شوند. تابع حالت صریحا نشان‌دهنده‌ی یک سیستم نیست بلکه نشان‌دهنده‌ی دانشی است که می‌توان از طریق برهم‌کنش با دستگاه اندازه‌گیری بدست آورد.

۲-۳ ناموضعیت کوانتمی

پس از ارائه‌ی مکانیک کوانتمی، اینشتین به مقابله با برخی از مهم‌ترین مبانی این نظریه پرداخت. اینشتین می‌خواست با طرح یک آزمایش ذهنی نشان دهد که روابط عدم قطعیت هایزنبرگ قابل نقض است. پس از آن اینشتین تمام همتش را صرف اثبات ناقص بودن مکانیک کوانتمی کرد. هدف کلی مقاله EPR نیز همین می‌باشد.

علم مکانیک را یک سری از اصول و قوانین در نظر می‌گیریم که حرکت اجسام را به‌صورت علّی تبیین می‌کنند، و مباحثی مانند، برخورد، مکان، سرعت و مسیر ذرات در آن دارای معنی می‌باشند. اصول موضوعه‌ای که در فرمول‌بندی مکانیک کوانتمی به‌کار می‌رود متفاوت با اصولی است که برای فرمول‌بندی مکانیک کلاسیک به کار می‌رود. این اصول، ناموضعیت را در فیزیک کوانتمی وارد می‌کند که مشابه آن را، در مکانیک کلاسیک نداریم. ناموضعیت کوانتمی در سیستم‌های درهم‌تنیده به خوبی نشان داده می‌شود.

در حال حاضر نظریه کوانتمی بسیار گسترده‌تر از مکانیک کوانتمی است. و نه تنها شامل مدل‌های دیگری برای خواص هسته‌ای و اتمی است، از نقطه نظر بنیادی‌تر، به نظریه میدان کوانتمی بسط یافته است. و از الکترودینامیک کوانتمی به نظریه‌های پیمانه‌ای الکتروضعیف و کرومودینامیک بسط یافته. با وجود توسعه‌های بنیادی‌تر فیزیک کوانتمی، مکانیک کوانتمی همچنان چارچوب فکری پایه‌ای برای تحقیق در تمام انواع پدیده‌های کوانتمی است.

۲-۳-۱ تعبیر دیوید بوهم از قضیه EPR[۱۳]

اسپین ذره را با دستگاهی موسوم به اشترن گرلاخ اندازه می‌گیرند. چنین دستگاهی تنها یک مولفه اسپین، که در امتداد محور عمودی آنالیزور است را اندازه می‌گیرد. خاطرنشان می‌شود عملگرهای مولفه‌های X و Z اسپین با هم جابجاپذیر نمی‌باشند:

$$\left[S_x, S_z\right] \neq 0 \qquad (۳-۲)$$

بنابراین اندازه‌گیری‌های S_x و S_z از رابطه عدم‌قطعیت پیروی می‌کنند:

[13] Einstein, Podolsky and Rosen

$$\Delta S_x . \Delta S_z \neq 0 \qquad (۴-۲)$$

بدین ترتیب امکان ندارد دستگاهی بتواند هر سه مولفه‌ی S_x و S_z و S_y را هم‌زمان اندازه بگیرد. در حالی که EPR مدعی است که می‌توان همه این مولفه‌ها را با به کارگیری دستگاه اشترن-گرلاخ با هر دقتی اندازه گرفت.

دیوید بوهم برای تشریح مقاله EPR یک منبع دو ذره‌ای در آنالیزور اشترن-گرلاخ را در نظر گرفت. منبع دو ذره‌ای ابزاری است که دو ذره شلیک می‌کند به‌طوری‌که اسپین کل آنها صفر و اسپین هر ذره $\frac{1}{2}$ می‌باشد. لذا جهت اسپین هر ذره مخالف جهت اسپین ذره دیگر است. یکی از ذرات به سمت آنالیزور اول و دیگری به سمت آنالیزور دوم ارسال می‌شود. این ذرات در مکان‌های دور از هم در فضا هستند. مشاهده‌گر اولی در مکان A و مشاهده‌گر دومی در مکان B قرار دارند.

مشاهده‌گر آلیس در مکان A و مشاهده‌گر باب در مکان B می‌توانند آنالیزور خود را به هر طرف که بخواهند جهت دهند. وقتی آزمایش شروع می‌شود منبع یک جفت ذره تولید می‌کند و آنها را به طرف بیرون یعنی به طرف دو آزمایشگر گسیل می‌دارد. فرض کنید در ابتدا آلیس آنالیزور اشترن–گرلاخ خود را در جهت $\hat{a}$ گرفته باشد که عمود بر سطح مسیر ذره‌ای است که به طرف او می‌رود (در جهت عمودی به سمت بالا یعنی در جهت Z نشانه رفته باشد) وقتی ذره وارد آنالیزور A می‌شود دستگاه یکی از دو جواب اسپین بالا یا اسپین پایین را می‌دهد. اگر در این اندازه‌گیری خاص اسپین بالا نتیجه شود چون جهت اسپین هر ذره مخالف جهت اسپین ذره دیگر است، آلیس نتیجه می‌گیرد که ذره باب در امتداد محور Z، اسپین پایین دارد. بدین طریق آلیس مولفه‌ی Z اسپین ذره‌ای را که به سمت باب می‌رود را اندازه گرفته است. مشاهده‌گرهای A و B اگر بخواهند می‌توانند این نتیجه را با جهت‌گیری آنالیزور مشاهده‌گر B ($\hat{b}$) در امتداد Z محک بزنند، یعنی در ابتدا مشاهده‌گر B اندازه‌گیری خود را انجام دهد و جهت اسپین آلیس را حدس بزند.

در مقاله EPR تاکید شده که به‌علت فاصله بسیار زیاد مکان‌های A و B، مقدار اندازه‌گیری شده یک کمیت در یک سیستم نمی‌تواند از اندازه‌گیری کمیتی روی سیستم دیگر تاثیرپذیر باشد. بنابراین نتیجه‌ای که آلیس بدست می‌آورد نمی‌تواند هیچ اثری بر روی اسپین ذره باب داشته باشد. از این نکته EPR نتیجه می‌گیرند که حتی پیش از اینکه آلیس اندازه‌گیری خود را انجام دهد ذره باب در امتداد محور Z باید اسپین داشته باشد. به منظور دانستن اسپین ذره باب مسلما اندازه‌گیری آلیس لازم است اما این اندازه‌گیری نمی‌تواند بر ذره باب اثری بگذارد. تنها کار آلیس این بوده که واقعیت موجود از پیش را پیدا کند.

حال فرض کنید انتخاب آلیس سمت‌گیری متفاوتی از آنالیزور قبلی‌اش داشته باشد، مثلا به جای مولفه Z مولفه X را انتخاب کند، دقیقا همان استدلال صادق است. یعنی آلیس اکنون می‌تواند مولفه X اسپین ذره‌ای را که به سمت ذره باب می‌رود اندازه بگیرد و اطمینان داریم که این مولفه بایستی پیش از اندازه‌گیری مشاهده‌گر A وجود داشته باشد. بدین‌سان EPR نتیجه می‌گیرد که هر دو متغیر مکملی که ذره باب را توصیف می‌کند (یعنی S_x، S_z) وجود خارجی دارند و دارای مقدار معینی هستند. در حالی که بنا بر اصل عدم قطعیت آنها نمی توانند هم‌زمان مشخص شوند. این استدلال را با اندکی تغییر می‌توان بیان کرد. اگر مشاهده‌پذیر A آنالیزور خود را در امتداد مولفه Z و مشاهده‌گر B آنالیزور خود را در امتداد X جهت دهند، با این استدلال مشاهده‌گر A می‌تواند به اسپین ذره مشاهده‌گر B در امتداد Z پی‌ببرد. اما اکنون مشاهده‌گر B می‌تواند مستقیما اسپین ذره خود را در امتداد محور X اندازه بگیرد، یعنی باز هم در مورد دو متغیر مکمل بر خلاف اصول مکانیک کوانتمی می‌توان به نتایج مشخصی دست یافت. بنابر نظر EPR یا مکانیک کوانتمی ناقص است چون نمی‌تواند S_x وS_z را به‌صورت هم‌زمان مشخص کند، یا این ذرات که به‌صورت فضاگونه از یکدیگر جدا شده‌اند مستقل از هم نیستند. و چون نمی‌توانست وجود ذرات درهم‌تنیده‌ی ناموضع را بپذیرد اظهار داشت که نظریه‌ی کوانتمی ناقص است [۴و۵].

۲-۳-۲موضعیت

موضعیت بدین معناست که نتیجه و یا نتیجه احتمال یک اندازه‌گیری که روی قسمتی از یک سیستم مرکب با حالت $|\psi\rangle$ (سیستم ۱ + سیستم ۲) انجام می‌شود مستقل از جنبه‌های مولفه‌های قسمت‌های دیگر است که آزمایشگر برای اندازه‌گیری انتخاب می‌کند این به هیچ وجه به این معنی نیست که نتوان با بررسی سیستم ۱ اطلاعاتی در مورد سیستم ۲ بدست آورد.

حالت $|\psi\rangle$ شامل اطلاعات مشترک مربوط به هر دو سیستم است و اندازه‌گیری روی یکی از این سیستم‌ها بخشی از این اطلاعات را آشکار می‌سازد. همچنین اگر یک اندازه‌گیری روی یک قسمت از سیستم مرکب انجام شود باعث اغتشاش موضعی آن قسمت می‌گردد و این با موضعیت مغایرتی ندارد [۶].

۲-۴ درهم‌تنیدگی[۱۴]

درهم‌تنیدگی کوانتمی یکی از منابع مهم مکانیک کوانتمی می‌باشد. با به کارگیری حالات درهم‌تنیده شده‌ی کوانتمی قادر به انجام اموری می‌شویم که در دنیای کلاسیک سخت یا غیر ممکن هستند. حالت‌های درهم‌تنیده نتیجه‌ی شگفت انگیزی را دربردارند. در این حالات چنانچه روی یکی از جفت ذرات اندازه‌گیری انجام دهیم با درنظرگرفتن اندازه‌گیری در جهت خاصی وضعیت ذره دیگر از حالت نامشخصی که قبل از اندازه‌گیری داشت در آمده و به وضعیت معین و ثابتی می‌رسد که توسط آزمایش ما تعیین می‌شود. این تاثیر حتی در وضعیتی که اندازه‌گیری‌های آلیس و باب فاصله فضا گونه داشته باشند نیز برقرار است.

اگر دو ذره در هم‌تنیده میلیونها کیلومتر ازهم دور باشند و روی یکی از آن دو ذره عمل اندازه‌گیری انجام دهیم در همان لحظه می‌توان اطلاعات ذره دوم را بدست آورد. اما می‌توان نشان داد

[14] Entanglement

که آلیس با اندازه‌گیری‌های خود تنها می‌تواند نتایج آزمایش‌های باب را پیش‌بینی کند و به هیچ وجه نمی‌تواند علامت یا سیگنالی را برای باب مخابره کند (عدم علامت دهی).

برای اثبات این مطلب فرض کنید حالت $|\psi\rangle$ بین آلیس و باب به اشتراک گذاشته شده و دارای عملگر چگالی[15] زیر می‌باشد:

$$\rho = |\psi\rangle\langle\psi| \qquad (۵-۲)$$

بنابراین ماتریس چگالی ذره‌ای که در دست باب خواهد بود به صورت زیر است:

$$\rho_B = Tr_A(|\psi\rangle\langle\psi|) \qquad (۶-۲)$$

حال فرض کنید که آلیس یک اندازه‌گیری تصویری با عملگرهای $\{P_m\}$ بر روی ذره‌ی خود انجام دهد در این صورت ماتریس چگالی کل سیستم به صورت زیر تبدیل می‌شود:

$$\rho' = \sum_m (P_m \otimes I)|\psi\rangle\langle\psi|(P_m^\dagger \otimes I) \qquad (۷-۲)$$

بعد از اندازه‌گیری، ماتریس چگالی ذره‌ای که در دست باب است برابر خواهد بود با:

$$\rho'_B = Tr_A(\rho') = Tr_A(\sum_m (P_m \otimes I)|\psi\rangle\langle\psi|(P_m^\dagger \otimes I)) \qquad (۸-۲)$$

از خاصیت دوره‌ای بودن تابع رد(که در آن مطابق رابطه‌ی زیر، عملگرهای X و Z روی فضای A عمل کرده و عملگر Y نیز روی هر دو فضای A و B عمل می‌کند) در رابطه‌ی بالا استفاده می‌کنیم:

$$Tr_A((X \otimes I)Y(Z \otimes I)) = Tr_A((Z \otimes I)(X \otimes I)Y) \qquad (۹-۲)$$

بنابراین رابطه بالا را می‌توان به شکل زیر بازنویسی کرد:

[15] Density operaror

$$\rho'_B = Tr_A(\sum_m (P_m^\dagger \otimes I)(P_m \otimes I)|\psi\rangle\langle\psi|) = Tr_A(|\psi\rangle\langle\psi|) = \rho_B \qquad (۱۰-۲)$$

از این رو حالت ذره‌ای که در دست باب است با اندازه‌گیری‌های آلیس تغییر نمی‌کند و در نتیجه اندازه‌گیری‌های آلیس به هیچ وجه باعث تغییر در حالت ذره‌ی باب نخواهد شد و در نتیجه هیچ نوع علامت یا اطلاعی به باب مخابره نمی‌شود.

درهم‌تنیدگی در کلاسیک مانند شکستن یک سکه به دو تکه است که با مشاهده یک نصفه از آن می توان به شکل و مشخصات تکه‌ی دیگر پی‌برد، زیرا دو تکه به صورت مشترک اطلاعات سکه کامل را دربردارند. به عبارتی مشاهده یک تکه از سکه مشخصات تکه دیگر را به طور کامل روشن می‌سازد. اینشتین معتقد بود ارتباط میان این دو تکه درهم‌تنیده توسط متغیرهای مخفی برقرار می‌شود که ما هیچ اطلاعاتی راجع به آنها نداریم.

پدیده شگفت انگیز درهم‌تنیدگی تحول عظیمی را در تئوری مکانیک کوانتمی بوجود آورده و به تبع آن نتایجی را در رایانه‌های کوانتمی به دنبال داشته است. از نتایج بسیار مهم درهم‌تنیدگی کوانتمی نقض موضعیت است.

۲-۴-۱ حالت‌های درهم‌تنیده‌ی بل

سیستم دو قسمتی، سیستمی است که شامل دو زیرسیستم باشد. یک مثال از این سیستم، زمانی است که دو مشاهده‌گر آلیس و باب هر کدام دارای یک ذره هستند و بر روی ذره‌ی مربوط به خود اندازه‌گیری انجام می‌دهند. فضای هیلبرت مربوط به چنین سیستمی به صورت $(H_A \otimes H_B)$ یعنی ضرب تانسوری حاصل از دو زیر سیستم است.

یک مثال ازسیستم‌های دو قسمتی حالت‌های بل هستند که به آنها حالات EPR هم می‌گویند به حالت $|\beta_{11}\rangle$حالت یگانه (تکتایی[۱۶]) می‌گوییم که دارای اسپین ۰ است و به حالت $|\beta_{01}\rangle$ به همراه حالت $|00\rangle$ و $|11\rangle$ حالت‌های سه‌گانه[۱۷] گوییم ($m_s = \pm 1, 0$) که دارای اسپین ا می‌باشند. این حالات به فرم کلی زیر نمایش داده می‌شوند:

$$|\beta_{ab}\rangle = \frac{|0b\rangle + (-1)^a |1\bar{b}\rangle}{\sqrt{2}} \qquad (۱۱-۲)$$

در عبارت بالا a را بیت فاز و b را بیت پاریته می‌نامیم ($\bar{b}$ مقدار عکس b را بیان می‌کند برای مثال چنانچه مقدار $b = 1$ آنگاه $\bar{b} = 0$)[۷].

هر کدام از دو ذره دارای اسپین $\frac{1}{2}$ می‌باشند. اگر آلیس اندازه‌گیری انجام ندهد آنگاه باب با احتمال $\frac{1}{2}$ ذره را در جهت مثبت و یا منفی Z اندازه‌گیری می‌کند. اگر مشاهده‌گر آلیس با اعمال عملگر S_z بر روی ذره خود اسپین ذره را مثبت بدست بیاورد آن‌گاه مشاهده‌گر باب با قطعیت مقدار اسپین ذره خود را منفی بدست می‌آورد و همین‌طور بالعکس، یعنی چنانچه مشاهده‌گر آلیس عملگر S_z را بر روی ذره مربوط به خود اعمال کند و مقدار منفی بدست آورد مشاهده‌گر باب با قطعیت مقدار اسپین ذره خود را مثبت بدست می‌آورد.

در ادامه فرض کنید مشاهده‌گر آلیس در انتخاب جهت اندازه‌گیری آزاد باشد و بتواند عملگر S_x یا S_z را بر روی ذره‌ی خود اعمال کند، در حالی که مشاهده‌گر باب ملزم به اعمال عملگر S_x باشد. حال اگر مشاهده‌گر آلیس عملگر S_x را بر روی ذره خود اعمال کند مشاهده‌گر باب با قطعیت جهت اسپین ذره‌ی خود را درمی‌یابد در حالی که اگر مشاهده‌گر آلیس عملگر S_z را بر روی ذره‌ی خود اعمال کند، مشاهده‌گر باب با احتمال $\frac{1}{2}$ اسپین خود را در جهت مثبت یا منفی محور Xها اندازه می‌گیرد.

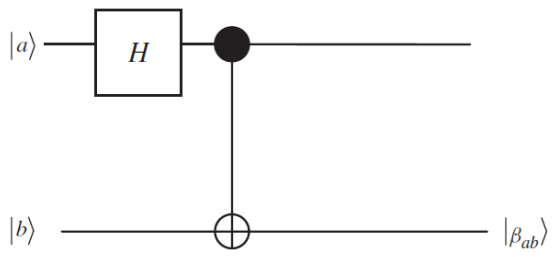
[16] Singlet
[17] Triplet

بنابراین می‌توان به این نکته پی برد که تصمیم مشاهده‌گر آلیس برای اعمال جهت اندازه‌گیری بر احتمال بدست آمدن نتیجه‌ی باب تاثیر می‌گذارد.

حالتی مثل $|\psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle$ را در نظر بگیرید. آلیس بدون اینکه اندازه‌گیری انجام دهد می‌تواند به طور قطع بگوید که حالت باب $|0\rangle$ است. حال اگر آلیس روی کیوبیت خود اندازه‌گیری در راستای محور Z انجام دهد و مقدار $|0\rangle$ را بدست آورد می‌تواند به طور قطع بگوید که حالت کیوبیتی که در دست باب است $|0\rangle$ می‌باشد. و اگر نتیجه‌ی اندازه‌گیری‌اش $|1\rangle$ باشد باز هم به طور قطع می‌تواند بگوید که حالت کیوبیتی که در دست باب است $|0\rangle$ می‌باشد. بنابراین نتیجه‌ی اندازه‌گیری آلیس بر روی اطلاعی که آلیس از حالت کیوبیت باب دارد تاثیری نخواهد گذاشت. چنین حالاتی را حالات جدایی پذیر[18] می‌گوییم.

۲-۴-۲ مدل ریاضی درهم‌تنیدگی کوانتمی

با استفاده از گیت‌های کوانتمی می‌توانیم مدل ریاضی یک زوج درهم‌تنیده را به‌صورت شکل (۲-۲) داشته باشیم. این مدار از سری کردن گیت هادامارد و C-NOT بدست می‌آید. اگر ورودی این مدار را یکی از حالات $|00\rangle$ و $|10\rangle$ و $|01\rangle$ و $|11\rangle$ در نظر بگیریم، چهار حالت درهم‌تنیده‌ی بل بدست می‌آید.



شکل (۲-۲): مدار کوانتمی ساخت حالات درهم‌تنیده‌ی بل

[18] Separable

ورودی را در حالت اول به‌صورت $|a\rangle\otimes|b\rangle=|ab\rangle=|00\rangle$ فرض کرده و خروجی مدار را محاسبه می‌کنیم. حالت $|0\rangle$ پس ازعبور از گیت هادامارد به حالت زیر تبدیل می‌شود:

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

در نتیجه قبل از تاثیر گیت C-NOT حالت کوانتمی ترکیبی عبارت است از:

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle) \qquad (۱۳-۲)$$

در اثر عبور این حالت کوانتمی از گیت C-NOT حالت درهم‌تنیده‌ی زیر حاصل می‌شود:

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle\xrightarrow{C-NOT}\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \qquad (۱۴-۲)$$

چنانچه ورودی را سه حالت دیگر $|01\rangle$ و $|10\rangle$ و $|11\rangle$ در نظر بگیریم سه حالت دیگر بل بدست می‌آیند. لذا داریم:

$$\begin{aligned}
&|00\rangle\rightarrow\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\\
&|10\rangle\rightarrow\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)\\
&|01\rangle\rightarrow\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)\\
&|11\rangle\rightarrow\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)
\end{aligned} \qquad (۱۵-۲)$$

چندین روش برای تشخیص درهم‌تنیدگی وجود دارد. یک حالت خالص دو طرفه را می‌توان به فرم زیرنوشت که به آن تجزیه‌ی اشمیت حالت $|\psi\rangle$ گفته می‌شود:

$$|\psi\rangle=\sum_{n=1}\lambda_n|a_n\rangle|b_n\rangle \qquad (۱۶-۲)$$

حالت $|\psi\rangle$ متعلق به فضای هیلبرت $(H_A \otimes H_B)$ می‌باشد. در اینجا ضرایب λ_n، ضرایب اشمیت نام دارند که دارای دو ویژگی $\lambda_n \geq 0$ و $\sum_n {\lambda^2}_n = 1$ هستند. به تعداد ضرایب اشمیت غیر صفر عدد اشمیت می‌گویند. با استفاده از عدد اشمیت می‌توان پی به درهم‌تنیدگی سیستم برد بدین صورت که[۷]:

- هر حالت جدایی پذیر عدد اشمیت ۱ دارد.
- اگر عدد اشمیت بزرگتر از ۱ باشد، آن را حالت درهم‌تنیده می‌گوییم.

در اینجا برای تشخیص جداپذیر بودن سیستم روش دیگری را ارائه می‌دهیم. فرض کنید سیستم M از دو زیر سیستم A و B تشکیل شده است. با فرض اینکه ρ_A و ρ_B ماتریس‌های چگالی مربوط به A و B باشند، $|\psi_{AB}\rangle$ را جداپذیر می‌گوییم اگر بتوان ماتریس چگالی آن را به صورت زیر نوشت:

$$\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}| = \sum a_{i\,\mu} \rho_A^i \otimes \rho_B^\mu \qquad (۱۷-۲)$$

که $a_{i\,\mu}$ بیانگر احتمال حضور سیستم در حالت $i\,\mu$ام می‌باشد. اگر ماتریس چگالی $|\psi_{AB}\rangle$ را نتوان به صورت حاصلضرب ماتریس چگالی زیر سیستم‌ها نوشت حالت ما، درهم‌تنیده می‌باشد.

برای سیستم‌هایی که بیشتر از دو زیر سیستم دارند، تعاریف درهم‌تنیدگی و جدایی‌پذیر بودن می‌تواند وسیع‌تر باشد. به طور کلی در سیستمی که از N قسمت تشکیل شده است، به روش‌های زیادی می‌توان سیستم را به ۲،۳،...و N قسمت تقسیم کرد. حتی اگر در یکی از این تقسیم‌بندی‌ها درهم‌تنیدگی بین اجزای مختلف غیر صفر باشد، می‌گوییم که درهم‌تنیدگی چند طرفی داریم. ولی اگر در همه‌ی این تقسیم‌بندی‌ها در هم‌تنیدگی بین اجزا صفر باشد می‌گوییم که سیستم جدایی‌پذیر کامل است و ماتریس چگالی آن را می‌توان به صورت زیر نوشت:

$$\rho = \sum_{i=1}^{n} p_i \rho_i^{(1)} \otimes \rho_i^{(2)} \otimes \rho^{(3)} ... \otimes \rho^{(N)} \qquad \sum_{i=1}^{n} p_i = 1 \qquad \forall p_i \geq 0 \qquad (۱۸-۲)$$

حالات درهم‌تنیده چند قسمته را حالاتی معرفی می‌کنیم که نتوان ماتریس چگالی آن‌ها را به‌صورت بالا نوشت. برای درک بهتر در اینجا سیستم‌های ساده‌ی سه قسمته را به عنوان مثال می‌آوریم. در سیستم‌های سه قسمته برخلاف سیستم‌های دو قسمته دو کلاس مختلف درهم‌تنیدگی داریم. این حالت‌های درهم‌تنیده $|GHZ\rangle$ و $|W\rangle$ می‌باشند. همچنین با افزایش تعداد قسمتهای این سیستم، تعداد این کلاس‌ها هم بیشتر می‌شود.

۲-۴-۳ حالت GHZ[۱۹]

حالت GHZ یک حالت درهم‌تنیده است. که از $N \geq 3$ قسمت تشکیل شده است که آن را به شکل زیر نمایش می‌دهیم:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}) \qquad (۱۹-۲)$$

مثلا حالت GHZ سه‌قسمته برابر است با:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \qquad (۲۰-۲)$$

بدیهی است که چنین حالتی را نمی‌توان به‌صورت ضرب تانسوری سه حالت مختلف، مربوط به سه زیر فضا نوشت. در اینجا اگر یک اندازه‌گیری در پایه Z روی یکی از کیوبیت‌ها انجام شود، حالت دو کیوبیت دیگر به یک حالت جدایی‌پذیر تبدیل می‌شود. بنابراین درهم‌تنیدگی چند طرفه بدین معنا نیست که بین هر طرفین سیستم درهم‌تنیدگی وجود داشته باشد [۸].

[19] Greenberger. Horne and Zelinger

۲-۴-۴ حالت W

حالت W یک حالت درهم‌تنیده است که از $N \geq 3$ قسمت تشکیل یافته است. به طور کلی حالت Wای که از N قسمت تشکیل شده باشد عبارت است از:

$$|W\rangle = \frac{1}{\sqrt{M}}(|000...1\rangle + |000...10\rangle + ... + |100...0\rangle) \qquad (۲۱-۲)$$

بنابراین حالت‌های W، برهم‌نهی حالت‌هایی هستند که در همه‌ی آنها یکی از کیوبیت‌ها در حالت برانگیخته‌ی $|1\rangle$ است و بقیه‌ی کیوبیت‌ها در حالت پایه‌ی $|0\rangle$ قراردارند. مثلا حالت W سه‌تایی برابراست با:

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \qquad (۲۲-۲)$$

بدیهی است که چنین حالتی را نمی‌توان به صورت ضرب تانسوری سه حالت مختلف، مربوط به سه زیر فضا نوشت. بنابراین می‌توان گفت که درهم‌تنیدگی چند قسمتی دارد [۸].

۲-۵ عدم علامت‌دهی[۲۰]

نظریه‌های مکانیک کوانتمی و نسبیت شالوده‌های اصلی دانش فیزیک را در عصر حاضر تشکیل می‌دهند. نسبیت خاص می‌گوید امکان ارسال ماده، انرژی و پیام با سرعتی بالاتر از نور میسر نمی‌باشد. مکانیک کوانتمی نیز نظریه‌ای است که در آزمایش موفق بوده، و پدیده‌های جدیدی را در مقایسه با مکانیک کلاسیک توجیه و پیش‌بینی کرده است، ولی به ساختارهای مفهومی آن ایرادهای بسیاری وارد شده است.

[20] No-signaling

پدیده‌هایی در مکانیک کوانتمی وجود دارد که در ظاهر سرعت بالاتر از نور را مجاز می‌داند، و در واقع با مبانی نسبیت ناسازگار است. مهم‌ترین این پدیده‌ها درهم‌تنیدگی می‌باشد. با مطرح شدن ناموضعیت در مکانیک کوانتمی به نظر می‌رسد که بین دو نظریه اصلی عصر حاضر تعارض اساسی وجود دارد. در نسبیت دارای توصیف موضعی از طبیعت می‌باشیم، در حالی که در فیزیک کوانتمی ناموضعیت را داریم. تلاش‌های بسیاری انجام شد که تضاد میان مکانیک کوانتمی و نسبیت به طور کامل نشان داده شود، در واقع تلاش شد تا ازپدیده‌ی درهم‌تنیدگی برای ارسال اطلاعات با سرعت بیشتر از نور استفاده شود. با این حال همه‌ی این تلاش‌ها به شکست انجامیده است. و با اثبات قضایایی نشان داده شده که امکان ارسال فوق نوری اطلاعات در مکانیک کوانتمی وجود ندارد. این اثبات‌ها به قضایای عدم علامت دهی مشهور هستند.

با رد شدن امکان پیام‌دهی فوق نوری، بعضی گفته‌اند که نظریه فیزیک کوانتمی و نسبیت همزیستی مسالمت آمیزی با هم دارند، یعنی اگر چه به نظر می‌آید ویژگی‌هایی در نظریه کوانتمی وجود دارد که با نسبیت ناسازگار هستند، ولی در سطح تجربه و مشاهدات آزمایشگاهی، تعارضی بین این دو نظریه وجود ندارد.

۲-۶ قضیه بل

بل درسال ۱۹۶۴ قضیه‌ای منتشرکرد که به نام وی شهرت یافت. نامساوی‌های بل بر اساس مدل‌های موضعی متغیر پنهان بوجود می‌آیند و این نامساوی‌ها در مکانیک کوانتمی نقض می‌شوند. در تمامی مدل‌های موضعی متغیر پنهان دو فرض اساسی موضعیت و واقعیت فیزیکی وجود دارد. از نقض این نامساوی توسط مکانیک کوانتمی می‌توان چنین نتیجه گرفت که مکانیک کوانتمی حداقل با یکی

از این دو فرض در تعارض است. از طرفی طبیعت، پیش‌بینی‌های مکانیک کوانتمی را تایید می‌کند پس یکی و یا هر دو فرضی که در اثبات نامساوی بل به کار رفته است نادرست می‌باشد.

۲-۶-۱ اثبات قضیه بل

سیستمی متشکل از ذرات A و B که به‌صورت جفت ذره و هر کدام با اسپین $\frac{1}{2}$ در حالت یگانه می‌باشند را در نظر می‌گیریم. اندازه‌گیری توسط دستگاه اشترن–گرلاخ روی مولفه‌های اسپینی انجام می‌گیرد. نتیجه اندازه‌گیری عملگر A روی ذره اول (A) بوسیله $\vec{a}$ و λ (متغیر پنهان) مشخص می‌شود و نتیجه اندازه‌گیری عملگر B روی ذره دوم (B) بوسیله $\vec{b}$ و λ (متغیر پنهان) مشخص می‌شود. نتایج اندازه‌گیری عملگرهای A و B به‌ترتیب با $A_{\vec{a}}(\lambda_{HV})$ و $B_{\vec{b}}(\lambda_{HV})$ نشان می‌دهیم. پارامتر اندازه‌گیری λ می‌تواند مربوط به ذره یا دستگاه اندازه‌گیری یا محیط و یا ترکیبی از اینها باشد. فرض کنیم که نتیجه اندازه‌گیری عملگر A روی ذره اول وابسته نیست به اندازه‌گیری عملگر B روی ذره دوم و همینطور بالعکس و هم‌چنین برهم‌کنشی بین دو ذره A و B وجود ندارد. فرض کنید پارامترهای غیر قابل کنترل λ دارای توزیع احتمال باشد(و همچنین $A_{\vec{a}}(\lambda_{HV})=\pm1, B_{\vec{b}}(\lambda_{HV})=\pm1$)،لذا مقدار انتظاری حاصل از اندازه‌گیری دو مولفه، توسط دو کاربر برابر است با:

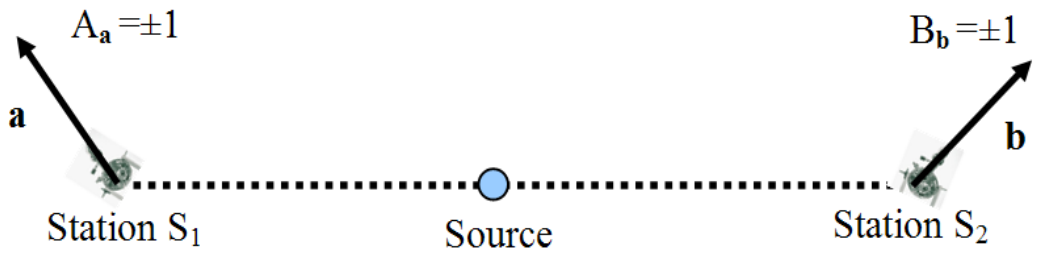
$$p(\vec{a},\vec{b})=\int d\,\lambda_{HV}\,p(\lambda_{HV})A_{\vec{a}}(\lambda_{HV})B_{\vec{b}}(\lambda_{HV}) \qquad (۲۳-۲)$$

با فرض شرط بهنجارش داریم:

$$\int d\,\lambda_{HV}\,p(\lambda_{HV})=1$$

با توجه به اینکه سیستم در حالت یگانه قرار دارد وقتی که $\vec{a}=\vec{b}$ باشد، $p(\vec{a},\vec{b})=-1$ خواهد شد و این زمانی صادق است که داشته باشیم:

$$A_{\vec{a}}(\lambda_{HV}) = -B_{\vec{b}}(\lambda_{HV})$$



شکل (۲-۳): نمایشی از آزمایش بل

در این صورت داریم:

$$p(\vec{a},\vec{b}) = -\int d\,\lambda_{HV}\, p(\lambda_{HV}) A_{\vec{a}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV}) \qquad (۲۴-۲)$$

با درنظرگرفتن دو اندازه‌گیری مختلف a و a' برای دستگاه اول و دو اندازه‌گیری مختلف b و b' برای دستگاه دوم داریم:

$$\begin{aligned} &p(\vec{a},\vec{b}) - p(\vec{a},\vec{b'}) = -\int d\,\lambda_{HV}\, p(\lambda_{HV})[A_{\vec{a}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV}) - A_{\vec{a}}(\lambda_{HV}) A_{\vec{b'}}(\lambda_{HV})] = \\ &-\int [A_{\vec{a}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV}) - A_{\vec{a}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV}) A_{\vec{b'}}(\lambda_{HV})] p(\lambda_{HV}) d\,\lambda_{HV} \\ &= \int A_{\vec{a}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV})[A_{\vec{b'}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV}) - 1] p(\lambda_{HV}) d\,\lambda_{HV} \end{aligned} \qquad (۲۵-۲)$$

از آنجایی‌که مقدار حداکثر $A_{\vec{a}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV})$، ۱+، و مینیمم مقدار آن ۱- می‌باشد، داریم:

$$\begin{aligned} &[p(\vec{a},\vec{b}) - p(\vec{a},\vec{b'})]_{\max} = \int (-1)[A_{\vec{b'}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV}) - 1] p(\lambda_{HV}) d\,\lambda_{HV} \\ &= \int (+1)[1 - A_{\vec{b'}}(\lambda_{HV}) A_{\vec{b}}(\lambda_{HV})] p(\lambda_{HV}) d\,\lambda_{HV} \end{aligned} \qquad (۲۶-۲)$$

خود را محدود به $A_{\vec{a}}(\lambda_{HV}) = \pm 1$ و $B_{\vec{b}}(\lambda_{HV}) = \pm 1$ نمی‌کنیم، بلکه مقادیر ضعیف‌تر را نیز در نظر می‌گیریم:

$$\left|p(\vec{a},\vec{b})-p(\vec{a},\vec{b'})\right| \le \int [A_{\vec{b'}}(\lambda_{HV})A_{\vec{b}}(\lambda_{HV})-1]p(\lambda_{HV})d\lambda_{HV} \qquad (۲۷-۲)$$

و در نهایت خواهیم داشت:

$$\left|p(\vec{a},\vec{b})-p(\vec{a},\vec{b'})\right| \le 1+p(\vec{b},\vec{b'}) \qquad (۲۸-۲)$$

رابطه فوق معروف به اولین نامساوی بل است.

۲-۷ متغیرهای پنهان

نامساوی بل بر واقعیت گرایی موضعی[۲۱] استوار است. نامساوی بل نتیجه کاربرد عقل سلیم و استدلال بر مبنای دو فرض اساسی یعنی موضعیت و فرض وجود واقعیت خارجی است. اصل موضعیت همانطور که قبلا هم اشاره کردیم به این معناست که دو سیستم نمی‌توانند به صورت آنی در محیطی که قرار گرفته‌اند با هم تبادل اطلاعات فیزیکی انجام دهند. واقعیت فیزیکی نیز بدین معناست که اگر بدون اینکه اختلالی به سیستم وارد کنیم بتوانیم مقدار آن کمیت را با دقت کامل (با احتمال برابر با یک) پیش‌بینی کنیم. پس بنابراین یک عنصر واقعیت فیزیکی وابسته به یک کمیت فیزیکی قبل از عمل اندازه‌گیری وجود دارد.

سوالی که بل مطرح می‌کند این است که رویدادهای تصادفی‌ای که ناشی از وجود پارامترهای پنهان هستند و دارای دو خاصیت موضعیت و واقعیت می‌باشند، چه نوع ویژگی‌ای دارند؟ در پاسخ به این سوال بل می‌گوید که نتایج رویدادهای تصادفی با دو ویژگی بارز موضعیت و واقعیت، در یک نامساوی بسیار ساده صدق می‌کنند. در آزمایشگاه مشاهده می‌کنیم که در طبیعت این نامساوی نقض

[21] Local reality

می‌شود، بنابراین به این نتیجه می‌رسیم که موضعیت یا واقعیت و یا هر دوی آنها که در نامساوی بل در نظر گرفته‌ایم درست نمی‌باشند.

متغیرهای پنهان در واقع وجود یک‌سری متغیرهایی است که نمی‌توانیم از آنها آگاه شویم، و کمیت‌های فیزیکی به‌وسیله آنها معین می‌شوند. بنابر مدل بوهم احتمال و شانسی که در مکانیک کوانتمی مطرح می‌شود به دلیل ندانستن این متغیرهاست. در یک تئوری متغیرهای پنهان، اندازه‌گیری اساسا به‌صورت علمی قطعی است اما نتایج در این تئوریها هم به‌صورت احتمالاتی بیان می‌شود، زیرا که درجات آزادی سیستم به‌دقت شناخته نمی‌شوند. اگر ما از مقدار متغیر پنهان آگاهی داشته باشیم آن‌گاه توزیع احتمالی که حاکم است بر اندازه‌گیری موافق با پیش‌بینی‌های نظریه کوانتمی است. زمانی که یک نظریه متغیرهای پنهان موضعی است این بدان معناست که دارای همان محدودیت‌های موضعی اینشتین می‌باشیم.

۲-۸ آنتروپی و اطلاعات کوانتمی

شانون با مقاله‌ای که در زمینه‌ی نظریه اطلاعات داد خود را یکی از تاثیرگذارترین افراد در این زمینه معرفی کرد. نتایج مطالعات شانون در زمینه کامپیوترهای کلاسیکی و نظریه اطلاعات هنوز هم اهمیت به‌سزایی در حل مشکلات این شاخه از علوم و مهندسی دارد. هدف این است که با استفاده از آنتروپی شانون محتوای اطلاعاتی یک سیستم کلاسیکی را تعیین کنیم و در ادامه ویژگی‌های مهم آن را معرفی کنیم. در ادامه نیز معادل کوانتمی آنتروپی شانون، یعنی آنتروپی فون نویمان[۲۲] را معرفی می‌کنیم.

[22] Von Neumann

۲-۸-۱ آنتروپی شانون[۲۳]

آنتروپی شانون به ازای توزیع احتمال یک متغیر تصادفی که می‌تواند شیر یا خط را با احتمال‌های $\frac{1}{2}$، $\frac{1}{2}$ اندازه بگیرد، همان مقدار اطلاعاتی را در بر دارد که اگر مقادیر 0 یا 1 را با احتمال‌های $\frac{3}{4}$ و $\frac{1}{4}$ اختیار می‌کرد. با توجه به تعریف آنتروپی متغیر تصادفی که در ادامه می‌آوریم این آنتروپی تابعی از احتمال مقادیر ممکن و مختلف است که متغیر تصادفی می‌تواند اختیار کند. اغلب آنتروپی به صورت تابعی از توزیع احتمال $p_1,p_2,p_3,...,p_n$ نوشته می‌شود. شانون نشان داد که آنتروپی متناسب با این توزیع احتمال را می‌توان به صورت زیر تعریف کرد:

$$H(x)=H(p_1,p_2,p_3,...,p_n)=-\sum_i p_i \log p_i \qquad (۲۹-۲)$$

شانون برای سازگاری‌اش با سیستم‌های دودویی پیشنهاد داد که مبنای لگاریتم 2 درنظر گرفته شود. تعریف آنتروپی به شکل (۲-۲۹) کمترین فضای لازمه برای ذخیره اطلاعات را به خود اختصاص می‌دهد و اگر این فرمولبندی را به شکل دیگری بیان کنیم قطعا مقداری از اطلاعات نادیده گرفته خواهد شد. ممکن است که $p=0$ تعجب برانگیز باشد(چون $0\log 0$ تعریف نشده است) به طور شهودی حادثه‌ای که هیچ‌گاه اتفاق نمی‌افتد سهمی در آنتروپی ندارد. بنابراین با قرار داد توافق می‌کنیم که $0\log 0=0$ یا به صورت فرمولی‌تر $\lim_{x\to 0} x\log x=0$. از رابطه شانون مشخص است که مقدار حداکثر $H(x)$ هنگامی است که همه خروجی‌های یک رویداد دارای احتمال یکسان باشند، در این‌صورت ناآگاهی ما از سیستم بیشینه است. و در صورتی که همه احتمال‌ها به جز یکی صفر باشند عدم‌قطعیت ما از سیستم کمینه بوده و برابر صفر می‌شود، که امری کاملا طبیعی است. هر چه، پیش آمدی که رخ داده محتمل‌تر باشد اطلاعاتی که بعد از اندازه‌گیری کسب کرده‌ایم کمتر، و هر چه آن اتفاق دور از انتظار باشد تعجب ما از وقوع آن رویداد بیشتر و در نتیجه اطلاعی که کسب کرده‌ایم

[23] Shannon entropy

بیشتر خواهد بود. بنابراین میزان اطلاعاتی که بعد از وقوع پیشامد بدست می‌آیند نسبتی معکوس با احتمال رخ‌دادن آن پیشامد قبل از وقوع دارند این نتایج با رابطه شانون کمال سازگاری دارند.

گفتیم حداکثر آنتروپی زمانی بدست می‌آید که ما حداقل دانش را قبل از اندازه‌گیری نسبت به سیستم داشته باشیم. و ما حداقل دانش را زمانی داریم که احتمال بدست آوردن هر یک از نتایج اندازه‌گیری یکسان باشد:

$$P_{\mathrm{n}} = \frac{1}{\mathrm{n}} \qquad (۳۰-۲)$$

که در این رابطه n تعداد پیشامدهاست. یک مثال ساده زمانی است که دو خروجی داریم. در ابتدا فرض می‌کنیم که هر دو احتمال برابر هستند یعنی $\mathrm{x}=\frac{1}{2}$ بنابراین آنتروپی را به‌صورت زیر داریم:

$$H(\mathrm{x}) = -\mathrm{x}\log \mathrm{x} - (1-\mathrm{x})\log(1-\mathrm{x}) = 1 \qquad (۳۱-۲)$$

حالا فرض کنید $x=0.2$ و احتمال دیگری برابر با 0.8 باشد. در اینجا آنتروپی را به‌صورت زیر داریم:

$$H = -0.2\log 0.2 - 0.8\log 0.8 = 0.72$$

در اینجا دانش ما نسبت به سیستم بیشتر از حالت قبل است که در آنجا هر دو خروجی با احتمال برابر اتفاق افتاد. پس به ازای خروجی‌های باینری هر گاه دو خروجی با احتمال یکسان روی دهد داریم $H(x)=1$، و در غیر این‌صورت $0 \le H(x)<1$ [۱۸].

آنتروپی شانون بیانگر عدم قطعیت و میزان اطلاعاتی است که قبل از اندازه‌گیری از آن آگاه نیستیم، و مربوط به توزیع احتمال کلاسیکی است. درحوزه‌ی مکانیک کوانتمی آنتروپی فون‌نویمان را داریم، که در این آنتروپی اپراتورهای چگالی یک حالت کوانتمی، جایگزین احتمال کلاسیکی یک متغیر تصادفی شده‌اند. آنتروپی فون‌نویمان برای حالت کوانتمی ρ با رابطه زیر توصیف می‌شود:

$$S(\rho) = -tr(\rho \log \rho) \qquad (۳۲-۲)$$

این آنتروپی یک کمیت نامنفی است که این ویژگی از نتیجه تعریف آنتروپی فون‌نویمان نتیجه شده است ولی فقط برای حالت خالص برابر صفر است[۷].

۲-۸-۲ احتمالات شرطی، آنتروپی شرطی

اگر دو رویداد A وB اتفاق بیافتد و خروجی‌های آنها به‌ترتیب $\{a_i\}$ و $\{b_j\}$ باشند، آنگاه می‌توان $p(a_i)$ را احتمال بدست آوردن a_i و $p(b_j)$را احتمال بدست آوردن خروجی b_j دانست، و می‌دانیم که این توابع احتمال در رابطه $0 \le p(a_i) \le 1$ و $0 \le p(b_j) \le 1$ صدق می‌کنند. احتمالات $p(a_i)$ و $p(b_j)$ تمام اطلاعات مورد نیاز را در اختیار ما قرار نمی‌دهند بلکه توصیف کاملتر را احتمالات توام $p(a_i,b_j)$ نشان می‌دهند. که این احتمال برابر است با احتمال اینکه به ازای رویداد A خروجی a_i را و به ازای رویداد B خروجی b_j را بدست آوریم. چنانچه دو رویداد مستقل از یکدیگر باشند یعنی رویدادها غیر همبسته باشند احتمال توامان را به‌صورت زیر داریم:

$$p(a_i,b_j) = p(a_i)p(b_j) \qquad (۳۳-۲)$$

چنانچه بخواهیم می‌توانیم احتمالات مجزای هر رویداد را با استفاده از جمع بر روی احتمالات توامان طبق روابط زیر بدست آوریم:

$$\begin{aligned} p(a_i) &= \sum_j p(a_i,b_j) \\ p(b_j) &= \sum_i p(a_i,b_j) \end{aligned} \qquad (۳۴-۲)$$

فرض کنید با دانستن متغیر تصادفی $A = a_0$ احتمال توامان را به‌صورت $p(a_0,b_j)$ داریم می‌خواهیم نشان دهیم رابطه‌ی زیر برقرار است:

$$p(a_0,b_j) = p(b_j \mid a_0)p(a_0) \qquad (۳۵-۲)$$

احتمال شرطی $p(b_j \mid a_0)$ یعنی احتمال اینکه $B = b_j$ به شرط آنکه $A = a_0$ را داشته باشیم. فرض کنید احتمال شرطی $p(b_j \mid a_0)$ را به‌صورت زیر داریم:

$$p(b_j \mid a_0) = p(a_0, b_j) k(a_0) \qquad (۳۶-۲)$$

در ادامه مقدار $k(a_0)$ را با جمع معادله بالا روی مجموعه‌ای از خروجی‌های b_j بدست می‌آوریم:

(۳۷-۲)

$$\sum_j p(b_j \mid a_0) = \sum_j k(a_0) p(a_0, b_j) \Rightarrow 1 = k(a_0) \sum_j p(a_0, b_j) = k(a_0) p(a_0) \Rightarrow k(a_0) = [p(a_0)]^{-1}$$

احتمالات شرطی تنها برای دو رویداد نمی‌باشند این احتمالات را می‌توانیم برای سه رویداد هم داشته باشیم:

$$p(a_i, b_j, c_k) = p(a_i \mid b_j, c_k) p(b_j, c_k) = p(a_i \mid b_j, c_k) p(b_j \mid c_k) p(c_k) \qquad (۳۸-۲)$$

علاوه بر آنتروپی مربوطه به یک رویداد که در بخش قبلی معرفی شد می‌توانیم آنتروپی توامان را همانند احتمالات توامان داشته باشیم. در واقع آنتروپی توامان میزان اطلاعاتی است که از وقوع دو پیشامد کسب می‌کنیم بنابراین آنتروپی توامان برای یک جفت متغیر تصادفی A و B را به‌صورت زیر تعریف می‌کنیم:

$$H(A,B) = -\sum_{i,j} p(a_i, b_j) \log p(a_i, b_j) \qquad (۳۹-۲)$$

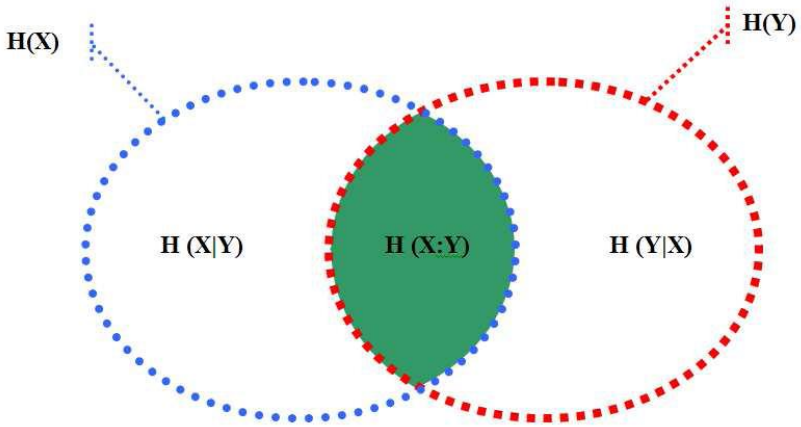
آنتروپی شرطی را نیز می‌توانیم به شکل $H(B \mid A)$ معرفی کنیم که بیانگر میزان ناآگاهی ما از مقدار B است وقتی که ما میزان A را می‌دانیم. به عبارتی آنتروپی شرطی، اطلاعات باقیمانده را مشخص می‌کند. در پایان ارتباط میان آنتروپی شرطی و آنتروپی توامان را با رابطه‌ای بیان می‌کنیم[۵]:

$$H(A,B) = H(B \mid A) + H(A) \qquad (۴۰-۲)$$

اثبات:

$$H(B|A)=\sum_i p(a_i)H(B|a_i)=-\sum_i p(a_i)\sum_j p(b_j|a_i)\log p(b_j|a_i)=-\sum_{i,j} p(b_j,a_i)\log p(b_j|a_i)=$$

$$-\sum_{i,j} p(b_j,a_i)\log\frac{p(a_i,b_j)}{p(a_i)}=-\sum_{i,j} p(a_i,b_j)\log p(a_i,b_j)+\sum_j p(a_i,b_j)\log p(a_i)=H(A,B)-H(A)$$



شکل (۲-۴): نمودار ون برای نمایش آنتروپی و ارتباط میان آنها

فصل سوم

وجود کاتورگی ذاتی در سیستم‌های کوانتمی

مقدمه

امروزه اعداد تصادفی اغلب برای کاربرد در رمزنگاری مورد استفاده قرار می‌گیرند. یکی از پارامترهای مهم در سیستم‌های رمزنگاری، امنیت است. امنیت بستگی به این دارد که مقادیر بعدی قابل پیش‌بینی نباشند. لذا به دنبال روشی هستیم تا امنیت را در این سیستم‌ها بالا ببریم .بنابراین از فیزیک کوانتمی استفاده می‌کنیم. زیرا چنان‌چه اثبات می‌کنیم کاتورگی مطرح شده در فیزیک کوانتمی کاتورگی ذاتی است و مانند سیستم‌های کلاسیک قابل بر طرف کردن نیست، و در واقع ناشی شده از نقص سیستم یا کمبود اطلاعات نمی‌باشد. بنابراین اعداد تصادفی تولید شده توسط سیستم‌های کوانتمی اعداد غیر قابل پیش بینی می‌باشند. بنابراین امنیت لازمه را به وجود می‌آورند.

هدف در این فصل این است که وجود متغیرهای پنهان را رد کنیم. در واقع رد این متغیرهای پنهان وجود کاتورگی ذاتی مطرح شده در مکانیک کوانتمی را اثبات می‌کند[۹]. در ادامه نیز میزان این کاتورگی را در سیستم‌های کوانتمی محاسبه می‌کنیم و انواع آن را بررسی می‌کنیم.

۳-۱ تولید اعداد تصادفی

تولید اعداد تصادفی[۲۴] یک موضوع مهم در کاربردهای مختلف می‌باشد. این کاربردها دارای تنوع وسیعی هستند. مانند رمزنگاری کوانتمی شبیه‌سازی مونت‌کارلو، الگوریتم‌های ژنتیک، مدلسازی سیستم‌ها و شبیه‌سازی‌های عددی. امروزه اعداد تصادفی اغلب برای کاربرد در رمزنگاری مورد استفاده قرار می‌گیرند.

الگوریتم تولید اعداد تصادفی به دو دسته تقسیم می‌شود. یکی تولید اعداد شبه‌تصادفی به روش الگوریتمی و دیگری تولید اعداد کاملا تصادفی است که به روش فیزیک کوانتمی انجام می‌گیرد. انتخاب روش تولید اعداد تصادفی برای یک کاربرد خاص بستگی به نیازهای آن سیستم به افزایش سرعت و کیفیت یا کاهش حجم تولید کننده دارد. در سیستم‌های رمزنگاری، امنیت بستگی به این دارد که مقادیر بعدی قابل پیش‌بینی نباشند.

تولید اعداد شبه‌تصادفی دارای یک مشکل جدی است و آن این است که دارای یک الگوریتم تولید قطعی و ثابت می‌باشند که این قطعیت به‌خاطر سیستم کلاسیک آنهاست. در این سیستم‌ها چنانچه جاسوس بتواند به برخی از اطلاعات سیستم رمزنگاری دسترسی پیدا کند، دنباله اعداد تولید شده توسط این افراد قابل شناسایی است. در رمزنگاری به روشی نیاز است که حتی اگر جاسوس, توانایی فوق‌العاده‌ای برای انجام محاسبات داشته باشد، و نیز تمام اطلاعات رشته را بدست آورد، قابلیت پیش‌بینی عدد بعدی را نداشته باشد. چنین رشته‌ای، دنباله‌ی اعداد تصادفی واقعی خوانده می‌شود.

مشکل دیگری که وجود دارد این است که تولید این دسته اعداد تصادفی که گاه مبتنی بر نرم‌افزار است، دارای الگوریتم پیچیده‌ای می‌باشند. این مولدها بدون در نظر گرفتن سرعت، در جهت

[24] Random number generators

افزایش پیچیدگی الگوریتم‌های مولد پیش می‌روند. برای پیاده‌سازی الگوریتم‌های تصادفی توسط سیستم‌های کلاسیک باید بخش مستقلی را برای روند کاتوره‌ای در نظر گرفت لذا این امر سرعت تولید این اعداد راکاهش می‌دهد. عملا تولید اعداد تصادفی یکی از مشکلات پروتکل‌های تصادفی محسوب می‌شود.

لذا به دنبال روشی هستیم تا اعدادتصادفی را با بهترین کیفیت تولید کنیم. بهترین روش این است که از فیزیک کوانتمی استفاده می‌کنیم. چنانچه اثبات می‌کنیم کاتورگی مطرح شده در فیزیک کوانتمی کاتورگی ذاتی است که به هیچ وجه قابل حذف کردن نیست. بنابراین اعداد تصادفی تولید شده توسط سیستم‌های کوانتمی اعداد غیر قابل پیش بینی می‌باشند.

۳-۳ تمایز میان کاتورگی مطرح شده در فیزیک کوانتمی با فیزیک کلاسیک

به دلیل اینکه در فیزیک نیوتن می‌توان دانش کاملی نسبت به سیستم پیدا کرد لذا در فیزیک کلاسیک نتیجه‌ی آزمایش قطعی است. کاتورگی که در فیزیک کلاسیک مطرح است کاتورگی است که ناشی از نقض اطلاعات می‌باشد. می‌خواهیم بررسی کنیم آیا کاتورگی مطرح شده در فیزیک کوانتمی نیز ناشی از نقض اطلاعات می‌باشد[۱۰].

چنان که می‌دانیم اینشتین به دلیل علاقه و اعتقاد عمیقی که به نظریه فیزیکی به عنوان توصیف کننده جهان خارج داشت، یعنی جهانی واقعی که مستقل از مشاهدات و تصورات ما وجود عینی دارد هرگز نتوانست مکانیک کوانتومی را به عنوان یک نظریه فیزیکی کامل بپذیرد. منظور از کامل بودن این است که هر عنصری از واقعیت در آن قابل توصیف باشد. ملاک واقعی بودن یک خاصیت را نیز می‌توان چنین توضیح داد که فرض کنید می‌خواهیم خصلتی مثل رنگ یک سیب را تعیین کنیم. اگر کسی

بتواند بدون اینکه مطلقا روی اندازه‌گیری ما تاثیری بگذارد، پیش‌گویی کند که ما حتما رنگ سیب را سرخ بدست خواهیم آورد و پیش‌بینی‌اش درست از آب درآید، حتما رنگ سرخ سیب یک واقعیت خارجی و مستقل از اندازه‌گیری ماست. به عبارت دیگر اندازه‌گیری ما سرخی سیب را (خلق) نکرده است بلکه فقط آن را که یک واقعیت خارجی بوده است آشکارکرده است. برای آنکه مطمئن شویم که شخص دوم هیچ گونه تاثیری روی اندازه‌گیری ما نداشته است ما می توانیم رابطه علّی اندازه‌گیری خودمان را با او به‌کلی قطع کنیم، یعنی کاری کنیم که اندازه‌گیری ما و عمل آن شخص در فاصله‌های فضاگونه انجام شود.

فیزیک کلاسیک مبتنی بر این خاصیت بود که آزمایش‌های یکسان نتایج یکسان دارند و فرض می‌شد که این خاصیت علی الاصول درسطح تک تک رویدادها و ذرات وجود دارد. اما مکانیک کوانتومی به ما می‌گوید که نتایج آزمایش‌های یکسان بر ذرات یکسان یقینی نیستند بلکه تصادفی و تابع شانس و احتمال‌اند و این تصادفی بودن در ذات خود پدیده‌ها نهفته است و با ظریف و دقیق کردن هر چه بیشتر ابزار آزمایش و روش‌های تهیه ذرات از بین نمی‌رود.

اما شاید متغیرهای بسیار ظریف و پنهانی وجود داشته باشند که عدم اطلاع و کنترل ما بر آنها و در نتیجه پراکنده بودن آنها در آزمایش‌های گوناگون این تصور کاذب را در ما بوجود می‌آورد که ما واقعا آزمایش‌های یکسان را بر ذرات یکسان انجام می‌دهیم و نتایج متفاوت را ناگزیر به شانس و احتمال نسبت می‌دهیم. اگر بر این متغیرها آگاهی داشته باشیم ممکن است بتوانیم یک توصیف یقینی از پدیده‌ها ارائه کنیم. این ایده‌ای بسیار جذاب برای رها شدن از شانس و تصادف و بازگشت به چارچوب فیزیک کلاسیک است که در آن می توان با داشتن شرایط اولیه به طور دقیق آینده جهان را به طور کامل پیش‌گویی کرد. آیا واقعا این کار امکان پذیراست؟ آیا متغیرهای پنهان وجود دارند؟ و می‌توان لااقل وجود آنها را فرض کرد و نتایج تصادفی‌ای را که در آزمایش‌های میکروسکوپی در نظر می‌گیریم به کمک فرض وجود آنها توضیح داد؟ باید دقت کنیم که در این‌جا به نوع و میزان ظرافت و

کوچکی این پارامترها کاری نداریم و فقط به امکان وجود آنها فکر می‌کنیم. در واقع اگر بتوانیم به این سوال پاسخ درست بدهیم می‌توانیم بگوییم که کاتورگی مطرح شده در مکانیک کوانتمی ذاتی است یا مانند کاتورگی کلاسیک بر طرف کردنی است[۹]. در واقع آن‌چه در بخش بعدی بررسی می‌کنیم نوع کاتورگی مطرح شده در سیستم‌های کوانتمی است.

کار مهم جان بل در ۱۹۶۳ آن بود که راه دقیقی برای پاسخگویی به مسئله پارامترهای پنهان پیدا کرد، راهی که به کمک آن می‌توان به طور تجربی تعیین کرد که آیا این پارامترها وجود دارند یا نه؟ یا به عبارت بهتر آیا نتایج تجربی آزمایشگاهی‌ای را که ما می‌بینیم و آنها را به شانس و تصادف تعبیر می‌کنیم، می‌توانیم با پارامترهای پنهان توضیح دهیم یا خیر؟

از سال ۱۹۸۲ تا کنون آزمایش‌های گوناگونی با فوتون‌ها انجام شده است که همگی نشان دهنده این هستند که نامساوی بل توسط طبیعت نقض می‌شود. این امر به این معناست که رفتار تصادفی‌ای را که اشیای میکروسکوپی از خود نشان می‌دهند نمی‌توان با یک نظریه موضعی که قائل به خواص واقعی اشیا و متغیرهای نهان باشد توضیح داد. آیا نتایج مکانیک کوانتومی با آزمایش‌های فوق سازگار است؟ پاسخ این سوال مثبت است. مکانیک کوانتومی نشان می‌دهد که اولا نامساوی بل که بر اساس موضعیت و واقعیت خارجی بنا نهاده شده نقض می‌شود، ثانیا مقداری که برای کمیت طرف چپ نامساوی بل پیش‌گویی می‌کند درست همانی است که در آزمایشگاه مشاهده می‌شود. در واقع هیچ نظریه متغیرهای پنهان و موضعی که قائل به مقادیر واقعی برای اسپین‌ها باشد قادر نیست این همبستگی‌های کوانتمی را توضیح دهد [۹].

می‌توان گفت سیستم‌های کوانتمی به‌صورت ذاتی تصادفی هستند و این کاتورگی ذاتی با کاتورگی کلاسیک متفاوت است. برای نشان دادن بیشتر این تمایز میان کاتورگی مطرح شده در فیزیک کوانتمی و فیزیک کلاسیک مثالی را مطرح می‌کنیم. فرض کنید ذره‌ای در درون یک جعبه قرار دارد. در یک لحظه توسط یک مانع جعبه را به دو قسمت تقسیم می‌کنیم. سپس هر دو بخش را

به اندازه کافی از هم دور می‌کنیم. طبق توصیف مکانیک کوانتمی ذره در هر دو بخش جعبه احتمال حضور دارد. حال اگر در جعبه را باز کنیم و ذره را در آن بیابیم، در همان لحظه احتمال حضور در جعبه دیگر (که به اندازه کافی از آن دور است) صفر خواهد شد و با توجه به این‌که دو جعبه را می‌توان به اندازه دلخواه از هم دور کرد. می‌توان گفت که این اثر، یک اثر ناموضعی است. شاید بیان شود اینکه احتمال حضور در یکی از جعبه‌ها پس از یافتن ذره در جعبه دیگر صفر می‌شود چیز عجیبی نیست و این چیزی است که در دنیای کلاسیک هم مشاهده می‌شود. و مختص مکانیک کوانتمی نیست. در جواب به این سوال باید گفت که تفاوت در آن‌جاست که در دنیای کلاسیک، احتمالات را ناشی از جهل خودمان نسبت به موضوع تعبیر می‌کنیم. یعنی قائل به این هستیم که ذره در یکی از جعبه‌ها هست و در دیگری نیست (حتی قبل از مشاهده درون جعبه‌ها) و مشاهده یک جعبه و یافتن ذره در آن صرفا یک عمل آشکارسازی است یعنی چیزی که از قبل بوده مشاهده کردیم. ولی در مکانیک کوانتمی احتمالات را ناشی از جهل نسبت به سیستم مورد بررسی نمی‌دانیم، یعنی در تعبیر رایج مکانیک کوانتمی احتمالات را ذاتی پدیده‌های کوانتمی می‌دانیم.

بنابر مکانیک کوانتومی، یک خصلت معین از یک ذره، از قبل یک مقدار مشخص ندارد که توسط عمل اندازه‌گیری مشاهده یا آشکار شود، بلکه عمل اندازه‌گیری یکی از مقادیر کمیت مشاهده‌پذیر را خلق می‌کند. هرگاه که قائل به وجود چنین کمیتی به عنوان کمیتی واقعی و از قبل موجود شویم به تناقض‌های آشکاری با آزمایش‌ها مواجه خواهیم شد. به‌عنوان مثال مولفه اسپین یک ذره در یک راستای معین، قبل از اندازه‌گیری مقدار معینی ندارد و نمی توان از مقدار واقعی آن قبل از اندازه‌گیری سخن گفت. می‌دانیم که نتایج اندازه‌گیری مولفه‌های اسپین یک ذره‌ی اسپین $\frac{1}{2}$ در هر راستایی همیشه دو مقدار $\frac{\hbar}{2}$ و $-\frac{\hbar}{2}$ را بدست می‌دهد، در صورتی که نمی‌توان برداری را تصور کرد که مولفه های آن در هر راستایی تنها همین دو مقدار را اختیار کند. در واقع وقتی که هیچ راه عملی برای

محک زدن یک خصلت واقعی مستقل از مشاهده وجود ندارد، بهتر است از اصرار براینکه آن خصلت واقعی و مستقل از مشاهده است دست برداریم.

آن‌چه تا اینجا بیان کردیم این است که کاتورگی مطرح شده در فیزیک کلاسیک و فیزیک کوانتمی متفاوت است. بنابراین می‌توان گفت سیستم‌های کوانتمی به‌صورت ذاتی کاتوره‌ای هستند و این کاتورگی ذاتی همتای کلاسیکی ندارد. بنابراین برای استفاده در الگوریتم‌های تصادفی بسیار مناسب می‌باشند. همانطور که گفتیم رد متغیرهای پنهان وجود کاتورگی ذاتی را اثبات می‌کند. بنابراین در بخش بعدی به رد متغیرهای پنهان در سیستم‌های درهم‌تنیده می‌پردازیم.

۳-۴ رد متغیرهای پنهان اثباتی بر کاتورگی ذاتی[۲۵]

ناموضعیت در همبستگی‌های EPR به‌وسیله‌ی احتمالات کوانتمی مشروط و توام نشان داده می‌شود. این احتمالات به‌دلیل ناموضعیت نامساوی بل را نقض می‌کنند. در اینجا می‌خواهیم دو مطلب را در پیش بگیریم یکی اینکه اثبات کنیم کاتورگی که در اینجا مطرح می‌کنیم از کاتوره‌ای منطبق بر واقعیت گرایی موضعی متفاوت می‌باشد، و دیگر اینکه ارتباط میان کاتورگی ذاتی و ناموضعیت را بیان کنیم که البته به این مبحث بیشتر در فصل بعدی پرداخته می‌شود.

[25] Intrinsic randomness

۳-۴-۱ همبستگی‌های EPR

خاصیت ناموضعیت در مکانیک کوانتمی درست در مقابل واقع‌گرایی موضعی قرار گرفته است. این ناموضعیت در هم‌بستگی‌های EPR برای $S=\frac{1}{2}$ به خوبی نشان داده شده است. به ازای S بزرگ این همبستگی‌ها به همبستگی‌های کلاسیکی تبدیل می‌شوند. می‌توان از همبستگی‌های ناموضع EPR برای نشان دادن اعداد کاملا تصادفی که متشکل از خروجی‌های 0 و 1 می‌باشند استفاده کرد در واقع می‌توان مقادیر 0 و 1 را ویژه‌مقادیر عملگرهای اعمالی مربوط به اسپین دانست. احتمال این خروجی‌ها همان احتمالات توام ناموضع هستند که نامساوی‌های بل را نقض می‌کنند، زیرا که نامساوی‌های بل منطبق بر واقعیت گرایی موضعی می‌باشند. ارتباط میان ناموضعیت و کاتورگی با استفاده از آنتروپی شانون نشان داده شده است.

دو ذره‌ی درهم‌تنیده EPR داریم که هر کدام دارای اسپین دلخواه S می‌باشند و حالت کلی سیستم به فرم کلی زیر نوشته می‌شود:

$$|\psi_{EPR}\rangle=\sum_{m=-s}^{s}\frac{(-1)^{s+m}}{\sqrt{2S+1}}|m,-m\rangle \qquad (۱-۳)$$

(توجه داشته باشید که چون حالت کلی سیستم تعمیمی از حالت درهم‌تنیده یگانه می‌باشد بنابراین m یکی از ذره‌ها مخالف m ذره دیگر است).

فرض کنید طرفین آلیس و باب را داریم که هر کدام دارای یک ذره می‌باشند. احتمال توامان ناموضع در چارچوب نظریه کوانتمی برای اینکه ذره‌ی آلیس با اعمال اندازه‌گیری بر روی ذره خود مقدار a را بدست آورد و سیستم باب با اعمال اندازه‌گیری بر روی ذره خود مقدار b را بدست آورد مقدار زیر می‌شود:

$$p(\vec{a},\vec{b})=\langle\psi_{EPR}|\hat{P}(\vec{a})\otimes\hat{P}(\vec{b})|\psi_{EPR}\rangle \qquad (۲-۳)$$

$\hat{P}(\vec{a}),\hat{P}(\vec{b})$ عملگرهای تصویرند که نوعی عملگر اندازه‌گیری می‌باشند. برای مثال عملگر تصویر مربوطه درجهت قطبش $\vec{a}$ را با $\hat{P}(\vec{a})=|a\rangle\langle a|$ نشان می‌دهیم. اگر سیستم‌ها را به‌صورت موضعی درنظر بگیریم با استفاده از متغیرهای پنهان احتمال توام را در چارچوب نظریه واقعیت‌گرایی موضعی به‌صورت زیر داریم:

$$p(\vec{a},\vec{b})=\int d\lambda_a \int d\lambda_b P(\lambda_a,\lambda_b)t(\vec{a},\lambda_a)t(\vec{b},\lambda_b) \qquad (۳-۳)$$

λ_a و λ_b به‌ترتیب متغیرهای پنهان موضعی مربوط به ذره‌ی آلیس و ذره‌ی باب می‌باشند. $t(\vec{a},\lambda_a)$ و $t(\vec{b},\lambda_b)$ توابع انتقال[۲۶] نرمال می‌باشند در واقع خروجی یک دستگاه اندازه‌گیری اسپین به واسطه‌ی اندازه‌گیری بوسیله‌ی تابع انتقال نرمال مشخص می‌شود که این توابع منطبق بر واقعیت گرایی موضعی می‌باشند:

$$0\le t(\vec{a},\lambda_a)\le 1 \qquad ، \qquad 0\le t(\vec{b},\lambda_b)\le 1$$

در نظریه واقعیت گرایی موضعی از آنجا که به اسپین یک واقعیت عینی می‌دهند که قبل از آزمایش وجود دارد لذا این توابع انتقال با σ به عنوان یک واقعیت عینی به‌صورت زیر رابطه دارند (که σ نیز با λ و جهت قطبش رابطه دارد و داریم $\sigma(\vec{a},\lambda_a)=\pm 1$)[۱۱]:

$$t(\vec{a},\lambda_a)=\frac{1}{2}(1+\sigma(\vec{a},\lambda_a)) \qquad (۴-۳)$$

در اینجا بنا بر فرض اینشتین به ازای مقادیر متفاوت λ، توابع انتقال متفاوت بدست می‌آید. λها نیز با یک تابع توزیع مثبت و نرمال شده‌ی زیر توزیع شده‌اند:

$$\int d\lambda_a \int d\lambda_b P(\lambda_a,\lambda_b)=1 \qquad P(\lambda_a,\lambda_b)\ge 1 \qquad (۵-۳)$$

[26] Transmission functions

تابع توزیع $P(\lambda_a,\lambda_b)$ یک تابع موضعی می‌باشد. زیرا مستقل از جهت قطبش $\vec{a}$ یا $\vec{b}$ می‌باشد. سیستم آلیس دارای دو عملگر $\vec{a}'$ و $\vec{a}$ می‌باشد و سیستم باب هم دارای دو جهت قطبش $\vec{b}$ و $\vec{b}'$ است. احتمالات توامان موضعی (۳-۳) در نامساوی بل زیر صادق می‌باشند:

$$-1\le p(\vec{a},\vec{b})+p(\vec{a},\vec{b}')-p(\vec{a}',\vec{b})+p(\vec{a}',\vec{b}')-p(\vec{a})-p(\vec{b})\le 0 \qquad (۶-۳)$$

این نامساوی CH اگرچه برای اسپین $\frac{1}{2}$ بدست آمده ولی برای تمام اسپینهای دیگر نیز صادق می‌باشد. در ادامه در رابطه (۳-۲) که رابطه احتمال توامان ناموضع می‌باشد λ را وارد می‌کنیم. برای این کار از تجزیه‌ی طیفی عملگر تصویر اسپین بر حسب λ استفاده می‌کنیم:

$$\hat{P}=\int \lambda\delta(\lambda-\hat{P})d\lambda \qquad (۷-۳)$$

این رابطه را در رابطه (۳-۲)جای می‌دهیم : [۱۱]

$$p(\vec{a},\vec{b})=\langle\psi_{EPR}|\hat{P}(\vec{a})\otimes\hat{P}(\vec{b})|\psi_{EPR}\rangle=\langle\psi_{EPR}|\int\lambda_a\delta(\lambda-\hat{P}(a))d\lambda_a\otimes\int\lambda_b\delta(\lambda-\hat{P}(b))d\lambda_b|\psi_{EPR}\rangle$$

$$=\int d\lambda_a\int d\lambda_b\,\langle\psi_{EPR}|\delta(\lambda-\hat{P}(a))\otimes\delta(\lambda-\hat{P}(b))|\psi_{EPR}\rangle\lambda_a\lambda_b$$

و با جایگزینی رابطه زیر در مقدار بالا:

$$p(\vec{a}\lambda_a,\vec{b}\lambda_b)=\langle\psi_{EPR}|\delta(\lambda-\hat{P}(a))\otimes\delta(\lambda-\hat{P}(b))|\psi_{EPR}\rangle \qquad (۸-۳)$$

به رابطه احتمال توامان ناموضع به فرم زیر می‌رسیم:

$$p(\vec{a},\vec{b})=\int d\lambda_a\int d\lambda_b P(\vec{a}\lambda_a,\vec{b}\lambda_b)\lambda_a\lambda_b \qquad (۹-۳)$$

چنانچه این رابطه را با رابطه (۳-۳) مربوط به احتمال توامان موضعی مقایسه کنیم علی رقم شباهت‌های بسیار به موارد زیر می‌رسیم:

$$\begin{cases} t(\vec{a},\lambda_a)\to\lambda_a \\ t(\vec{b},\lambda_b)\to\lambda_b \\ P(\lambda_a,\lambda_b)\to P(\vec{a}\lambda_a,\vec{b}\lambda_b) \end{cases} \qquad (۱۰-۳)$$

در اینجا مشاهده می‌کنیم که تابع توزیع موضعی $P(\lambda_a,\lambda_b)$، به یک تابع توزیع ناموضعی $P(\vec{a}\lambda_a,\vec{b}\lambda_b)$ تبدیل شده است. این تابع توزیع ناموضع وابسته به جهت $\vec{a}$ در اولین قطبش و به جهت $\vec{b}$ در دومین قطبش می‌باشد. ناموضعیت این تابع توزیع سبب نقض نامساوی CH می‌شود. پس در اینجا یک تابع توزیع احتمال ناموضع داریم که ارتباط ناموضع میان آلیس و باب را نشان می‌دهد. و در واقع نقض نامساوی بل توسط این احتمالات توام، رد متغیرهای پنهان را نشان می‌دهد. با استفاده از آنالیز بایاسی می‌توانیم ازتابع توزیع احتمال ناموضع به تابع توزیع احتمال شرطی برسیم [۱۲]:

$$P(\vec{a}\lambda_a,\vec{b}\lambda_b)=P(\vec{a}\lambda_a\,|\,\vec{b}\lambda_b)P(\vec{b}\lambda_b) \qquad (۱۱-۳)$$

در واقع احتمال شرطی $P(\vec{a}\lambda_a\,|\,\vec{b}\lambda_b)$ یعنی احتمال پیدا کردن λ_a تحت این شرط که قبلا باب با اعمال اندازه‌گیری بر روی ذره‌ی خود مقدار λ_b را بدست آورده باشد. اگر حالت کلی سیستم یعنی رابطه (۳-۱) را به‌صورت زیر باز کنیم:

$$|\psi_{EPR}\rangle=\frac{1}{\sqrt{2S+1}}[(-1)^0|-S,+S\rangle+(-1)^{+1}|-S+1,S-1\rangle+\ldots+(-1)^S|0,0\rangle+\ldots+ (-1)^{S+S-1}|S-1,-S+1\rangle+(-1)^{2S}|S,-S\rangle] \qquad (۱۲-۳)$$

احتمال اینکه ما مقدار بلی را بدست می‌آوریم یعنی $P(1)$، برابر با زمانی است که $\lambda=1$ بدست آید، یعنی زمانی که به ازای یک S دلخواه، یکی از حالات برگزیده شود. پس تنها باید احتمال بدست آوردن یکی از مقادیر بالا را بدست آوریم و چون حالت کلی سیستم به فرم $|\psi\rangle=\sum u_i|\alpha\rangle$ می‌باشد. بنابراین احتمال بدست آوردن یکی از حالات برای مثال بدست آوردن $|0,0\rangle$ در واقع همان احتمال

بدست آوردن $P(1)$ می‌شود. بنابراین مقدار $P(1)$، $\frac{1}{2S+1}$ می‌شود که توان دوم ضریب $|0,0\rangle$ می‌باشد. و احتمال بدست آوردن مابقی حالات که برابر با احتمال بدست آوردن $\lambda=0$ می‌باشد از این اصل بدست می‌آید که می‌دانیم مجموع احتمالات ۱ می‌شود. بنابراین احتمال اینکه $|0,0\rangle$ را بدست نیاوریم و یا به بیان دیگر احتمال اینکه $\lambda=0$ باشد و در واقع جواب خیر را بدست بیاوریم طبق فرآیند زیر بدست می‌آید:

$$P(0)+P(1)=1\Rightarrow P(0)=1-P(1)\Rightarrow P(0)=\frac{2S}{2S+1} \qquad (۱۳-۳)$$

این احتمالات مستقل از جهت قطبش می‌باشند و در روابط مربوطه به آنها اصلا زاویه وجود ندارد. در واقع روابط زیر احتمالات موضعی می‌باشند:

$$\begin{aligned} P(0)&=\frac{2S}{2S+1}\\ P(1)&=\frac{1}{2S+1}\end{aligned} \qquad (۱۴-۳)$$

احتمالات شرطی را به فرم کلی زیر خواهیم داشت:

$$P(\lambda_a\,|\,\lambda_b)=\begin{bmatrix} P(0|0)P(0|1)\\ P(1|0)\;P(1|1)\end{bmatrix} \qquad (۱۵-۳)$$

برای احتمالات شرطی با S دلخواه روابط زیر را داریم:

$$\begin{aligned} P(0\,|\,0)&=\frac{1}{2S}(2S-1+(\sin\frac{\phi}{2})^{4s})\\ P(0\,|\,1)&=1-(\sin\frac{\phi}{2})^{4s}\end{aligned} \qquad (۱۶-۳)$$

در اینجا α زاویه میان دو بردار $\vec{a}$ و $\vec{b}$ می‌باشد ($\cos\phi=\vec{a}\vec{b}$). روابط بهنجارش را برای این احتمالات شرطی داریم:

$$P(0|0)+P(1|0)=1$$
$$P(0|1)+P(1|1)=1 \qquad (۱۷-۳)$$

برای هر قطبش به صورت موضعی خروجی‌ها کاملا کاتوره‌ای‌اند. همبستگی‌های EPR سبب می‌شوند که این خروجی‌های کاملا کاتوره‌ای با هم مرتبط شوند. این ارتباط را با همان احتمالات شرطی نشان می‌دهیم. پس احتمال بدست آوردن خروجی آلیس به نتیجه‌ی خروجی باب وابسته است. و این همان ناموضع بودن می‌باشد. ما در فرستادن اطلاعات از سیگنال‌ها استفاده می‌کنیم. هر سیگنال، تکراری از حروف تصادفی 0 و 1 است. حال چون زوج EPR داریم بنابراین دو طرف A و B داریم که هر کدام سیگنال تصادفی مربوطه به خود را ارسال می‌کند که برای مثال این سیگنال‌ها را با توابع انتقال زیر نشان می‌دهیم:

$$t(\vec{a},\lambda_a)=011001010001....$$
$$t(\vec{b},\lambda_b)=100100111001.... \qquad (۱۸-۳)$$

همبستگی‌های درهم‌تنیده‌ی EPR به‌عنوان یک همبستگی ناموضع میان توالی‌های دوتایی اعداد بالا نمایش داده می‌شوند. ناموضعیت اینها بدان معناست که برای مثال هرگاه $t(\vec{b},\lambda_b)=1$ باشد یعنی اگر ما مقدار 1 را در جهت قطبش b بدست آوریم بایستی $t(\vec{a},\lambda_a)=0$ و یا $t(\vec{a},\lambda_a)=1$ را در جهت قطبش a به‌ترتیب با احتمالات $P(1|1)$ و $P(0|1)$ داشته باشیم. این احتمالات شرطی نشان می‌دهند که احتمال خروجی‌های a به‌وسیله‌ی خروجی‌های b مشخص می‌شود، لذا این سیگنال‌ها رابطه‌ی ناموضع دارند به جز در سه مورد زیر که به آنها همبستگی‌های کامل[۲۷] می‌گوییم:

(۱) وقتی $\phi=0$ باشد، یعنی جهت قطبش $\vec{a}$ و $\vec{b}$ یکسان است. آن‌گاه تابع توزیع را به‌صورت زیر داریم:

[27] Perfect correlations

$$P(\lambda_a \mid \lambda_b) = \begin{bmatrix} 01 \\ 10 \end{bmatrix} \qquad (۱۹-۳)$$

برای مثال اگر آلیس و باب هر کدام در جهت z اندازه‌گیری کنند و در واقع عملگر σ_z را بر روی سیستم خود اعمال کنند، چون زوج EPR داریم اگر آلیس 0 را بدست آورد قطعا باب مقدار 1 را بدست می‌آورد و همینطور بالعکس. سیگنال‌های مربوطه‌ی موضعی را به صورت زیر داریم:

$$t(\vec{a}, \lambda_a) = 011011010001....$$
$$t(\vec{b}, \lambda_b) = 100100101110....$$

(۲) وقتی عملگرهای $\vec{a}$ و $\vec{b}$ در خلاف جهت یکدیگر باشند. یعنی وقتی زاویه میان قطبش‌ها $\phi = 180$ می‌باشد. آن‌گاه تابع توزیع را به صورت زیر داریم:

$$P(\lambda_a \mid \lambda_b) = \begin{bmatrix} 10 \\ 01 \end{bmatrix} \qquad (۲۰-۳)$$

چنانچه در اینجا آلیس و باب در خلاف جهت یکدیگر اندازه‌گیری کنند، آنگاه دو سیگنال دقیقا مانند یکدیگر خواهند بود:

$$t(\vec{a}, \lambda_a) = 100100111001....$$
$$t(\vec{b}, \lambda_b) = 100100111001....$$

(۳) چنانچه $S \to \infty$ برود آن‌گاه داریم:

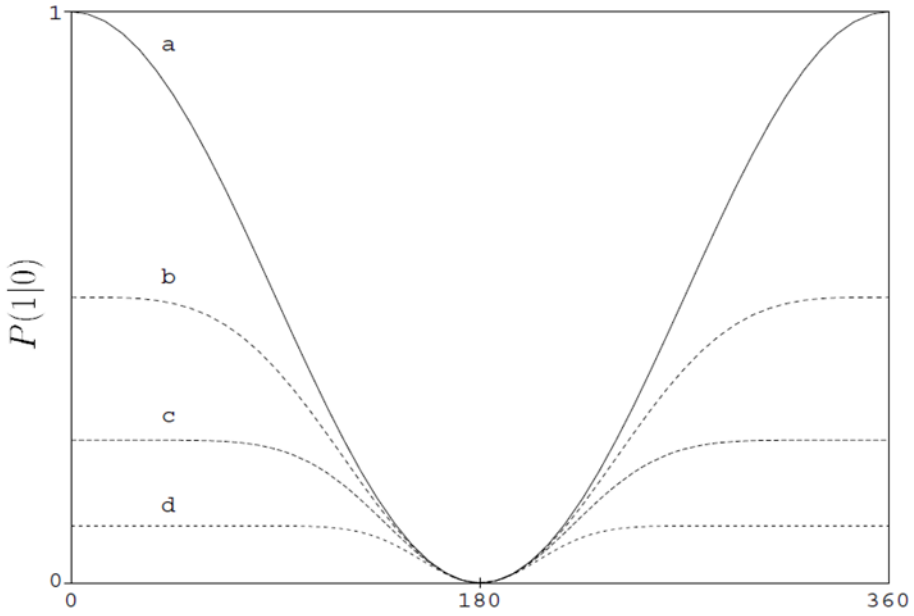
$$P(\lambda_a \mid \lambda_b) = \begin{bmatrix} 11 \\ 00 \end{bmatrix} \qquad ,\phi \neq \pi \qquad (۲۱-۳)$$

و تابع انتقال را به صورت زیر داریم:

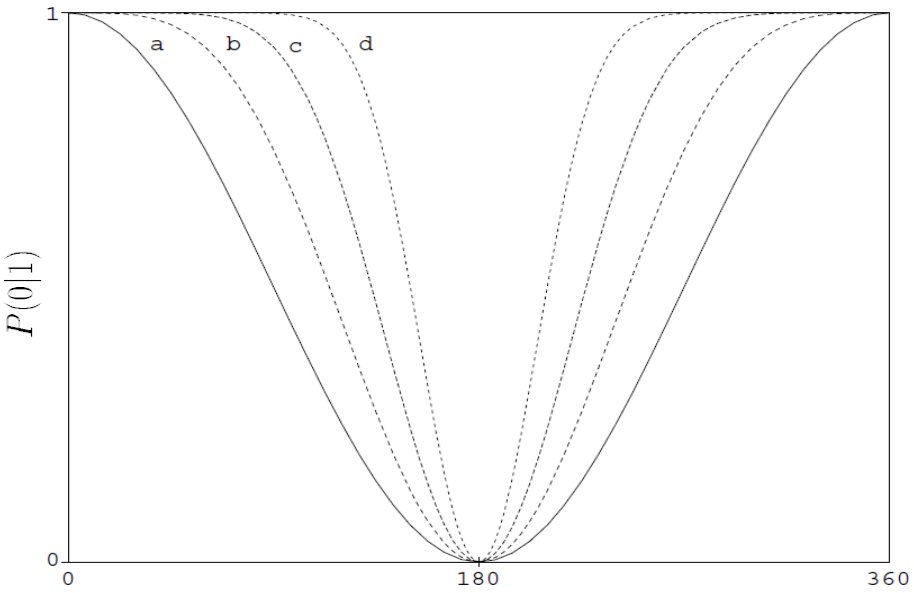
$$t(\vec{a}, \lambda_a) = 000000000000....$$
$$t(\vec{b}, \lambda_b) = 100100111001....$$

و رابطه بالا بدان معناست که اگر S به سمت بینهایت برود یکی از سیگنال‌ها به صورت مکرر یک مقدار را نشان می‌دهد. و هیچ ارتباطی با اینکه سیگنال دیگر چه ارسال می‌کند ندارد. یعنی در اینجا سیگنال باب هر چه باشد آلیس با احتمال صد درصد مقدار 0 را بدست می‌آورد. با استفاده از روابط (۳-۱۶) و (۳-۱۷) می‌توان مقدار $P(1|0)=\frac{1}{2S}(1-(\sin\frac{\phi}{2})^{4s})$ را بدست آورد. همانطور که از شکل‌های (۳-۱) و (۳-۲) برمی‌آید با افزایش مقدار اسپین مقادیر احتمالاتی ما به سمت قطعیت پیش می‌روند (البته توجه داشته باشید که به ازای زاویه‌ی $\phi=\pi$، برای هر مقداری از S ما این قطعیت را داریم).

آن‌چه تا اینجا نشان دادیم این بود که خروجی‌های همبستگی‌های EPR به‌عنوان همبستگی‌های ناموضع توالی‌های کاملا کاتوره‌ای از اعداد 0و 1 می‌باشند. توالی این اعداد کاتوره‌ای و همبستگی میان آنها اطلاعاتی را راجع به سیستم نشان می‌دهد. این دانش اطلاعات نامیده می‌شود و با آنتروپی شانون نشان داده می‌شود. در این همبستگی‌های EPR به ازای همبستگی‌های کامل انطباق کاملی میان نظریه متغیرهای پنهان و نظریه مکانیک کوانتمی برقرار است در حالی که این انطباق را برای همبستگی‌های کامل GHZ نمی‌بینیم. در واقع همبستگی‌های GHZ رد قوی‌تری برای متغیرهای پنهان موضعی می‌باشند. در ادامه آنتروپی سیستم را بدست می‌آوریم [۱۲].



شکل(۳-۱): توزیع شرطی $P(1|0)$ به‌عنوان تابعی از S برای مقادیر متفاوت اسپین (منحنی a به ازای اسپین $S=\frac{1}{2}$، منحنی b به ازای اسپین $S=1$، منحنی c به ازای اسپین $S=2$، منحنی d به ازای اسپین $S=5$)



شکل(۳-۲): توزیع شرطی $P(0|1)$ به‌عنوان تابعی از S برای مقادیر متفاوت اسپین (منحنی a به ازای اسپین $S=\frac{1}{2}$، منحنی b به ازای اسپین $S=1$ ، منحنی c به ازای اسپین $S=2$، منحنی d به ازای اسپین $S=5$)

۳-۴-۲ آنتروپی اطلاعات

توالی λ_a و λ_b با همبستگی میان آنها اطلاعاتی را راجع به سیستم در اختیار ما قرار می‌دهد. آنتروپی سیستم در واقع متوسطی از آن اطلاعات است که بدان می‌رسیم. آنتروپی اطلاعات را با رابطه زیر نشان می‌دهیم:

$$H(\vec{a},\vec{b}) = -\sum_{\lambda_a\lambda_b} p(\lambda_a\vec{a},\lambda_b\vec{b})\log_2 p(\lambda_a\vec{a},\lambda_b\vec{b}) \qquad (۲۲-۳)$$

آنتروپی‌های مرزی را نیز به‌صورت زیر تعریف می‌کنیم:

$$\begin{aligned} H(\vec{a}) &= -\sum_{\lambda_a} p(\lambda_a\vec{a})\log_2 p(\lambda_a\vec{a}) \\ H(\vec{b}) &= -\sum_{\lambda_b} p(\lambda_b\vec{b})\log_2 p(\lambda_b\vec{b}) \end{aligned} \qquad (۲۳-۳)$$

این آنتروپی توامان یعنی رابطه (۳-۲۲) در نامساوی بل AL[۲۸] به‌صورت زیر صدق می‌کند:

$$\left|H(\vec{a})-H(\vec{b})\right| \le H(\vec{a},\vec{b}) \le H(\vec{a})+H(\vec{b}) \qquad (۲۴-۳)$$

با استفاده از معادلات رابطه (۳-۱۴) مربوط به احتمالات موضعی می‌توانیم روابط (۳-۲۳) را به‌صورت زیر محاسبه کنیم[۱۲] :

$$H(\vec{a}) = H(\vec{b}) = -P(0)\log P(0) - P(1)\log P(1) \qquad (۲۵-۳)$$

$$= \frac{-2S}{(2S+1)}\log\frac{2S}{(2S+1)} - \frac{1}{(2S+1)}\log\frac{1}{(2S+1)} = \frac{-1}{2S+1}\log\frac{(2S)^{2S}}{(2S+1)^{2S+1}}$$

رابطه (۳-۲۴) با استفاده از رابطه(۳-۲۵) به‌صورت زیر تبدیل می‌شود:

[28] Araki and Lieb

$$0 \le H(\vec{a},\vec{b}) \le \frac{-2}{2S+1}\log\frac{(2S)^{2S}}{(2S+1)^{2S+1}} \qquad (۲۶-۳)$$

به ازای $S=\frac{1}{2}$ مقدار رابطه (۳-۲۵) یعنی مقدار آنتروپی موضعی به میزان یک بیت می‌شود. و مقادیر احتمالات موضعی برابر با مقدار $P(0)=P(1)=\frac{1}{2}$ می‌شود و میزان حداکثر سمت راست رابطه (۳-۲۶) دو بیت می‌شود ($\frac{-2}{2}\log\frac{1}{2^2}=-\log 2^{-2}=2$). و به ازای $S\to\infty$ مقدار آنتروپی موضعی صفر بیت می‌شود. و مقادیر احتمالات موضعی برابر با $P(0)=1$ و $P(1)=$ ۱ می‌شوند. و این بدین معناست که مقدار خروجی ۰ با قطعیت اتفاق می‌افتد. در واقع نتیجه‌ای که به آن رسیدیم این است که به ازای $S=\frac{1}{2}$ به میزان حداکثر آنتروپی توامان به میزان 2 بیت و میزان حداقل آنتروپی 0 بیت می‌رسیم. آنتروپی فون نویمان به ازای یک حالت خالص EPR مقدار 0 را به ما می‌دهد در حالی که به ازای آنسامبلی از حالات پس از اندازه‌گیری از آنتروپی شانون استفاده می‌کنیم و مقدار اطلاعات سیستم را بدست می‌آوریم.

۳-۴-۳ همبستگی‌های GHZ

این همبستگی دارای سه قسمت می‌باشد، برای مثال آلیس و باب و چارلی قسمتهای سیستم می‌باشند که هر کدام دارای یک ذره با اسپین $\frac{1}{2}$ هستند. یک فرم این همبستگی که به‌وسیله‌ی مرمین ارائه شد به‌صورت زیر است:

$$|\psi_{GHZ}\rangle=\frac{(|000\rangle-|111\rangle)}{\sqrt{2}} \qquad (۲۷-۳)$$

در ادامه احتمال توامان اینکه، در فرمالیزم مکانیک کوانتمی آلیس ذره‌ی خود را در جهت ϕ_1 اندازه بگیرد باب ذره‌ی خود را در جهت ϕ_2 اندازه بگیرد و چارلی ذره خود را در جهت ϕ_3 اندازه بگیرد برابر با مقدار زیر می‌باشد:

$$p(\phi) = p(\phi_1, \phi_2, \phi_3) = \langle \psi_{GHZ} | \hat{P}(\phi_1) \otimes \hat{P}(\phi_2) \otimes \hat{P}(\phi_3) | \psi_{GHZ} \rangle \qquad (۲۸-۳)$$

$$= \frac{1}{8}(1 - \cos(\phi_1, \phi_2, \phi_3)) = \frac{1}{8}(1 - \cos(\phi))$$

اثبات:

هر بردار قطبش در جهت بردار یکه‌ی $\hat{n}$ را با یک زاویه‌ی قطبی θ و یک زاویه سمتی ϕ توصیف می‌کنیم. بردار قطبش را به‌صورت زیر نمایش می‌دهیم:

$$|n_{\pm}\rangle = \cos\frac{\theta}{2}|0\rangle \pm e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

چنانچه این بردار قطبش را درصفحه x-y در نظر بگیریم زاویه قطبی برابر با $\theta = \frac{\pi}{2}$ خواهد بود بنابراین داریم:

$$|n_{\pm}\rangle = \frac{|0\rangle \pm e^{i\phi}|1\rangle}{\sqrt{2}}$$

عملگر تصویر نیز به صورت زیر بدست خواهد آمد:

$$\hat{P}(\phi) = |n_{+}\rangle\langle n_{+}| = \frac{1}{2}\begin{bmatrix} 1 & e^{-i\phi} \\ e^{i\phi} & 1 \end{bmatrix}$$

این عملگر را در رابطه (۳-۲۸) به کار می‌گیریم:

$$p(\phi) = \langle \psi_{GHZ} | \hat{P}(\phi_1) \otimes \hat{P}(\phi_2) \otimes \hat{P}(\phi_3) | \psi_{GHZ} \rangle =$$

$$\frac{1}{2}[1\,0\,0\,0\,0\,0\,0\,-1]\left[\frac{1}{2}\begin{bmatrix}1 & e^{-i\phi}\\ e^{i\phi} & 1\end{bmatrix}\otimes\frac{1}{2}\begin{bmatrix}1 & e^{-i\phi}\\ e^{i\phi} & 1\end{bmatrix}\otimes\frac{1}{2}\begin{bmatrix}1 & e^{-i\phi}\\ e^{i\phi} & 1\end{bmatrix}\right]\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\-1\end{bmatrix}=\frac{1}{8}(1-\cos(\phi))$$

توجه داشته باشید که در رابطه بالا مقدار $\phi=\phi_1+\phi_2+\phi_3$ را قرار داده‌ایم.

در ادامه رابطه $\hat{P}(\phi)=\int d\lambda\,\delta(\lambda-\hat{P})$ را جایگزین عملگرهای تصویر در رابطه (۳-۲۸) می‌کنیم و این رابطه با جایگزینی مقدار زیر:

$$P(\phi_1\lambda_a,\phi_2\lambda_b,\phi_3\lambda_c)=\langle\psi_{GHZ}\,|\,\delta(\lambda_a-\hat{P}(\phi_1))\otimes\delta(\lambda_b-\hat{P}(\phi_2))\otimes\delta(\lambda_c-\hat{P}(\phi_3))\,|\psi_{GHZ}\rangle \quad (۲۹-۳)$$

(این رابطه توزیع احتمال توامان ناموضع را نشان می‌دهد زیرا که این رابطه وابسته به زوایای عملگرها می‌باشد) به فرم رابطه زیر درمی‌آید که یک رابطه احتمال توامان ناموضع است:

$$p(\phi)_Q=\int d\lambda_a\int d\lambda_b\int d\lambda_c\;P(\phi_1\lambda_a,\phi_2\lambda_b,\phi_3\lambda_c)\,\lambda_a\,\lambda_b\,\lambda_c \quad (۳۰-۳)$$

علاوه بر آن احتمال توامان منطبق بر نظریه متغیرهای پنهان موضعی را نیز به‌صورت زیر داریم:

$$p(\phi)_{LHV}=\int d\lambda_a\int d\lambda_b\int d\lambda_c\;P(\lambda_a,\lambda_b,\lambda_c)\,t(\phi_1,\lambda_a)\,t(\phi_2,\lambda_b)\,t(\phi_3,\lambda_c) \quad (۳۱-۳)$$

رابطه بالا یک رابطه موضعی است زیرا که اصلا به جهت عملگرها بستگی ندارد. از مقایسه‌ی دو رابطه بالا یعنی رابطه (۳-۳۰) و (۳-۳۱) علی رقم شباهت‌های بسیار به موارد زیر می‌رسیم:

$$\begin{cases} t(\vec{a},\lambda_a)\to\lambda_a \\ t(\vec{b},\lambda_b)\to\lambda_b \\ t(\vec{c},\lambda_c)\to\lambda_c \\ P(\lambda_a,\lambda_b,\lambda_c)\to P(\vec{a}\lambda_a,\vec{b}\lambda_b,\vec{c}\lambda_c) \end{cases} \qquad (۳۲-۳)$$

توزیع احتمال $P(\lambda_a,\lambda_b,\lambda_c)$ یک توزیع احتمال موضعی است که به ازای آن نامساوی بل نقض نمی‌شود در حالی که به ازای توزیع احتمال ناموضع $P(\vec{a}\lambda_a,\vec{b}\lambda_b,\vec{c}\lambda_c)$ نامساوی بل نقض می‌گردد. این همبستگی‌های GHZ به ازای زوایای $\phi_1+\phi_2+\phi_3=0$ و $\phi_1+\phi_2+\phi_3=\pi$ موضعی می‌باشند و با قطعیت پیش‌بینی می‌شوند. به ازای این زوایا همبستگی‌های GHZ کامل‌اند یعنی با اندازه‌گیری دو اسپین، اسپین سوم را می‌توان با قطعیت پیش‌بینی کرد. در همبستگی EPR همان گونه که قبلا نشان دادیم همبستگی‌های کامل به ازای زوایای $\alpha=0$ و $\alpha=180$ و هم‌چنین به ازای زمانی که اسپین به سمت بینهایت می‌رود اتفاق می‌افتد. هم‌بستگی‌های کامل GHZ به ازای حالتی که $\phi_1+\phi_2+\phi_3=0$ باشد دیگر با نظریه متغیرهای پنهان تطابق ندارند و این عدم تطابق ادعای دیگری است که سبب رد نظریه‌ی متغیرهای پنهان می‌شود. در حالی که در هم‌بستگی‌های EPR کامل تطابق میان متغیرهای پنهان و مکانیک کوانتمی وجود داشت. همانطور که قبلا مشاهده کردید احتمالات شرطی بهتر می‌توانند ناموضعیت میان خروجی‌ها را نشان دهند لذا در ادامه با تعمیم آنالیز بایاسی می‌توانیم رابطه زیر را برای احتمال توامان ناموضع (۳-۲۹) داشته باشیم [۱۲]:

$$P(\phi_1\lambda_a,\phi_2\lambda_b,\phi_3\lambda_c)=P(\phi_1\lambda_a\,|\,\phi_2\lambda_b,\phi_3\lambda_c)P(\phi_2\lambda_b\,|\,\phi_3\lambda_c)P(\phi_3\lambda_c) \qquad (۳۳-۳)$$

$P(\phi_2\lambda_b\,|\,\phi_3\lambda_c)$ یعنی احتمال اینکه رویداد λ_b اتفاق بیافتد به این شرط که قبلا λ_c اتفاق افتاده باشد. و $P(\phi_1\lambda_a\,|\,\phi_2\lambda_b,\phi_3\lambda_c)$ نیز احتمال این است که λ_a اتفاق بیافتد با رعایت این شرط که قبلا λ_b و λ_c اتفاق افتاده‌اند. در اینجا می‌دانیم که به ازای حالت GHZ برای همه‌ی مقادیر λ_b و λ_c مقادیر احتمالاتی $P(\phi_3\lambda_c)=\frac{1}{2}$ و $P(\phi_2\lambda_b\,|\,\phi_3\lambda_c)=\frac{1}{2}$ را داریم.

احتمالات شرطی را به‌صورت زیر داریم:

$$P(1|11)=P(0|01)=P(1|00)=P(0|10)=\frac{1}{2}(1-\cos\phi)$$
$$P(1|10)=P(1|01)=P(0|11)=P(0|00)=\frac{1}{2}(1+\cos\phi)$$

مشاهده خواهیم کرد که تنها به ازای دو زاویه‌ی $\phi=\pi$ و $\phi=0$ مقادیر احتمالات شرطی یا مقدار 0 می‌پذیرد یا مقدار 1. به ازای زاویه‌ی $\phi=\pi$ که منطبق بر جایگشت‌های (x,y,y) و (y,x,y) و (y,y,x) می‌باشد احتمالات شرطی زیر را داریم[۱۲]:

$$P(1|11)=P(0|01)=P(1|00)=P(0|10)=1$$
$$P(1|10)=P(1|01)=P(0|11)=P(0|00)=0$$

بنابراین خروجی‌های این آزمایش به‌صورت زیر می‌باشند:

$$t(\vec{a},\lambda_a)=0110...$$
$$t(\vec{b},\lambda_b)=0101...$$
$$t(\vec{c},\lambda_c)=1100...$$

و آن‌چه با توجه به نظریه متغیرهای پنهان می‌توان به آن دست یافت رابطه‌ی زیر می‌باشد:

$$4t(x,\lambda_a)t(y,\lambda_b)t(y,\lambda_c)-2[t(x,\lambda_a)t(y,\lambda_b)+t(y,\lambda_b)t(y,\lambda_c)+t(x,\lambda_a)t(y,\lambda_c)]$$
$$+[t(x,\lambda_a)+t(y,\lambda_b)+t(y,\lambda_c)]=1$$

با استفاده از نمادگزاری مختصر $t_i^{\phi}=t(\phi_i,\lambda_i)$داریم:

$$4t_a^x t_b^y t_c^y-2(t_a^x t_b^y+t_b^y t_c^y+t_a^x t_c^y)+(t_a^x+t_b^y+t_c^y)=1 \qquad (۳۴-۳)$$

روابط مشابهی نیز برای (y,x,y) و (y,y,x) برقرار می‌باشد. خروجی‌های آزمایش در رابطه بالا صدق می‌کنند. لذا آن‌چه در آزمایش بدست می‌آید منطبق بر نظریه متغیرهای پنهان می‌باشد.

می‌دانیم که به ازای زاویه $\phi = 0$ یا به عبارتی (x, x, x) نیز همبستگی‌های کامل راداریم به ازای این زاویه احتمالات شرطی را به صورت زیر داریم:

$$P(1|11) = P(0|01) = P(1|00) = P(0|10) = 0$$
$$P(1|10) = P(1|01) = P(0|11) = P(0|00) = 1$$

بنابراین به ازای این زاویه خروجی‌های زیر را داریم[۷]:

$$t(\vec{a}, \lambda_a) = 1100...$$
$$t(\vec{b}, \lambda_b) = 1010...$$
$$t(\vec{c}, \lambda_c) = 0110...$$

مرمین با تکیه بر نظریه واقعیت‌گرایی موضعی رابطه زیررا دست آورد:

$$4t_a^x t_b^x t_c^x - 2(t_a^x t_b^x + t_b^x t_c^x + t_a^x t_c^x) + (t_a^x + t_b^x + t_c^x) = 1 \qquad (۳۵-۳)$$

خروجی‌های آزمایش در رابطه بالا صدق نمی‌کنند پس مشاهده خواهیم کرد که نظریه متغیرهای پنهان منطبق بر مکانیک کوانتمی نخواهد بود و در واقع آن‌چه در واقعیت اتفاق می‌افتد منطبق بر نظریه مکانیک کوانتمی خواهد بود. بنابراین نظریه متغیرهای پنهان رد خواد شد[۱۱و۱۹].

۳-۵ محاسبه میزان کاتورگی

حال که وجود کاتورگی ذاتی را پذیرفتیم بنابراین می‌دانیم که با استفاده از آزمایشاتی که بر روی سیستم‌های کوانتمی انجام می‌دهیم می‌توانیم خروجی بدست بیاوریم که کاملا تصادفی باشد. و از این خروجی‌ها در فرآیند اطلاعات و رمزنگاری کوانتمی استفاده کنیم. میزان حداقل آنتروپی شانون میزان کاتوره‌ای بودن را به‌صورت یک مقدار کمّی نشان می‌دهد[۱۰]. هر چه سیستم ما کاتوره‌ای‌تر، تخمین

رفتار بعدی آن دشوارتر خواهد شد. در ادامه قصد داریم میزان کاتورگی ذاتی سیستم خالص را محاسبه کنیم.

در ابتدا یک سیستم درهم‌تنیده کوانتمی را در نظر می‌گیریم و یک آزمایش بل را انجام می‌دهیم. می‌دانیم که ناموضعیت یکی از ویژگی‌های اصلی سیستم‌های کوانتمی است. لذا خروجی‌های این آزمایش نامساوی بل را نقض می‌کند چرا که یک نامساوی بل در شرایط موضعیت کلاسیک حاکم است. و در صورت نقض نامساوی بل الزاما کاتورگی داریم.

یک حالت دو کیوبیتی ψ را میان طرفین آلیس و باب به اشتراک می‌گذاریم که آنها به‌ترتیب عملگرهای A و B را بر روی ذره خود اعمال می‌کنند. به ازای اعمال عملگر A بر روی ذره آلیس خروجی a را داریم، و به ازای اعمال عملگر B بر روی ذره باب خروجی b را داریم. خروجی‌های این آزمایش اعداد کاملا تصادفی می‌باشند.

خروجی‌های آزمایش یک توزیع احتمال را تشکیل می‌دهد. این احتمالات را می‌توان با استفاده از رابطه (۳-۲) و وارد کردن عملگرهای A و B و حالت ψ به صورت $P(ab|\psi,A,B)$ نمایش داد. به مقدار حداکثر این احتمالات، احتمال حدسی[۲۹] می‌گوییم:

$$G(\psi,A,B)=\max P(ab|\psi,A,B) \qquad (۳۶-۳)$$

با لگاریتم گرفتن از این مقدار حداقل آنتروپی[۳۰] سیستم را بدست می‌آوریم که همان کاتورگی سیستم را تشکیل می‌دهد:

$$H_{\infty}(\Psi,A,B)=-\log_2 G(\Psi,A,B) \qquad (۳۷-۳)$$

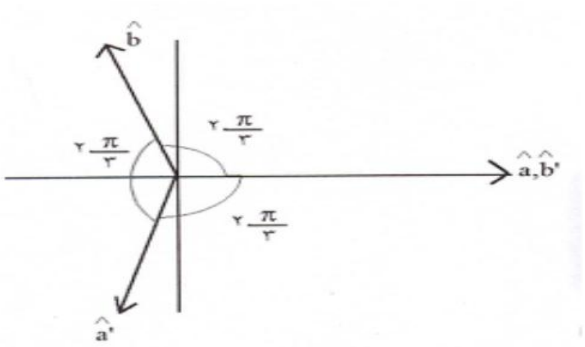
برای مثال یکی از حالات بل را درنظر می‌گیریم:

[29] Guessing probability
[30] Min-entropy

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad (۳۸-۳)$$

این حالت میان آلیس و باب به اشتراک گذاشته شده. آزمایش بلی را ترتیب می‌دهیم که به ازای خروجی‌های آزمایش نامساوی بل CH را به ازای زوایای زیر (همانند شکل(۳-۳))نقض می‌کنند:

$$\theta_{a',b'} = \frac{2\pi}{3}, \theta_{a,b} = \frac{2\pi}{3}, \theta_{a',b} = \frac{2\pi}{3}, \theta_{a,b'} = 0$$



شکل(۳-۳): نمایشی از زوایای میان a',a,b',b در آزمایش CH

به دلیل نقض نامساوی بل برای این سیستم درهم‌تنیده دارای مقداری کاتورگی هستیم. برای محاسبه‌ی میزان کاتورگی سیستم ابتدا احتمالات ناموضع را بدست خواهیم آورد:

$$p(a,b) = \frac{1}{2}\sin^2(\frac{\theta_{a,b}}{2}) = \frac{3}{8}$$
$$p(a',b') = \frac{1}{2}\sin^2(\frac{\theta_{a',b'}}{2}) = \frac{3}{8}$$
$$p(a',b) = \frac{1}{2}\sin^2(\frac{\theta_{a',b}}{2}) = \frac{3}{8}$$
$$p(a,b') = \frac{1}{2}\sin^2(\frac{\theta_{a,b'}}{2}) = 0$$
$$p(a') = \frac{1}{2}$$
$$p(b') = \frac{1}{2} \qquad (۳۹-۳)$$

در ادامه به ازای جایگذاری مقادیر احتمال بالا در نامساوی بل یعنی در رابطه (۳-۵) مقدار این نامساوی ۰/۱۲۵ می‌شود[۱۳]:

$$p(\vec{a},\vec{b})+p(\vec{a},\vec{b'})-p(\vec{a'},\vec{b})+p(\vec{a'},\vec{b'})-p(\vec{a})-p(\vec{b})=\frac{3}{2}\sin^2(\frac{\pi}{3})-1=\frac{1}{8}>0$$

مشاهده می‌کنیم که این نامساوی نقض می‌گردد و میزان این نقض میزان ناموضعیت سیستم را نشان می‌دهد. در ادامه میزان احتمال حدسی سیستم را بدست می‌آوریم. در اینجا فرض کنید عملگرهای اعمالی آلیس و باب به صورت A,B باشند. میزان احتمال حدسی طبق رابطه (۳-۳۶) به صورت زیر می‌باشد:

$$G(\psi,A,B)=\max P(ab\,|\,\psi,A,B)=\frac{3}{8}$$

میزان کاتورگی سیستم به‌صورت زیر بدست خواهد آمد:

$$H_\infty(\psi,A,B)=-\log_2 G(\psi,A,B)=-\log_2 0.375=1.42$$

پس در این مثال مشاهده می‌کنیم که به ازای 0.125 ناموضعیت از سیستم به ازای نامساوی CH به میزان 1.42 بیت کاتورگی می‌رسیم. گرچه میزان حداکثر کاتورگی به ازای این سیستم دو کیوبیتی به میزان 2 بیت می‌باشد، که در این‌جا حاصل نشده است. برای مثال حالت دیگری را درنظرمی‌گیریم:

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

در اینجا عملگرهای زیر را بر روی سیستم اعمال می‌کنیم:

$$A_1 = \sigma_X$$
$$A_2 = \sigma_Z$$
$$B_1 = \frac{\sqrt{2}}{2}(\sigma_X + \sigma_Z) \qquad (۴۰-۳)$$
$$B_2 = \frac{\sqrt{2}}{2}(\sigma_X - \sigma_Z)$$

نامساوی CHSH[۳۱] را به‌صورت زیر داریم[۹]:

$$I = \langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle \le 2 \qquad (۴۱-۳)$$

این نامساوی به ازای مقادیر رابطه (۳-۴۰) نقض می‌شود:

$$\langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = \frac{4}{\sqrt{2}} = 2\sqrt{2} > 2$$

در ادامه مقادیر احتمالاتی را طبق رابطه زیر داریم:

$$P(\mathrm{ab}\,|\,\mathrm{uv}) = \langle \Psi | \hat{P}(a) \otimes \hat{P}(b) | \Psi \rangle = \frac{1}{4}(1 + a\langle A_{\mathrm{u}} \rangle + b\langle B_{\mathrm{v}} \rangle + ab\langle A_{\mathrm{u}} B_{\mathrm{v}} \rangle) \qquad (۴۲-۳)$$

u و v به‌ترتیب عملگرهای مربوط به سیستم آلیس و باب می‌باشند. با استفاده از روابط (۳-۴۰) مقادیر انتظاری ما به‌صورت زیر می‌باشد[۱۴]:

$$\langle A_{\mathrm{u}} \rangle = \langle B_{\mathrm{v}} \rangle = 0$$
$$\langle A_1 B_{\mathrm{v}} \rangle = \frac{1}{\sqrt{2}} \qquad (۴۳-۳)$$
$$\langle A_2 B_{\mathrm{v}} \rangle = \frac{(-1)^{\mathrm{v}}}{\sqrt{2}}$$

[31] Clauser-Horn-Shimony-Holt

در ادامه با جایگذاری مقادیر انتظاری بالا (رابطه (۳-۴۳)) در رابطه (۳-۴۲) می‌توانیم به مقادیر احتمالاتی دست پیدا کنیم[۱۴]. مقدار حداکثر احتمالات (۳-۴۲) مقدار احتمال حدسی را نشان می‌دهد:

$$G(\Psi, A_{\mathrm{u}}, B_{\mathrm{v}}) = \max P(\mathrm{ab} \mid \Psi, A_{\mathrm{u}}, B_{\mathrm{v}}) = \frac{1}{4} + \frac{1}{4\sqrt{2}} = 0.427$$

در انتها با جایگذاری این احتمال حدسی در رابطه (۳-۳۷) به مقدار کاتورگی سیستم دست می‌یابیم:

$$H_{\infty}(\Psi, A_{\mathrm{u}}, B_{\mathrm{v}}) = -\log_2 G(\Psi, A_{\mathrm{u}}, B_{\mathrm{v}}) = -\log 0.427 = 1.23$$

مشاهده می‌کنیم که میزان کاتورگی حاصله در اینجا 1.23 می‌باشد در صورتی که در مثال اولی میزان کاتورگی 1.42بود لذا می‌توان سیستم‌های کوانتمی را از لحاظ میزان کاتورگی سیستم با یکدیگر مقایسه کرد.

۳-۶ انواع کاتورگی

در فرمالیزم کوانتمی دو نوع کاتورگی داریم که از یکدیگر متمایزند. یکی کاتورگی حالات خالص و دیگری کاتورگی حالات مخلوط که صرفا نمایشی از فقدان دانش در مورد حالات محکم و قطعی یک سیستم است. یک توزیع p زمانی یک مقدار قطعی شده‌ی موضعی دارد که یک اندازه‌گیری u همیشه مقدار خروجی $a = \alpha_u$ را بدهد و اندازه‌گیری بر روی v همیشه مقدار خروجی $b = \alpha_v$ را بدهد یعنی داشته باشیم:

$$p(ab \mid uv) = \delta(a, \alpha_u)\delta(b, \beta_v) \qquad (۳-۴۴)$$

حال میزان کاتورگی خروجی‌های اندازه‌گیری یک آزمایش بل را کمّی می‌کنیم. اگر بتوانیم میزان خروجی آزمایش را با قطعیت حدس بزنیم میزان احتمال حدسی مقدار حداکثری 1 را دارد و به میزان 0 بیت کاتورگی داریم:

$$G(\psi,A,B)=1\Rightarrow H_{\infty}(\psi,A,B)=0$$

و اگر همه‌ی چهار خروجی احتمال برابر داشته باشند آن‌گاه احتمال حدسی ما دارای کمترین مقدار خود یعنی $\frac{1}{4}$ می‌باشد که مطابق با دو بیت کاتورگی هستیم:

$$G(\Psi,A,B)=\frac{1}{4}\Rightarrow H_{\infty}(\psi,A,B)=2$$

فرض کنید برای مثال می‌خواهیم کاتورگی سیستم خالص $|\psi\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ را حساب کنیم اگر فرض کنید $A=\sigma_z$ و $B=\sigma_x$ و به ازای همه‌ی مقادیر $a,b=0,1$ مقدار احتمال توام را $P(ab|\psi,A,B)=\frac{1}{4}$ داریم. بنابراین مقدار احتمال حدسی $G(\psi,A,B)=\frac{1}{4}$ می‌باشد. از این رو دارای مقدار کاتورگی حداکثری 2 بیت می‌باشیم[۱۴].

۳-۶-۱ کاتورگی سیستم مخلوط

به ازای یک حالت مخلوط کاتورگی سیستم را طبق رابطه زیر بدست می‌آوریم:

$$G(\rho,A,B)=\max_{q_\lambda\psi_\lambda}\sum_{\lambda}q_\lambda G(\psi_\lambda,A,B) \qquad (۴۵-۳)$$

در اینجا max بر روی همه‌ی مقادیر خالصی که بر طبق تجزیه‌ی حالت مخلوط به آن‌ها می‌رسیم گرفته می‌شود یعنی برطبق رابطه زیر:

$$\rho = \sum_i q_j \left|\psi_i\right\rangle\left\langle\psi_i\right| = \sum_j p_i \left|\varphi_j\right\rangle\left\langle\varphi_j\right| \qquad (۴۶-۳)$$

به عنوان مثالی از کاتورگی موجود در سیستم‌های مخلوط، حالت مخلوط $\rho = \frac{(|00\rangle\langle 00| + |11\rangle\langle 11|)}{2}$ را درنظربگیرید. آن‌گاه عملگرهای اعمالی آلیس و باب به‌ترتیب $A = \sigma_z$ و $B = \sigma_x$ می‌باشند. آن‌گاه $P(ab \mid \Psi, A, B) = \frac{1}{4}$ را به‌عنوان مقدار احتمال توام به ازای همه‌ی مقادیر $a,b = 0,1$ خواهیم داشت. بر طبق روابط بالا می‌توانیم مقدار احتمال حدسی را $G(\rho, A, B) = \frac{1}{2}$ بگیریم، که البته این مقدار احتمال حدسی به ازای پایه‌ی دیگری بدست آمده است:

$$\begin{cases} \frac{1}{2}G(\psi_1, A, B) + \frac{1}{2}G(\psi_2, A, B) \\ P_1 G(\varphi_1, A, B) + P_2 G(\varphi_2, A, B) \end{cases} \qquad (۴۷-۳)$$

در واقع به ازای حالات خالص φ_j ما به مقدار حداقل کاتورگی ذاتی سیستم دست می‌یابیم[۱۴].

فصل چهارم

ارتباط میان کاتورگی و ناموضعیت

مقدمه

با رد متغیرهای پنهان موضعی وجود کاتورگی ذاتی پذیرفته می‌شود. بنابراین سیستم‌های کوانتمی مولدهای بسیار خوبی برای تولید اعداد واقعا تصادفی می‌باشند زیرا که می‌توانند امنیت لازمه را در سیستم‌های کوانتمی بوجود آورند. هدف این است که سیستمی انتخاب کنیم که بتواند بیشترین کاتورگی را بوجود آورد. سوال اینجاست که آیا سیستم‌های کوانتمی که نامساوی بل را بیشتر نقض می‌کنند، و در واقع ناموضعی‌ترند می‌توانند این میزان کاتورگی حداکثری را برای ما بوجود بیاورند.

ارتباط کمّی میان ناموضعیت و کاتورگی بودن به سختی کشف شده است. در اینجا رابطه‌ی میان ناموضعیت، درهم‌تنیدگی و مقادیری از کاتورگی[۳۲] که به ازای نقض یک نامساوی بل در آزمایش موجود می‌باشد را بررسی می‌کنیم. نتایج نشان می‌دهند که کمیت‌های ناموضعیت، درهم‌تنیدگی و مقادیری از کاتورگی که در یک آزمایش بل وجود دارد ارتباط نابرابری با یکدیگر دارند. نشان خواهیم داد که تولید کاتورگی مطلوب با سرعت بهینه و با استفاده از همبستگی‌های تقریبا موضعی و یا حالات تقریبا غیر درهم‌تنیده نیز اتفاق می‌افتد.

[32] Randomness

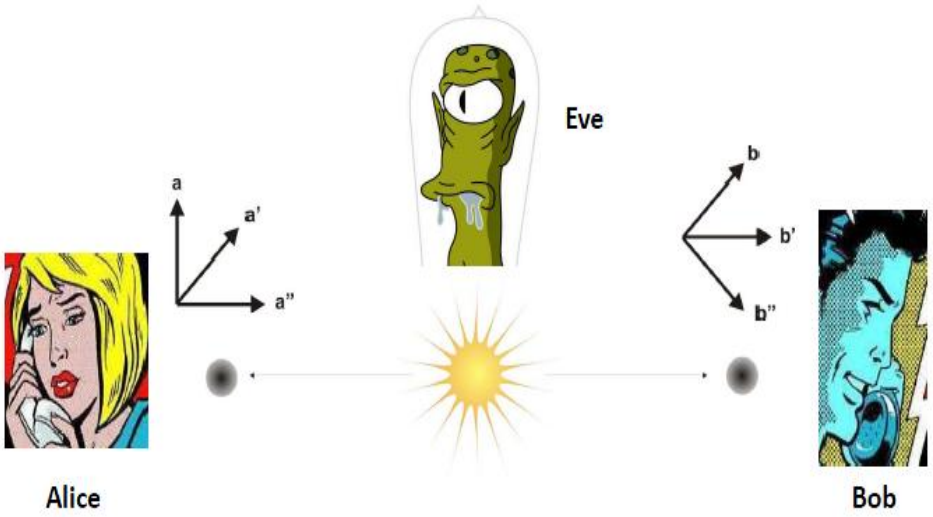
۴-۱ ناموضعیت و کاتورگی

بر طبق نظریه‌ی کوانتمی خروجی‌های یک آزمایش بل، برای یک حالت درهم‌تنیده‌ی خالص که نامساوی بل را نقض می‌کند، الزاما یک مقدار کاتورگی را نشان می‌دهد. همانطور که می‌دانیم حالات درهم‌تنیده ممکن است مخلوط یا خالص باشند، ولی ازآنجایی که حالات خالص همواره نامساوی بل را نقض می‌کنند لذا همواره به ازای حالات خالص درهم‌تنیده کاتورگی داریم.

همانطور که در فصل قبل مشاهده کردید به ازای نقض حداکثری نامساوی CHSH به میزان 1.23 بیت کاتورگی داریم، در حالی که با انجام اندازه‌گیری‌هایی با خروجی‌های باینری از دو زیر مجموعه دارای 2 بیت کاتورگی سراسری[۳۳] هستیم. در واقع به ازای حداکثر نقض نامساوی بل حداکثر کاتورگی بوجود نیامده است. می‌توانیم نشان دهیم برای حالاتی که نامساوی CHSH را کم نقض می‌کنند، و یا حالاتی که درهم‌تنیدگی کمی دارند، نزدیک به حداکثر 2 بیت کاتورگی داریم. در واقع می‌توان توزیع کلید کوانتمی[۳۴] با یک کاتورگی مطلوب و با سرعتی خوب را به ازای حالاتی که ناموضعی کمی دارند و یا حالاتی که درهم‌تنیدگی کمی دارند مشاهده نمود.

دو ویژگی اساسی نظریه‌ی کوانتمی کاتورگی ذاتی و خصوصیت ناموضعیت آن است. برای اولین بار بورن به خصوصیت کاتورگی ذاتی در نظریه‌ی کوانتمی دست یافت. همبستگی‌هایی که ناموضعیت را نشان می‌دهند حالات درهم‌تنیده‌ای هستند که بر روی آنها اندازه‌گیری انجام می‌شود و این همبستگی‌های ناموضع، نامساوی‌های بل را نقض می‌کنند. همانطور که در فصول قبلی اشاره کردیم می‌توان بل را بنیانگذار اصلی نامساوی‌هایی دانست که برای حالات موضعی برقرار هستند.

[33] Global randomness
[34] Quantum key distribution



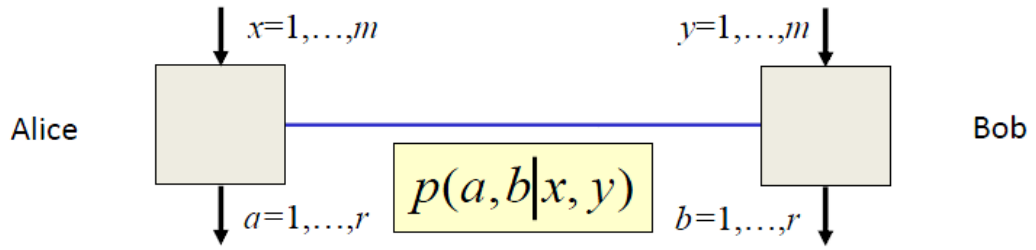
شکل (۴-۱): حضور Eve به‌عنوان جاسوس در فرآیند QKD

هر گاه هیچ نامساوی بلی در یک آزمایش بل نقض نشود آنگاه نتایج یک سری توضیحات قطعی شده می‌باشند. اندازه‌گیری های ما ساده‌ترین و واقعی ترین نامساوی یعنی نامساوی CHSH رانقض می‌کند این نامساوی به ازای دو زیرسیستم و خروجی‌های باینری برقرار است. نقض این نامساوی شرط لازمی برای وجود کاتورگی می‌باشد. میزان نقض نامساوی CHSH میزان ناموضعیت را نشان می‌دهد. به سادگی می‌توانیم انتظار داشته باشیم رابطه‌ی مستقیمی میان مقادیری ازنقض نامساوی CHSH و بنابراین درهم‌تنیدگی و کاتورگی تولید شده در یک آزمایش بل وجود داشته باشد. انتظار داریم که هرچه نقض نامساوی CHSH کمتر باشد، و یا درهم‌تنیدگی کمتر باشد، میزان کاتورگی نیز کمتر باشد، ولی آزمایش نشان می‌دهد که این درک مستقیم درست نمی‌باشد، و ارتباط میان این سه مفهوم دقیق‌تر از آن است که انتظار داریم.

۴-۲ طرح آزمایش بل

یک آزمایش بل استاندارد را با (N, M, d) نشان می‌دهیم. که N بخش جدا از هم داریم که هر کدام از بخش‌های جدا از هم M تا اندازه‌گیری انجام می‌دهند. و به ازای هر اندازه‌گیری دارای d خروجی می‌باشیم. با تکرار آزمایش دارای یک توزیع احتمال می‌شویم. توزیع احتمال را به فرم کلی $P(a_1,...,a_N \mid x_1,...,x_N)$ نشان می‌دهیم، که مقدار a_i خروجی آزمایش است که از اعمال اندازه گیری x_i بر روی ذره i پدید می‌آید $(1 \le i \le N)$. اغلب اندازه‌گیری‌هایی را درنظر می‌گیریم که دارای خروجی باینری هستند یعنی $d = 2$ (همانند نامساوی CHSH)[۱۰].

در اینجا اندازه‌گیری‌هایمان را بر روی دو سیستم مجزای آلیس و باب انجام می‌دهیم. بر سیستم آلیس دو عملگر اندازه‌گیری A_u اعمال می‌شود، که $u \in \{1,2\}$ می‌باشد، که به ازای هر اندازه‌گیری دو خروجی داریم (در واقع خروجی‌ها باینری می‌باشند)، که خروجی‌ها را با $a \in \{0,1\}$ نشان می‌دهیم. به همین ترتیب بر روی سیستم باب نیز دو عملگر اندازه‌گیری B_v اعمال می‌شود که $v \in \{1,2\}$ می‌باشد. و به ازای هر اندازه‌گیری باب بر روی ذره مربوط به خود دو خروجی داریم که خروجی‌ها را با $b \in \{0,1\}$ نشان می‌دهیم (داریم $(2,2,2)$)[۱۰].



شکل(۴-۲): آزمایش بل به ازای m تا ورودی و r تا خروجی

توزیع احتمال کلی را به‌صورت زیر داریم[۱۱]:

$$P(a_1,...,a_N \mid x_1,...,x_N) = \frac{1}{d^N}(1+\sum_{i=1}^{N} a_i \langle A_i \rangle + \sum_{i<j} a_i a_j \langle A_i A_j \rangle + \sum_{i<j<k} a_i a_j a_k \langle A_i A_j A_k \rangle + ...$$
$$+a_1 a_2 a_3 ... a_N \langle A_1 A_2 ... A_N \rangle)$$

در ادامه با استفاده از رابطه بالا احتمال توامان اینکه آلیس با اعمال عملگر A_u بر روی ذره‌ی خود مقدار a را بدست آورد و باب با اعمال عملگر B_v بر روی ذره‌ی خود مقدار b را بدست آورد مقدار زیر خواهد شد:

$$P(ab \mid uv) = tr[M_{a|u} \otimes M_{b|v} \rho] = \langle \psi | M_{a|u} \otimes M_{b|v} | \psi \rangle$$
$$= \frac{1}{4}(1 + a\langle A_u \rangle + b\langle B_v \rangle + ab\langle A_u B_v \rangle) \qquad (۱-۴)$$

ρ حالت سیستم و $M_{a|u}$، $M_{b|v}$ عملگرهای اندازه‌گیری در فضای هیلبرت دلخواه $H_A \otimes H_B$ می‌باشند در واقع $M_{a|u}$، $M_{b|v}$ عملگرهای مثبتی هستند و مجموع آنها 1 می‌شود. با افزایش ابعاد فضای هیلبرت H_B و H_A ما می‌توانیم بدون اینکه از کلیت مسئله بکاهیم فرض کنیم $M_{a|u}$ و $M_{b|v}$ عملگرهای تصویر هستند. اندازه‌گیری‌ها بر روی دو سیستم مجزا به‌وسیله‌ی مشاهده‌پذیرهای هرمیتی $A_u = M_{0|u} - M_{1|u}$ و $B_v = M_{0|v} - M_{1|v}$ توصیف می شود که دارای ویژه مقادیر ± 1 می‌باشند[۱۴].

در چنین آزمایشی به ازای یک اندازه‌گیری دارای حداکثر $\log_2 d$ مقدار بیت کاتورگی موضعی و به میزان حداکثر $N\log_2 d$ بیت کاتورگی سراسری هستیم. مقدار حداکثر کاتورگی سراسری به ازای یک توزیع یکنواخت، برای هر دسته خروجی $a_0 = a_i,...,a_N$ که دارای دسته اندازه‌گیری $x_0 = x_i,...,x_N$ می‌باشد، به‌میزان $P(a_0 \mid x_0) = \frac{1}{d^N}$ صورت می‌پذیرد [۱۵].

با استفاده از بسطی که بر روی احتمالات موضعی نوشته می‌شود می‌توان به نامساوی‌های بل دست یافت. نامساوی بل به فرم کلی زیر می‌باشد:

$$I = \sum_{abuv} I_{abuv} P(ab|uv) \le I_L \qquad (۲-۴)$$

I_L مرز موضعی نامساوی[۳۵] نامیده می‌شود.

احتمالات توامان کوانتمی (۴-۱) ناموضع می‌باشند زیرا بستگی به جهت اندازه‌گیری‌ها دارند. ناموضعیت همان طور که می‌دانیم به این معناست که تصمیم آلیس برای اعمال عملگر اندازه‌گیری بر روی ذره‌ی خودش بر روی احتمال نتیجه‌ی باب تاثیر بگذارد. نامساوی بل (۴-۲) با استفاده از این مقادیر احتمالاتی ناموضع نقض می‌شود. هدف این است که با محاسبه‌ی میزان نقض یک نامساوی بل میزان ناموضعیت یک سیستم را محاسبه کنیم.

عبارت بل به فرم کلی زیر می‌باشد:

$$I_\alpha^\beta = \beta\langle A_1\rangle + \alpha\langle A_1B_1\rangle + \alpha\langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle \qquad (۳-۴)$$

رابطه بالا وابسته به مقادیر β و α می‌باشد. بدون اینکه از کلیت مسئله بکاهیم فرض می‌کنیم $\beta \ge 0$ و $\alpha \ge 1$. مقدار حداکثر رابطه (۴-۳)، $\beta + 2\alpha$ می‌باشد[۱۴].

چنانچه داشته باشیم $\beta = 0$: برای اینکه به فرم ساده‌تری از عبارت (۴-۳) برسیم مقدار $\beta = 0$ را قرار می‌دهیم. بنابراین عبارت بل ما به‌صورت زیر تبدیل می‌شود:

$$I_\alpha = I_\alpha^0 = \alpha\langle A_1B_1\rangle + \alpha\langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle \qquad (۴-۴)$$

در ادامه می‌خواهیم مقدار حداکثر I_α را حساب کنیم، لذا در ابتدا سه اقدام تکنیکی انجام می‌دهیم:

۱) اولین اقدام این است که کارمان را محدود به سیستم‌های دو کیوبیتی کنیم، یعنی برای هر قسمت یک ذره داشته باشیم. می‌دانیم که حالت کلی درهم‌تنیده می‌تواند به ازای قسمتهای بیشتر و تعداد

[35] Local bound of the inequality

ذرات بیشتر هم اتفاق بیافتد. ولی در اینجا اندازه‌گیری‌هایمان را بر روی یک سیستم خالص دو کیوبیتی به فرم کلی زیر انجام می‌دهیم:

$$|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle \qquad 0 \le \theta \le \pi/4 \qquad (۵-۴)$$

این حالت میان طرفین آلیس و باب به اشتراک گذاشته شده. هر یک از این طرفین مشاهده‌پذیرهای زیر را بر روی کیوبیت مربوط به خود اعمال می‌کنند:

$$\begin{aligned} \mathrm{A_u} &= \vec{\mathrm{a}}_\mathrm{u}.\vec{\sigma} \\ \mathrm{B_v} &= \vec{\mathrm{b}}_v.\vec{\sigma} \end{aligned} \qquad (۶-۴)$$

بردارهای یکه $\vec{\mathrm{a}}_\mathrm{u} = (a_u^1, a_u^2, a_u^3)$ و $\vec{\mathrm{b}}_v = (b_v^1, b_v^2, b_v^3)$ به‌ترتیب جهت قطبش‌های عملگرهای آلیس و باب هستند و $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ عملگرهای پاولی می‌باشند. دو تابع محدب $f_{uv}(I)$ و $g_u(I)$ را نیز در نظر می‌گیریم که این توابع مرزهای $G(\psi, A_u, B_v) \le f_{uv}(I)$ و $G(\psi, A_u) \le g_u(I)$ را بر روی احتمالات حدسی اعمال می کنند[۱۵].

۲) به ازای اندازه‌گیری‌های رابطه (۴-۶) بر روی حالت دو کیوبیتی به فرم رابطه (۴-۵) حدود زیر بر مقادیر انتظاری عملگرها اعمال می‌شود:

$$\begin{aligned} -\cos 2\theta \le \langle \mathrm{A_u} \rangle \le \cos 2\theta \\ -\cos 2\theta \le \langle \mathrm{B_v} \rangle \le \cos 2\theta \end{aligned} \qquad (۷-۴)$$

که مقادیر مرزی این حدود به ازای $\mathrm{A_u} = \pm\sigma_z$ و $\mathrm{B_v} = \pm\sigma_z$ حاصل می‌شوند.

۳) نامساوی‌های بل برای حالتی که قسمتها بیشتر باشند و به ازای هر قسمت، تعداد ذرات بیشتر هم اتفاق می‌افتد. به‌عنوان آخرین اقدام هر تناقض I_α را به ازای سیستم‌های 2×2 در نظر می‌گیریم. و به ازای هر دسته از اندازه‌گیری‌های به فرم رابطه (۴-۶) نامساوی بل به‌صورت زیر می‌باشد:

$$\alpha\langle A_1B_1\rangle+\alpha\langle A_1B_2\rangle+\langle A_2B_1\rangle-\langle A_2B_2\rangle\le 2\sqrt{\alpha^2+\sin^2 2\theta} \qquad (۸-۴)$$

یا به عبارتی:

$$I_\alpha \le 2\sqrt{\alpha^2+\sin^2 2\theta}$$

حال می‌خواهیم ببینیم این مقدار حداکثری چگونه حاصل شده است، لذا مشاهده‌پذیرهای آلیس و باب را به فرم زیر در نظر می‌گیریم (با اعمال عملگرهای زیر می‌توانیم به مقدار حداکثر نامساوی (۴-۸) برسیم):

$$\begin{aligned}
A_1 &= \sigma_z \\
A_2 &= \cos\varphi\sigma_x+\sin\varphi\sigma_y \\
B_1 &= \cos\mu\sigma_z+(\sin\mu\cos\varphi)\sigma_z-(\sin\mu\sin\varphi)\sigma_y \\
B_2 &= \cos\mu\sigma_z-(\sin\mu\cos\varphi)\sigma_z+(\sin\mu\sin\varphi)\sigma_y
\end{aligned} \qquad (۹-۴)$$

با در نظر گرفتن عملگرهای اعمالی (۴-۹) بر روی سیستم، جهت محورهای قطبش اندازه‌گیری آلیس و باب را به صورت زیر داریم:

$$\begin{aligned}
\vec{a}_1 &= (0,0,+1) \\
\vec{a}_2 &= (\cos\varphi,\sin\varphi,0) \\
\vec{b}_1 &= (\sin\mu\cos\varphi,-\sin\mu\sin\varphi,\cos\mu) \\
\vec{b}_2 &= (-\sin\mu\cos\varphi,\sin\mu\sin\varphi,\cos\mu)
\end{aligned} \qquad (۱۰-۴)$$

مقادیر انتظاری عملگرهای رابطه (۴-۹) به‌صورت زیر تبدیل خواهد شد:

$$\begin{aligned}
\langle A_1B_1\rangle &= \langle A_1B_2\rangle = \cos\mu \\
\langle A_2B_1\rangle &= -\langle A_2B_2\rangle = \sin\mu\sin 2\theta
\end{aligned} \qquad (۱۱-۴)$$

برای مثال اولین مقدار را به‌صورت زیر محاسبه می‌کنیم:

$$\langle A_1B_1\rangle = \langle \sigma_z \otimes (\cos\mu\sigma_z + (\sin\mu\cos\varphi)\sigma_z - (\sin\mu\sin\varphi)\sigma_y)\rangle$$

$$= \cos\mu\langle\sigma_z\otimes\sigma_z\rangle + \sin\mu\cos\varphi\underbrace{\langle\sigma_z\otimes\sigma_x\rangle}_{0} - (\sin\mu\sin\varphi)\underbrace{\langle\sigma_z\otimes\sigma_y\rangle}_{0}$$
$$= \cos\mu\langle\psi|(|00\rangle\langle 00| - |10\rangle\langle 10| - |01\rangle\langle 01| + |11\rangle\langle 11|)|\psi\rangle$$
$$= \cos\mu(\cos\theta^2 + \sin\theta^2) = \cos\mu$$

با استفاده از روابط (۴-۱۱) و قرار دادن این مقادیر انتظاری در رابطه I_α به مقدار زیر می‌رسیم:

$$I_\alpha = \alpha\langle A_1B_1\rangle + \alpha\langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle = 2(\sin\mu\sin 2\theta + \alpha\cos\mu) \qquad (۴-۱۲)$$

برای محاسبه‌ی میزان حداکثری رابطه بالا مشتق این رابطه را بر حسب μ بدست می‌آوریم و آن را برابر با صفر قرار می‌دهیم:

$$-\alpha\sin\mu + \cos\mu\sin 2\theta = 0 \Rightarrow \sin 2\theta = \alpha\tan\mu$$

با استفاده از رابطه بالا به مقادیر زیر خواهیم رسید:

$$\sin\mu = \frac{\sin 2\theta}{\sqrt{\alpha^2 + \sin^2 2\theta}}$$
$$\cos\mu = \frac{\alpha}{\sqrt{\alpha^2 + \sin^2 2\theta}} \qquad (۴-۱۳)$$

با جایگذاری مقادیر رابطه (۴-۱۳) در رابطه (۴-۱۲) به مقدار حداکثری رابطه (۴-۱۲) می‌رسیم[۱۴و۲۰]:

$$\mathrm{Max}I_\alpha = 2\sqrt{\alpha^2 + \sin^2 2\theta} \qquad (۴-۱۴)$$

۴-۲-۱ کاتورگی زیاد به ازای ناموضعیت کم

مقدار حداکثری رابطه شماره (۴-۱۴) به ازای مقدار زاویه $\theta = \pi/4$ حاصل می‌شود. یا به عبارتی به ازای زاویه‌ی $\theta = \pi/4$ به مقدار حداکثر ناموضعیت می‌رسیم. در این صورت حالت کلی سیستم یا همان رابطه (۴-۵) که میان آلیس و باب به اشتراک گذاشته شده به صورت زیر تبدیل خواهد شد:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad (۴-۱۵)$$

که این حالت دارای حداکثر درهم‌تنیدگی است. لذا به ازای حداکثر ناموضعیت، حداکثر درهم‌تنیدگی پدید آمده است. به ازای این حداکثر درهم‌تنیدگی مقادیر انتظاری عملگرها با استفاده از روابط(۴-۱۱) و (۴-۱۳) به‌صورت زیر درخواهد آمد:

$$\begin{aligned} &\langle \mathrm{A_u} \rangle = \langle \mathrm{B_v} \rangle = 0 \\ &\langle \mathrm{A_1 B_v} \rangle = \frac{\alpha}{\sqrt{1+\alpha^2}} \\ &\langle \mathrm{A_2 B_v} \rangle = \frac{(-1)^v}{\sqrt{1+\alpha^2}} \end{aligned} \qquad (۴-۱۶)$$

قابل ذکر است که به ازای این حداکثر درهم‌تنیدگی دارای حداکثر کاتورگی موضعی هستیم یعنی $G(P,u) = G(P,v) = \frac{1}{2}$ را داریم. حال سوال اینجاست که چه زمانی می‌توانیم مقدار کاتورگی موضعی حداکثری را داشته باشیم؟ یک روش ساده برای پاسخگویی داریم. با درنظرگرفتن دو فرض تقارن‌ها و یکانی بودن توزیع احتمال بر روی نامساوی استاندارد CHSH به این سوال پاسخ داده می‌شود. در مرجع شماره [۱۰] با اعمال این دو فرض مقادیر انتظاری زیر را خواهیم داشت:

$$\langle A_1 \rangle = \langle B_1 \rangle = \langle B_2 \rangle = \langle A_2 \rangle = 0$$

صفر بودن مقدار همبستگی‌های تک‌تایه[۳۶] در واقع متقارن بودن خروجی آزمایش را نشان می‌دهد، یعنی برای مثال در نصف اندازه‌گیری‌ها بر روی ذره مقدار اسپین را در جهت بالا یافته‌ایم، و در نصف دیگر جهت اسپین پایین بوده است، که این امر همان توزیع یکنواخت خروجی موضعی است. و چون دو خروجی داریم لذا مقدار احتمال را $\frac{1}{2}$ می‌یابیم که این همان مقدار احتمال حدسی ما را نشان می‌دهد:

$$G(P,u)=G(P,v)=\frac{1}{2}$$

با لگاریتم گرفتن از این مقدار میزان کاتورگی موضعی را و یا به عبارتی میزان کاتورگی به ازای یکی از خروجی‌ها را به‌میزان $\mathrm{H}_{\infty}=-\log G(P,v)=-\log_2\frac{1}{2}=1$ داریم[۱۰و۲۱] .

در ادامه می‌خواهیم مقدار کاتورگی حالت حداکثر درهم‌تنیده‌ی(۴-۱۵) را محاسبه کنیم. لذا برای محاسبه‌ی میزان کاتورگی در ابتدا میزان احتمالات توام را محاسبه می‌کنیم. با توجه به رابطه‌ی مربوط به احتمالات توام یعنی رابطه (۴-۱) و با جایگذاری روابط (۴-۱۶) در آن به احتمالات توام زیر می‌رسیم:

$$\begin{aligned}\mathrm{P(ab\,|1v)}&=\frac{1}{4}(1+\mathrm{a}\langle \mathrm{A}_1\rangle_0+\mathrm{b}\langle \mathrm{B}_v\rangle_0+\mathrm{ab}\langle \mathrm{A}_1\mathrm{B}_v\rangle)=\frac{1}{4}(1+\frac{\alpha}{\sqrt{1+\alpha^2}})\\ \mathrm{P(ab\,|2v)}&=\frac{1}{4}(1+\mathrm{a}\langle \mathrm{A}_2\rangle_0+\mathrm{b}\langle \mathrm{B}_v\rangle_0+\mathrm{ab}\langle \mathrm{A}_2\mathrm{B}_v\rangle)=\frac{1}{4}(1+\frac{(-1)^v}{\sqrt{1+\alpha^2}})\end{aligned} \qquad (۴-۱۷)$$

با قرار دادن مقدار $\alpha=1$ در رابطه I_{α} به عبارت بل ساده‌ی CHSH می‌رسیم:

$$\mathrm{I}_1=\langle \mathrm{A}_1\mathrm{B}_1\rangle+\langle \mathrm{A}_1\mathrm{B}_2\rangle+\langle \mathrm{A}_2\mathrm{B}_1\rangle-\langle \mathrm{A}_2\mathrm{B}_2\rangle \qquad (۴-۱۸)$$

[36] One-body correlators

به ازای نامساوی CHSH بررسی‌مان را در ادامه با جایگذاری دو مقدار $\alpha=1$ و $\alpha>1$ در روابط مقادیر انتظاری (همانطور که فرض کرده بودیم $\alpha\geq1$) انجام می‌دهیم. مقدار حداکثر نامساوی بل CHSH به ازای حداکثر درهم‌تنیدگی همانطور که قبلا داشتیم، به میزان $I_1=2\sqrt{2}$ می‌شود. به ازای $\alpha=1$ مقدار حداکثر روابط (۴-۱۷) یعنی در واقع احتمال حدسی مقدار زیر خواهد شد:

$$G(P,u,v)=G(P,1,v)=G(P,2,v)=\frac{1}{4}(1+\frac{1}{\sqrt{2}})=\frac{1}{4}+\frac{\sqrt{2}}{8}\approx0.427 \qquad (۱۹-۴)$$

از احتمال حدسی لگاریتم می‌گیریم و میزان کاتورگی سیستم را بدست خواهیم آورد:

$$H_{\infty}=-\log G_{uv}=-\log(0.427)=1.23 \qquad (۲۰-۴)$$

پس به ازای $\alpha=1$ نامساوی بل به میزان $2\sqrt{2}$ نقض می‌شود. و به ازای این درجه از نقض که حداکثر درجه نقض نامساوی بل شماره (۴-۱۸) می‌باشد دارای 1.23 بیت کاتورگی هستیم.

با توجه به اینکه میزان حداکثر کاتورگی 2 بیت می‌باشد ولی مشاهده می‌کنیم که این میزان کاتورگی به ازای یک سیستم حداکثر درهم‌تنیده که نامساوی بل را به صورت حداکثری نقض می‌کند و یا به عبارتی دارای حداکثر ناموضعیت است حاصل نمی‌شود. لذا نتیجه می‌گیریم که به ازای حداکثر ناموضعیت الزاما حداکثر کاتورگی را نداریم. سوال اینجاست که این میزان حداکثر کاتورگی به ازای چه درجه‌ای از نقض حاصل خواهد شد؟

در رابطه (۴-۱۷) مقدار $\alpha>1$ قرار می‌دهیم. آنگاه میزان حداکثر نامساوی بل CHSH با توجه به اینکه باید مقادیر انتظاری حداکثری رابطه (۴-۱۸) را وارد کنیم به این صورت خواهد شد:

$$I_1=\langle A_1B_1\rangle+\langle A_1B_2\rangle+\langle A_2B_1\rangle-\langle A_2B_2\rangle=\frac{2\alpha}{\sqrt{1+\alpha^2}}+\frac{2}{\sqrt{1+\alpha^2}}=\frac{2(\alpha+1)}{\sqrt{\alpha^2+1}}\approx2+\frac{2}{\alpha} \qquad (۲۱-۴)$$

با افزایش مقدار α میزان عبارت بالا که همان میزان نقض نامساوی CHSH است کاهش می‌یابد. در ادامه کاتورگی سیستم را به ازای $\alpha>1$ محاسبه می‌کنیم. ابتدا میزان حداکثر روابط (۴-۱۷) را بدست می‌آوریم:

$$G(\mathrm{P},2,\mathrm{v})=\frac{1}{4}(1+\frac{1}{\sqrt{1+\alpha^2}}) \qquad (۴-۲۲)$$

(که این مقدار احتمال حدسی به ازای $\mathrm{u}=2$ بدست آمده است) از این مقدار لگاریتم می‌گیریم تا میزان کاتورگی سیستم را بدست آوریم:

$$\mathrm{H}_\infty=-\log G(\mathrm{P},2,\mathrm{v})\approx 2-\ln(2)/\alpha \qquad (۴-۲۳)$$

چنانچه میزان α افزایش یابد مشاهده خواهیم کرد که میزان کاتورگی سیستم افزایش می‌یابد. و به میزان حداکثری 2 بیت می‌رسد.

لذا با افزایش مقدار α میزان درجه نقض نامساوی بل کاهش خواهد یافت و از ناموضعیت سیستم کاسته می‌شود ولی میزان کاتورگی سیستم افزایش می‌یابد. پس به ازای ناموضعیت کم حداکثر کاتورگی سیستم که به میزان 2 بیت می‌باشد حاصل می‌شود [۱۴].

چنانچه داشته باشیم $\beta\neq 0$: در بالا مشاهده نمودید که به ازای $\beta=0$ در نامساوی CHSH حداکثر نقض نامساوی بل یا همان حداکثر ناموضعیت در شرایطی به‌وجود می‌آید که ما حداکثر کاتورگی سراسری را نداریم. ولی با توجه به اینکه مقدار $\theta=\frac{\pi}{4}$ قرار می‌دهیم حداکثر درهم‌تنیدگی را داریم و حداکثر کاتورگی موضعی نیز برقرار است. علاوه بر این به ازای $\beta=0$ و $\alpha>1$ دارای میزان حداکثر کاتورگی سراسری هستیم در حالی که حداکثر درجه نقض نامساوی بل را نداریم. در این شرایط مشاهده کردیم که سیستم دارای حداکثر درهم‌تنیدگی و حداکثر کاتورگی موضعی می‌باشد.

می‌خواهیم سیستم را به ازای $\beta>0$ بررسی کنیم، و ارتباط میان ناموضعیت، درهم‌تنیدگی و کاتورگی سراسری و کاتورگی موضعی را بررسی کنیم. سه تکنیک قبلی را به کار می‌گیریم. بنابراین سیستم‌های دو کیوبیتی خالص را در نظر می‌گیریم. هدف اصلی این است که به مقدار حداکثری رابطه (۴-۳) دست یابیم یعنی در واقع مقدار حداکثر عبارت بل (I_α^β) را بدست آوریم. با استفاده از رابطه $I_\alpha^\beta \le 2\sqrt{\alpha^2+\sin^2 2\theta}$ و همچنین حدی که به ازای رابطه $-\cos 2\theta \le \langle A_u \rangle \le \cos 2\theta$ برروی $\langle A_u \rangle$ اعمال می‌شود:

$$\frac{I_\alpha}{2} \le \sqrt{\alpha^2+\sin^2 2\theta} \Rightarrow \frac{I_\alpha{}^2}{4} \le \alpha^2+\sin^2 2\theta \Rightarrow \frac{I_\alpha{}^2}{4}-\alpha^2 \le 1-\cos^2 2\theta \Rightarrow$$
$$\cos 2\theta \le \sqrt{1+\alpha^2-\frac{I_\alpha{}^2}{4}} \xrightarrow[\langle A_1\rangle \le \cos 2\theta]{} \langle A_1 \rangle \le \sqrt{1+\alpha^2-\frac{I_\alpha{}^2}{4}}$$

به رابطه زیر می‌رسیم:

$$\langle A_1 \rangle \le \sqrt{1+\alpha^2-\frac{I_\alpha{}^2}{4}} \qquad (۲۴-۴)$$

این رابطه به ازای $u=1$ نوشته شده است. عبارت بل (۴-۳) را به‌صورت زیر داریم:

$$I_\alpha^\beta = \beta\langle A_1 \rangle + \underbrace{\alpha\langle A_1B_1 \rangle + \alpha\langle A_1B_2 \rangle + \langle A_2B_1 \rangle - \langle A_2B_2 \rangle}_{I_\alpha^0} = \beta\langle A_1 \rangle + I_\alpha^0 \qquad (۲۵-۴)$$

طرفین رابطه (۴-۲۴) را در β ضرب می‌کنیم و با مقدار I_α^0 جمع می‌کنیم:

$$\underbrace{I_\alpha^0+\beta\langle A_1 \rangle}_{I_\alpha^\beta} \le I_\alpha^0+\beta\sqrt{1+\alpha^2-\frac{I_\alpha{}^2}{4}} \Rightarrow I_\alpha^\beta \le I_\alpha^0+\beta\sqrt{1+\alpha^2-\frac{I_\alpha{}^2}{4}} \qquad (۲۶-۴)$$

نامساوی بل را به‌صورت زیر بدست می‌آوریم:

$$I_\alpha^\beta \le I_\alpha^0+\beta\sqrt{1+\alpha^2-\frac{I_\alpha{}^2}{4}} \qquad (۲۷-۴)$$

چنانچه مشتق طرف راست عبارت (۴-۲۷) را نسبت به I_{α}^{0} بدست آوریم و آن را برابر صفر قرار دهیم می‌توانیم مقدار حداکثری نامساوی را بدست آوریم. طرف راست عبارت (۴-۲۷) زمانی حداکثر می‌شود که داشته باشیم $\mathrm{I}_{\alpha}^{0}=\frac{2\sqrt{1+\alpha^{2}}}{\sqrt{1+\frac{\beta^{2}}{4}}}$. با جایگذاری این مقدار در رابطه (۴-۲۷) خواهیم داشت:

$$\mathrm{I}_{\alpha}^{\beta}\le 2\sqrt{(1+\alpha^{2})(1+\frac{\beta^{2}}{4})} \qquad (۴-۲۸)$$

طبق این رابطه مشاهده می‌کنیم که مقدار حداکثری عبارت بل یا همان رابطه (۴-۲۷) مقدار $2\sqrt{(1+\alpha^{2})(1+\frac{\beta^{2}}{4})}$ می‌شود.

در اینجا مقدار حداکثری عبارت بل به ازای $\mathrm{I}_{\alpha}^{0}=\frac{2\sqrt{1+\alpha^{2}}}{\sqrt{1+\frac{\beta^{2}}{4}}}$ حاصل شد و از طرف دیگر با توجه به نتایج قبلی می‌دانیم که این مقدار حداکثری I_{α}^{0} طبق رابطه (۴-۱۴) به ازای $\mathrm{I}_{\alpha}=2\sqrt{\alpha^{2}+\sin^{2}2\theta}$ بدست می‌آید:

$$\mathrm{I}_{\alpha}^{0}=\frac{2\sqrt{1+\alpha^{2}}}{\sqrt{1+\frac{\beta^{2}}{4}}}=2\sqrt{\alpha^{2}+\sin^{2}2\theta}\Rightarrow\sin 2\theta=\sqrt{(1-\frac{\alpha^{2}\beta^{2}}{4})\Big/(1+\frac{\beta^{2}}{4})} \qquad (۴-۲۹)$$

همانطور که ملاحظه می‌کنیدرابطه (۴-۲۹) به ازای هر θ برقرار است. یعنی در اینجا ما هر درجه‌ای از درهم‌تنیدگی را داریم. یعنی حتی به ازای درهم‌تنیدگی‌های جزئی هم این رابطه برقرار است. و چون مقدار $\langle A_{2}\rangle=0$ یعنی $G_{2}=\frac{1}{2}$ (به شرط آنکه $\beta\neq\frac{2}{\alpha}$ باشد). و برای مثال به ازای $\alpha=1$ و $0<\beta<2$ دارای کاتورگی موضعی یک بیت می‌باشیم که همان کاتورگی حداکثری موضعی است. در پایان می‌توان این نتیجه را گرفت که با توجه به رابطه (۴-۲۹) می‌توان درهم‌تنیدگی جزئی را داشت زیرا که این رابطه به ازای θ جزئی نیز صادق می‌باشد [۱۴].

۴-۲-۲ کاتورگی سراسری زیاد به ازای حالات تقریبا غیردرهم‌تنیده

با توجه به آنچه قبلا مشاهده کردیم به ازای $\beta=0$ و $\alpha>1$ می‌توانیم نزدیک به حداکثر 2 بیت کاتورگی داشته باشیم که این امر به ازای حالات حداکثر درهم‌تنیده اتفاق می‌افتد. در اینجا نشان می‌دهیم این حداکثر کاتوره‌ای سراسری می‌تواند به ازای حالات تقریبا غیر درهم‌تنیده اتفاق بیافتد.

در اینجا شرایط کمی پیچیده‌تر می‌شود به طوری که هر یک از آلیس و باب چهار عملگر اندازه‌گیری را بر روی ذره‌ی خود اعمال می‌کنند (یعنی داریم $M=4$). خروجی‌های اندازه‌گیری همانند قبل باینری می‌باشند ($d=2$)، و میزان حداکثر کاتورگی سراسری به ازای یک جفت خروجی همان دو بیت کاتورگی سراسری می‌باشد ($N\log_2 d=2\log_2 2=2$). آلیس چهار عملگر A_1,A_2,A_1',A_2' را بر روی ذره خود اعمال می‌کندو طرف باب نیز چهار عملگر B_1,B_2,B_1',B_2' را بر روی سیستم خود اعمال می‌کند. به ازای چهار عملگر A_1,A_2,B_1,B_2 عبارت (۴-۳) را به‌صورت زیر داشتیم:

$$\mathrm{I}_\alpha^\beta=\beta\langle \mathrm{A}_1\rangle+\alpha\langle \mathrm{A}_1\mathrm{B}_1\rangle+\alpha\langle \mathrm{A}_1\mathrm{B}_2\rangle+\langle \mathrm{A}_2\mathrm{B}_1\rangle-\langle \mathrm{A}_2\mathrm{B}_2\rangle \qquad (۳-۴)$$

چنانچه عملگرهای جدید را به‌صورت A_1',A_2',B_1',B_2'، درنظر بگیریم و نقش آلیس و باب را جابجا کنیم عبارت بل (۴-۳) را به صورت زیر خواهیم داشت:

$$\mathrm{I}_\alpha'^\beta=\beta\langle \mathrm{B}_1'\rangle+\alpha\langle \mathrm{B}_1'\mathrm{A}_1'\rangle+\alpha\langle \mathrm{B}_1'\mathrm{A}_2'\rangle+\langle \mathrm{B}_2'\mathrm{A}_1'\rangle-\langle \mathrm{B}_2'\mathrm{A}_2'\rangle \qquad (۳۰-۴)$$

طبق رابطه (۴-۲۸) مقدار حداکثر $I_\alpha'^\beta$ و I_α^β به ازای مقدار زیر حاصل می‌شود:

$$\mathrm{I}_\alpha^\beta=\mathrm{I}_\alpha'^\beta=2\sqrt{(1+\alpha^2)(1+\frac{\beta^2}{4})} \qquad (۳۱-۴)$$

به ازای خروجی عملگرهای A_2, B_2' دارای کاتورگی حداکثری موضعی می‌باشیم زیرا که داریم $\langle \mathrm{A}_2 \rangle_\psi = \langle \mathrm{B}_2' \rangle_\psi = 0$ (توجه داشته باشید که در اینجا $\beta \neq \frac{2}{\alpha}$).

در ادامه می‌خواهیم به جای استفاده از شرط $\beta \neq \frac{2}{\alpha}$، مقدار β را به سمت 2 میل دهیم یعنی داشته باشیم $\beta \to \frac{2}{\alpha}$. هدف این است که ثابت کنیم نتایج اندازه‌گیری‌ها به ازای عملگرهای A_2 و B_2' به سمت حالات تقریبا غیردرهم‌تنیده می‌روند. بنابر مرجع [۱۰] خواهیم داشت:

$$\left|\langle \mathrm{A}_2 \mathrm{B}_2' \rangle\right| = \sqrt{(1-\frac{\alpha^2\beta^2}{4}) \Big/ (1+\frac{\beta^2}{4})} = \sin 2\theta \qquad (۳۲-۴)$$

اگر برای مثال مقدار $\alpha = 1$ و $\beta = 2-\varepsilon$ را در رابطه بالا قرار دهیم به مقدار زیر خواهیم رسید:

$$\left|\langle \mathrm{A}_2 \mathrm{B}_2' \rangle\right| = \sin 2\theta = \sqrt{\frac{\varepsilon}{2}} \qquad (۳۳-۴)$$

چنان‌چه مقدار احتمال حدسی را حساب کنیم خواهیم داشت:

$$G(\psi, \mathrm{A}_2, \mathrm{B}_2') = \frac{(1+\left|\langle \mathrm{A}_2 \rangle_\psi\right| + \left|\langle \mathrm{B}_2' \rangle_\psi\right| + \left|\langle \mathrm{A}_2 \mathrm{B}_2' \rangle\right|)}{4} = \frac{1}{4}(1+\sqrt{\frac{\varepsilon}{2}}) \qquad (۳۴-۴)$$

پس طبق رابطه (۴-۳۴) می‌بینیم که مقدار احتمال حدسی به سمت حداقل مقدار خود یعنی مقدار $\frac{1}{4}$ پیش می‌رود و میزان کاتورگی سراسری به صورت زیر خواهد شد:

$$\mathrm{H}_\infty = -\log G(P, \mathrm{A}_2, \mathrm{B}_2') = -\log \frac{1}{4}(1+\sqrt{\frac{\varepsilon}{2}}) \approx 2 \qquad (۳۵-۴)$$

بنابراین نزدیک به 2 بیت کاتورگی حداکثری حاصل شده است، در حالی که بنابر رابطه (۴-۳۲) درهم‌تنیدگی جزئی داریم [۱۴].

نتیجه‌گیری

. هدف کلی این رساله بررسی میزان کاتورگی سیستم‌های کوانتمی و در ادامه بررسی ارتباط میان کاتورگی و ناموضعیت است. در این رساله نشان دادیم که اولا سیستم‌های کوانتمی به‌دلیل خاصیت کاتورگی ذاتی برای تولید اعداد کوانتمی منابع خوبی هستند و بهتر از سیستم‌های کلاسیکی می‌توانند امنیت لازم را برقرار کنند. در ادامه رابطه‌ی میان کاتورگی ذاتی و میزان نقض نامساوی بل را محاسبه کردیم. در این رساله میزان کاتورگی به‌صورت کمّی مطرح می‌شود. با توجه به این‌که می‌دانیم سیستم‌های کوانتمی خالص درهم‌تنیده نامساوی بل را نقض می‌کنند با محاسبه‌ی میزان این نقض در واقع میزان ناموضعیت را بدست آوردیم. سپس این میزان ناموضعیت را با میزان کاتورگی مقایسه کردیم. آنچه دریافتیم این بود که ارتباط میان ناموضعیت و کاتورگی سیستم مستقیم نیست و گاه اتفاق می‌افتد که میزان کاتورگی حداکثری دو بیت را به ازای مقادیر کمی از ناموضعیت داشته باشیم، و حتی مواردی داریم که با وجود درهم‌تنیدگی کم کاتورگی حداکثری بوجود آمده است. در ادامه پیشنهاد می‌شود که بررسی در سیستم‌های با تعداد کیوبیت بالا انجام پذیرد و یا حتی به ازای نامساوی‌های دیگری میزان کاتورگی محاسبه گردد، و در سطح بالاتر علت این ارتباط غیر مستقیم میان ناموضعیت ،کاتورگی و درهم‌تنیدگی به‌خوبی توجیه گردد.

مراجع

[۱] قجاوند. مجید، (۱۳۹۰)، پایان‌نامه ارشد:"بهینه‌سازی تولید درهم‌تنیدگی در زنجیره‌های اسپینی"، دانشکده فیزیک، دانشگاه صنعتی شریف.

[2] Seevinck.M.P (2011). "No-signaling, perfect bipartite dichotomic correlations and local randomness", AIP Conf. Proc. **1327, 36-53**.

[3] Michael A. Nielsen & Isaac L.Chuang. (2000). "Quantum Computation And Quantum Information",Cambridge University press.chapter 1, PP.13.

[4] Bohm. D, (1951). "A suggested interpretation of the Quantum Theory interms of hidden variabels". Physical Review **85: 166–179**.

[5] Bohm. D, (1952). "Nonlocality, Lorentz Invariance, and Bohmian Quantum Theory" Phys. Physical Review A S3, **2062-2073**.

[6] Greenstein. G,Zajonc. A.G, (1997)."The Quantum Challenge: Modern Research on the Foundations of Quantum Mechanics".jones and Bartlett publishers. Chapter 1.

[7] McMahon. D, (2008). "Quantum Computing Explained", John Wiley and Sons, Inc, USA, ISBN 978-0-470-09699-4 (cloth).

[۸] محسنی نیا.راضیه، (۱۳۹۰)، پایان‌نامه ارشد:" درهم‌تنیدگی چندبخشی"، دانشکده فیزیک، دانشگاه صنعتی شریف.

[۹] کریمی‌پور.وحید، (۱۳۹۱)، درسنامه محاسبات کوانتمی، درس چهارم:"شناخت جهان واقعی، متغیرهای پنهان و مکانیک کوانتومی" دانشکده فیزیک، دانشگاه صنعتی شریف.

[10] Chirag Dhara, Giuseppe Prettico, and A. Acin. (2013). "Maximal quantum randomness in Bell tests" , Phys. Rev. **A 88, 052116**.

[11] K. Wddkiewicz, Liwei Wang, and J. H. Eberly. (1992) "Perfect Correlations of Three-Particle Entangled States". Physical Review A.

[12] Krzysztof Wodkiewicz, (1995) "Randomness, Nonlocality and Information In Entangled correlations". arXiv: **9505020v1.**

[۱۳] فهمی.اکبر، (۱۳۸۴)، پایان نامه دکتری:"درهم‌تنیدگی و ناموضعیت در نامساوی بل و کاربرد آن در تئوری اطلاعات" دانشکده فیزیک، دانشگاه صنعتی شریف.

[14] Antonio Acin, Serge Massar, Stefano Pironio. (2011).“Randomness vs Non Locality and Entanglement”. arXiv:**1107.275**.

[15] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe.(2010). “Random Numbers Certied by Bell's Theorem”. Nature **464, 1021**.

[16] SBarnett, (2009),“Quantum Information”.Oxford university press.chapter 3.5.8.

[17] A.Einstein, B.Podolsky and N.Rosen, (1935) “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?”, Phys. Rev. **47, 777 - 780** .

[18] Samuel L.Braunstein and Carlton M. (1988). “Caves, Information-theoretic Bell Inequalities”. Phys RevLett.**60.1351**.

[19] Homi Bhabha Road, Mumbai, (2005). “The incompatibility between local hidden variable theories and the fundamental conservation laws”. Pramna journal of physics. Vol. 65. pp. 359-379.

[20] Andre Allan Methot and Valerio Scarani. (2006) “An anomaly of non-locality”. Quantum Information and Computation 7**: 157-170, 2007**.

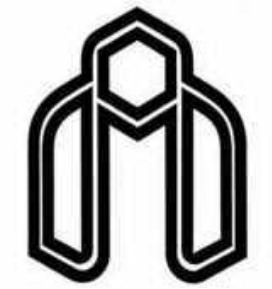
[21] Stefano Pironio, Jean-Daniel Bancal, Valerio Scarani. (2011) “Extremal correlations of the tripartite no-signaling polytope”. Mathematical and Theoretical **44, 065303** .

Abstract

Today, especially in cryptography, random numbers generation is of tremendous importance. To generate random numbers depending on their applications we use different generation methods. Security is an important parameter in cryptography. In this scientific reaserch we're attempting to generate random numbers that are not detected by eavesdropper and contains a strong security. In Newtonian physics, as the complete knowledge of initial conditions along with interactions of a system allows one to predict its future dynamics deterministically There is no securit in determinestic classical methods of generating random numbers. Quantum theory also incorporates a form of randomness in its framework that does not have a classical counterpart. Quantum physics is inherently random, consequently it is convenient to use random numbers generating. In this scientific reaserch we determine randomness through outputs obtained by a bell experiment, then we choose the best system in order to random number generation.

According to quantum theory, the outcomes obtained by measuring an entangled state necessarily exhibit some randomness if they violate a Bell inequality. We are going to investigate the relation between non-locality and the amount of randomness necessarily present in a Bell experiment. Naively, we expect a direct relation between the amount of nonlocallity and the randomness produced in a Bell-type experiment, i.e.,for eaxample the less nonlocality, the less randomness. Our analysis, however, show that this intuition is not correct and that the relation between these two concepts is much subtler than expected. We can consider the amount of violation of the CHSH inequality a natural measure of non-locality then compute the amount of randomness in system. in this scientific reaserch We introduce little non-local correlations that violate arbitrarily little the CHSH inequality yet which necessarily imply that the maximal amounts of randomness. We know that by performing measurements with binary outcomes on two subsystems one could in principle generate up to two bits of randomness. We show that states with arbitrarily little entanglement can be used to certify that close to the maximum of two bits of randomness are produced.

Key words: nonlocallity, randomness, CHSH inequality, entanglement, Guessing probability.



Shahrood University of Technology

Faculty of Physics

Master of Science Thesis

The Connection between Non-locality and Randomness

By:

Fatemeh Adalatkhah

Supervisor:

Dr.HosseinMovahhedian

Winter 2014