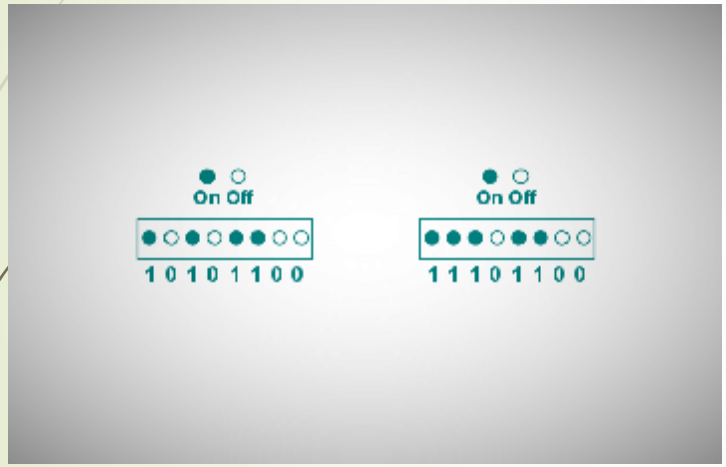
کامپیوترهای کوانتومی

تهیه کننده

جلال حسینی

نحوه کار کامپیوترهای معمولی



- تصویر بالا را در نظر بگیرید، ما در این تصویر 2 بایت مختلف داریم (هر 8 بیت 1 بایت را تشکیل می‌دهد) مجموعه‌ی سمت چپ (10101100) نماینده‌ی عدد 172 و مجموعه‌ی سمت راست (11101100) نماینده‌ی عدد 236 می‌باشد.
- هرکدام از این اعداد با توجه به وضعیت سیستم می‌توانند به شکل متفاوتی تفسیر شوند، مثلا یک کارکتر در نرم‌افزار ورد، یک عدد در ماشین حساب، یک دستورالعمل در پردازنده، بخشی از یک موسیقی یا تصویر و...

ویژگی کوانتومی اشیا چیست؟

- ویژگی کوانتومی بیان می‌کند، یک شی می‌تواند در لحظه چند شی باشد، یا در چندین حالت مختلف باشد!
- فرض کنید سکه‌ای را به هوا پرتاب می‌کنید، سکه‌ی در حال چرخش هم می‌تواند شیر باشد و هم خط و تا وقتی به زمین نرسد به هیچ‌وجه نمی‌توانیم درباره‌ی وضعیت آن اظهار نظر کنیم، مثال بسیار معروفی در این زمینه وجود دارد به نام آزمایش گربه‌ی شرودینگ
- در ادامه برای درک بهتر مفهوم فیزیک کوانتوم این مثال را بررسی می‌کنیم.

آزمایش گربه‌ی شرودینگر

- آزمایش گربه‌ی شرودینگر، یک آزمایش فکری است که توسط اروین شرودینگر (فیزیکدان اتریشی) ابداع شد، این آزمایش به ما نشان می‌دهد هنگامی که قوانین کوانتومی در زندگی روزمره‌ی ما اعمال شوند چه اتفاقی می‌افتد، توصیف این آزمایش به شرح زیر است:
- فرض کنید، گربه‌ای در یک جعبه قرار دارد و یک ظرف سم نیز در آن جعبه است، تا وقتی در جعبه بسته است ما هیچ پیشفرضی درباره سرنوشت گربه نداریم، 50 درصد این احتمال وجود دارد که گربه مرده باشد یا به احتمال 50 درصد زنده باشد (در دنیای کوانتوم مقدار دقیق این احتمال برابر با $1\sqrt{2}$ درصد استتا وقتی در جعبه را باز نکرده‌ایم نمی‌توانیم هیچ اظهار نظری در این‌باره کنیم، به بیان دیگر این گربه هم زنده است و هم مرده، تا اینکه در جعبه را باز کرده و آن‌را نگاه کنیم.

حالات مختلف یک شی

- به طور کلی می‌توان گفت نظریه‌ی فیزیک کوانتومی اینطور بیان می‌کند که همه‌ی اشیا می‌توانند انواع حالات مختلف را در هر لحظه داشته باشند مگر اینکه به آن‌ها نگاه کنیم، اجسام تنها زمانی که به آن‌ها توجه می‌کنیم ویژگی‌های منطقی خود را می‌گیرند و تا قبل از آن هر شی می‌تواند هر چیزی باشد!
- بر هم نهی یا superposition
- در هم تنیدگی (Entanglement) : با اندازه گیری یک ذره ، مقدار ذره کناری را هم حدس بزنید.

مبنای کوانتومی محاسبات

حال که کمی با مفهوم کوانتوم آشنا شدیم بهتر می‌توانید نحوه‌ی کار کامپیوترهای کوانتومی را درک کنید، هر بیت در این کامپیوترها می‌تواند در آن واحد مقداری برابر با 0 و 1 را به طور همزمان داشته باشد تا به آن نگاه کنید (نتیجه‌ی محاسبات را فراخوانی کنید)

کامپیوتر کوانتومی؟

- همانطور که بالاتر گفتیم کامپیوترهای کوانتومی می‌توانند در یک لحظه انواع حالات مختلف مسئله را در خود داشته باشند، مثالی که در ابتدای ارائه گفتیم را به یاد دارید؟ بیت‌هایی که نمایان‌گر دو عدد مختلف بودند.
- گفتیم در یک کامپیوتر معمولی در هر لحظه هر بیت تنها یک مقدار می‌پذیرد، بنابراین مقدار مجموعه‌ی بیتی برابر با 172 یا 236 است، اما در یک کامپیوتر کوانتومی مجموعه‌ی بیتی در هر لحظه برابر با تمام اعداد موجود در این بازه است و می‌تواند به طور همزمان هم برابر 172 و هم برابر 236 باشد!
- در کامپیوترهای کوانتومی اطلاعات در مفهومی بنام کیو بیت ذخیره میشوند. هر کیوبیت به صورت همزمان میتوان هم 0 باشد و هم 1

کامپیوتر کوانتومی و حجم حافظه

- آیا بخاطر دارید که گفتم 8 بیت در کامپیوترهای معمولی تنها میتواند نشان دهنده یک عدد باشد!
- به عبارت دیگر برای نشان دادن 256 حالت عددی نیاز به 8 بیت فضا داریم. که در هر زمان تنها میتواند یک عدد را نشان بدهد
- اما در اسلاید بعدی دقت کنید که 8 کیوبیت میتواند چقدر حافظه تولید کند.

کامپیوتر کوانتومی؟

- مقایسه فضا در کامپیوترهای معمولی و کامپیوترهای کوانتومی
- N=2^q * q

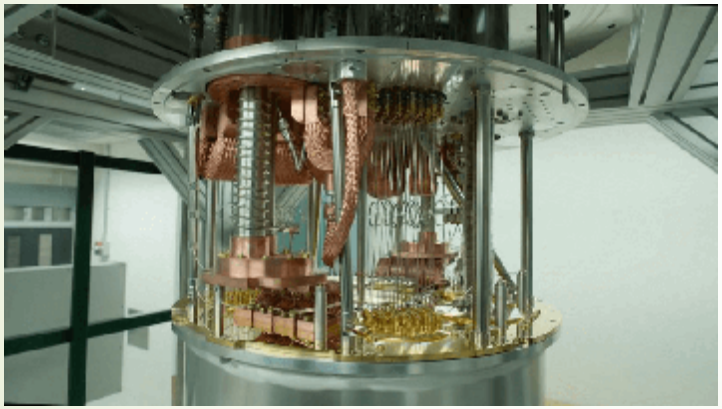
- 1 QB = 2 Bit
- 2 QB = 8 Bit
- 3 QB = 24 Bit
- 4 QB = 64 Bit
- 8 QB = 2048 Bit
- 10 QB = 1.25 Kbyte
- 20 QB = 2.5 M Byte
- 30 QB = 3.75 G Byte
- 40 QB =5 T B
- 43 QB = 43 TB
- 49 QB = 3136 TB
- 50 QB = 6400 T B
- 53 QB = (Google computer) 54272 TB
- 59 QB (IBM Computer) = 3 866 624 TB
- 100 QB = 14,411,518,807,585,587,200 TB
- 100 QB = 14,411,518,807.5 Zeta Byte

- هر زتا بایت معادل 1,000,000,000ترابایت میباشد.
- کل داده های موجود در جهان در سال 2018 حدود 33 زتا بایت بوده است و در سال 2025 ، به حدود 175 زتا بایت خواهد رسید.

کامپیوتر کوانتومی؟

کامپیوترهای کوانتومی به دلیل اینکه در لحظه تمام حالات پاسخ یک سوال را در خود دارند به میزان حافظه‌ی بسیار کمتری احتیاج دارند، چرا که در یک کامپیوتر معمولی چنین پردازش‌هایی ملزم اختصاص یک فضای جداگانه به هر راه‌حل است، در حالی که کامپیوتر کوانتومی تمام حالات پاسخ را به طور همزمان در کیوبیت‌های خود نگهداری می‌کند.

کامپیوترهای کوانتومی چگونه کار می‌کنند؟



- طبق توضیحات بالا در می‌یابیم که یک کامپیوتر کوانتومی تمام راه‌حل‌های یک مسئله را در آن واحد درون کیوبیت‌های خود دارد، فقط کافیست مقدار این کیوبیت‌ها در لحظه‌ی درست خوانده شود تا به جواب مسئله برسیم.
- کامپیوتر کوانتومی برای یک مساله خاص باید برنامه ریزی شود.

- برای اینکه بتوانیم کیوبیت‌های یک کامپیوتر کوانتومی را به وجود آوریم لازم است تا کامپیوتر در شرایط دمایی نزدیک به صفر مطلق نگهداری گردد تا بیت‌های سخت‌افزاری دارای خاصیت کوانتومی شوند.
- بنابراین فعلا نمی‌توان کامپیوترهای کوانتومی را مانند کامپیوترهای معمولی در خانه و محل کار استفاده کرد، این کامپیوترها معمولا در شرایط آزمایشگاهی و با اهداف علمی و پژوهشی استفاده می‌شوند، هرچند هنوز کامپیوترهای کوانتومی خیلی قدرتمندتر از کامپیوترهای معمولی نیستند، اما این فناوری به سرعت در حال پیشرفت بوده و به زودی دنیای جدیدی به روی ما گشوده خواهد شد، در حال حاضر شرکت‌هایی مانند گوگل، IBM و مایکروسافت در حال کار روی پردازش کوانتومی هستند.

پردازش‌های کوانتومی تا چه حد قابل اطمینان هستند؟

یکی از چالش‌هایی که در حال حاضر پیش‌روی رایانه‌های کوانتومی قرار دارد، مشکل عدم اطمینان به پاسخ آن‌هاست، ساز و کار تصحیح خطا در کامپیوترهای کلاسیک به این صورت است که معمولا بیت‌های اضافه‌ای برای بررسی خطای بیتی و در صورت نیاز تصحیح آن‌ها در نظر گرفته می‌شود، اما این ساز و کار در کامپیوترهای کوانتومی امروزی قابل اجرا نیست، چرا که برای افزودن بیت‌های تست خطا چیزی حدود 2000 کیوبیت مورد نیاز است، در حالی که در حال حاضر قوی‌ترین کامپیوترهای کوانتومی موجود چیزی در حدود 100 کیوبیت در پردازنده‌های خود دارند!

خطرات پردازش‌های کوانتومی

- همانطور که گفتیم کامپیوترهای کوانتومی در یک لحظه تمام حالات یک مسئله را در خود دارند، حال فرض کنید از این قدرت برای شکستن رمزهای عبور و پروتکل‌های رمزنگاری استفاده شود، چراکه یک کامپیوتر کوانتومی در لحظه تمام رمزهای موجود را در خود دارد، تنها کافیست رمز صحیح در یک لحظه انتخاب شود!
- به همین دلیل بسیاری از دولت‌ها در حال رقابت در این زمینه هستند، در حقیقت اولین کسی که بتواند به تکنولوژی رایانش کوانتومی دست پیدا کند قادر است تمام پسوردهای جهان را یافته و از هر قفلی عبور کند!
- رمزنگاری حساب‌های کاربری، پروتکل‌های امنیتی شبکه، انتقال داده‌ها و... همه و همه با خطر رو به رو خواهند شد، البته مراکز امنیتی نیز بیکار ننشسته و در حال تلاش برای حل این مشکلات هستند، آن‌ها سعی می‌کنند سیستم رمزنگاری ایجاد کنند که بتواند در برابر کامپیوترهای کوانتومی مقاومت کند.

مروری بر مفاهیم سرعت در کامپیوترها

- فلاپس FLOPS واحد اندازه‌گیری سرعت پردازش داده‌ها توسط رایانه است.
- سرعت ابررایانه بر اساس FLOPS محاسبه می‌شود که مخفف تعداد عملیاتی است که پردازنده میتواند روی اعداد اعشاری در هر ثانیه انجام دهد
- معمولاً هم یک پسوند مثل ترا یا پتا با آن همراه است.
- در صورت ترا بودن آن را TFLOPS ترافلاپ ده به توان دوازده (FLOP(1012 و در حالت پتا بودن PFLOPSپتافلاپ ده به توان پانزده (10^{15})می‌گویند.
- به عبارت دیگر اگر سرعت پردازش یک کامپیوتر 1 ترا فلاپ باشد ، این کامپیوتر میتواند در هر ثانیه 10 به توان 12 دستورالمعل را در ثانیه انجام دهد.
- سرعت ابر کامپیوتر Summit شرکت IBM معادل 200 PFLOPS است. معادل $200 * 10^{15}$ عملیات در هر ثانیه است. لازم به ذکر است که این کامپیوتر قوی ترین ابر کامپیوتر جهان در حال حاضر میباشد.
- شرکت گوگل ادعا نموده است که برای حل مسئله ای که توسط Summit به 10000 سال زمان نیاز داشت از کامپیوتر کوانتومی گوگل استفاده شده که تنها در 3 دقیقه مسئله را حل کرده است.
- یعنی تقریبا سرعت کامپیوتر کوانتومی 2 میلیارد(109 *2) بار بیشتر از سرعت کامپیوتر های معمولی است.

سرعت محاسبات برحسب FLOPS	نوع کامپیوتر
$2 * 10^{24}$	کامپیوتر کوانتومي
10^{15}	سوپر کامپیوترهای کلاسیک

یک مثال : پیدا کردن یک عدد در لیستی از اعداد

- 0000 = 0
- 0001 = 1
- 0010 = 2
- 0011 =3
- 0100 = 4
- 0101 = 5
- 0110 = 6
- 0111 = 7
- 1000 = 8
- 1001 = 9
- 1010 = 10
- 1011 = 11
- 1100 = 12
- 1101 = 13
- 1110 =14
- 1111 =15

یک مثال : پیدا کردن یک عدد در لیستی از اعداد

- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx

یک مثال : پیدا کردن یک عدد در لیستی از اعداد

- 0xxx
- 0xxx
- 0xxx
- 0xxx
- 0xxx
- 0xxx
- 0xxx
- 0xxx
- 1xxx
- 1xxx
- 1xxx
- 1xxx
- 1xxx
- 1xxx
- 1xxx
- 1xxx

مثال : پیدا کردن یک رمز عبور 8 کاراکتری - بدون هیچ کد گذاری

- تعداد حالتهای یک رشته 8 کاراکتری که رمز را در خود نگه دارد ، عدد زیر میباشد
- 8 به توان 256 = 18446744073709551616 حالت
- زمان لازم برای انجام عملیات با تعداد فوق در کامپیوتر سامیت IBM حدود 5 ساعت میباشد.
- زمان لازم برای انجام عملیات با تعداد فوق در کامپیوتر کوانتومی گوگل حدود 0.000009 ثانیه که معادل حدود 9 میکرو ثانیه میباشد. حدود 2 میلیارد بار سریعتر از سوپر کامپیوتر جهان

- فرمول پیدا کردن رمز درست در کامپیوترهای معمولی معادل n/2 حالتها است که صرف مرتب کردن حالتها بر اساس صعودی میشود.
- فرمول پیدا کردن رمز در کامپیوترهای کوانتومی معادل جذر n میباشد. که صرف مسیریابی بین احتمالی بین 0 و 1 ها خواهد شد.

منابع

- https://www.nature.com/articles/s41586-019-1666-5#Sec4
- https://www.scientificamerican.com/article/what-makes-a-quantum-comp/
- https://www.scientificamerican.com/article/what-makes-a-quantum-comp/