بسم الله الرحمن الرحيم

٤٧٢١٧

دانشگاه سیستان و بلوچستان

تحصیلات تکمیلی

یک مدار جمع کننده در کامپیوتر های کوانتومی

نگارش:

فیروز امیری ۱۳۸۲/۶/۱

مرکز اطلاعات و مدارک علمی ایران
تهیه مدارک ۱۳۸۲/۶/۱

پایان نامه ی کارشناسی ارشدفیزیک

استاد راهنما :

دکتر وحید کریمی پور

۴۲۱۷

بسمه تعالی

صفحه الف

این پایان‌نامه با عنوان ***یک مدار جمع‌کننده در کامپیوترهای کوانتومی*** قسمتی از برنامه آموزشی دوره کارشناسی ارشد ***فیزیک*** گرایش ***حالت جامد*** توسط دانشجو ***فیروز امیری*** تحت راهنمائی استاد پایان‌نامه آقای ***دکتر وحید کریمی‌پور*** تهیه شده است. استفاده از مطالب آن بمنظور اهداف آموزشی با ذکر مرجع و اطلاع کتبی به حوزه تحصیلات تکمیلی دانشگاه سیستان و بلوچستان مجاز می‌باشد.٪

امضاء دانشجو

این پایان‌نامه ۶ (شش) واحد درسی شناخته می‌شود و در تاریخ ۸۲/۳/۲۸ توسط هیئت داوران بررسی و نمره ۱۸/۵ با درجه عالی به آن تعلق گرفت.٪

	نام و نام خانوادگی	امضاء	تاریخ
۱ـ استاد راهنما:	***دکتر وحید کریمی‌پور***		۸۲/۳/۲۸
۲ـ استاد مشاور:	---		
۳- داور ۱:	***دکتر محمدرضا رحیمی‌تبار***		۸۲/۳/۲۸
۴ـ داور ۲:	***دکتر حسین حکیمی پژوه***		
۵ـ تحصیلات تکمیلی:	***دکتر محمدنبی گرکیج***		۸۲/۳/۲۸

قدر دانی

باسپاس فراوان از ؛

درگاه خداوند حکیم به خاطر الطاف نهان وآشکارش به من، در طول نوشتن این پایان نامه

استاد ارجمندم،جناب آقای دکتر وحید کریمی پور،استاد فیزیک از دانشگاه صنعتی شریف که مرا با الفبای تحقیق آشنا نمودند،

جناب آقای دکترولیزاده ریاست محترم تحصیلات تکمیلی وهمکارانش دردانشکده ی علوم که دلسوزانه دفاعیه این پایان نامه را پی گیری کردند،

پدرومادر عزیزم که با دسترنج خودشان امکان ادامه تحصیل را برایم فراهم کردند،

خانواده ی همسرم که در این مدت مرا یاری نمودند،

همسر عزیزم که شروع این پایان نامه مقارن با آغاز زندگی مشترکمان بود و نگارش این تحقیق بدون کمک او شاید غیر ممکن بود.

چکیده

با کوچکتر شدن روز افزون اجزاء کامپیوتر، به زودی زمانی فراخواهد رسید که فاصله بین دو تا از سلولهای حافظه اینقدر کوچک خواهد شد که برای توصیف رفتار این دو سلول حافظه ناچار خواهیم بود؛ از قوانین مکانیک کوانتومی استفاده کنیم. این بدان معناست که باید، ثبت اطلاعات ، خواندن اطلاعات، محاسبات منطقی و الگوریتم ها را با نحوه ی رفتار مکانیک کوانتومی سازگارکنیم.در حد کلاسیک عنصر اصلی حافظه یعنی بیت می تواندر یکی از دو حالت 0 یا 1 باشد. ولی واحد اطلاع کوانتومی که به آن اصطلاحا"((کیو بیت)) می گویند، یک سیستم میکروسکوپی نظیر اسپین یک هسته اتمی ، یا قطبش یک فوتون است و در نتیجه، با یک بردار در یک فضای هیلبرت دو بعدی با پایه های $|0\rangle$و$|1\rangle$ توصیف می شود. بنابر این، یک کیو بیت می تواند در ترکیبی خطی از حالتهای $|0\rangle$و$|1\rangle$ نیز قرار گیرد.در این پایان نامه با معرفی جبر بول دو ارزشی و دروازه های منطقی کلاسیک، ابتدا به جمع دو عدد n رقمی با کمک جدول درستی و توابع منطقی بول و مدارهای جمع کننده می پردازیم ، سپس با تعریف اصول اساسی کامپیوترهای کوانتومی از منظری مشابه روش کلاسیک اما به شیوه ای کوانتومی،به توصیف و طراحی مدارهای جمع کننده ی کوانتومی خواهیم پرداخت.

واژه های کلیدی: کیوبیت، دروازه، توازی کوانتومی، الگوریتم کوانتومی.

فهرست مندرجات

مقدمه ٦

۲- مقدمه ای بر جبر بول و مدارهای منطقی کلاسیکی ۱۳

۲ -۱ تعریف اصول جبر بول ۱۳

۲ -۱-۱ مقایسه جبر بول با جبر معمولی ١٤

۲-۱-۲ تعریف منطق دو دویی ۱۵

۲-۲ قضیه های اصلی و خواص جبر بول ۱۷

۲-۳ دروازه های منطقی ۱۸

۲-٤ دروازه های کلی ۲۱

۳- محاسبات برگشت پذیر ۲۳

۳-۱ مقدمه ۲۳

۳-۲ برگشت پذیر کردن یک تابع دلخواه ٢٤

۳-۳ دروازه های برگشت پذیر ۲۵

۳ -۳-۱ دروازه یXOR ۲۵

۳-۳-۲ دروازه ی توفولی ۲۷

مرکز اطلاعات و مدارک علمی ایران
تهیه مدارک

۳-٤ معکوس پذیر کردن دروازه هایAND, NAND , OR ۲۹

۳-٤-۱ AND معکوس پذیر ۲۹

۳-٤-۲NAND معکوس پذیر ۲۹

۳-٤-۳ OR معکوس پذیر ۳۰

۳-۵ ساخت تابع معکوس پذیر n بیتی با استفاده از $\theta^{(3)}$ و دروازه NOT ۳۰

۳-٦ خواص XOR ۳۳

٤- اصول اساسی محاسبات کوانتومی ۳٤

٤-۱ مقدمه ۳٤

٤ -۲ کیو بیت ۳٤

٤ -۲-۱ کیوبیت چند گانه ۳٦

٤-۳ دروازه ی کوانتومی ۳۸

٤-۳-۱دروازه ی تک کیوبیتی ۳۸

٤-۳-۲ دروازه های چند کیو بیتی ٤۳

٤-٤ توازی کوانتومی ٤٦

٤-۵ الگوریتمهای کوانتومی ٤۸

٤-۵-۱ الگوریتم دویچ ٤۹

٤-٥-٢ الگوریتم دویچ- جوزا ٥١
٤-٥-٣ الگوریتم سیمون ٥٦
٤-٥-٤ الگوریتم گرور ٥٩
٤ -٥-٤-١دروازه ی تبدیل وارونگی در حدود میانگین ٦٤
٤-٥-٥ الگوریتم شور ٦٦
٤-٥-٥-١ الگوریتم محاسبه پرید ٦٨
٤-٥-٥-٢ تبدیل فوریه کوانتومی ٧١

٥ – مدارهای جمع کننده ی کلاسیک ٧٧

٥-١ مقدمه ٧٧
٥-٢ جمع کننده ها ٧٨
٥-٢-١ نیم جمع کننده ی (HA) ٧٨
٥-٢-٢ تمام جمع کننده ی(FA) ٧٩
٥-٣جمع دو عدد یک رقمی ٨١
٥-٤جمع دو عدد دو رقمی ٨٢
٥-٥جمع دو عدد n رقمی ٨٥

٦- مدارهای جمع کننده ی کوانتومی ٨٧

٦-١ مقدمه ٨٧

٦-٢ روش طراحی مدارهای جمع کننده ی کوانتومی ٨٨

٦-٣ مدارهای عددی ٨٩

٦-٣-١دروازه ی تمام جمع کننده ی(SUM) ٩٠

٦-٣-٢ دروازه ی حامل(CARRY) ٩١

٦-٤ جمع دو عدد یک رقمی به روش کوانتومی ٩٢

٦-٥ جمع دو عدد دو رقمی به روش کوانتومی ٩٣

٦-٦ جمع دو عدد n رقمی به روش کوانتومی ٩٥

٦-٦-١ طراحی مدار کوانتومی جمع کننده ی دو عدد n رقمی ٩٦

٧- مدارهای جمع کننده ی پیمانه ای ١٠١

٧-١ مقدمه ١٠١

٧-٢مباحث مقدماتی نظریه اعداد ١٠٢

٧-٢-١ بخشپذیری ١٠٢

٧-٢-٢ همنهشتی ١٠٢

٧-٣ دروازه ی تفریق کننده ١٠٤

٧-٤ طراحی مدارهای جمع کننده ی پیمانه ای ١٠٥

۷-۵ نتیجه گیری ۱۱۰

کتابنامه ۱۱۱

فصل ۱
مقدمه

بدون تردید یکی از دستاوردهای شگرف بشر در قرن بیستم میلادی ابداع کامپیوتر بود. کامپیوترها بسیاری از پیشرفت های علمی ، صنعتی وتجاری را که به صورت دیگرقابل دسترسی نبودند، ممکن ساخته اند . طرح های فضایی، امروزه بدون نظارت دائمی و بلا درنگ کامپیوتر غیر ممکن بوده و نیز بسیاری از اعمال مهم تجاری بطور موثر تنها به کمک پردازش خودکار داده ها میسر می باشد . کامپیوتر ها در محاسبات عملی ، پردازش داده های تجاری ، کنترل ترافیک هوایی ، هدایت فضایی، زمینه های فرهنگی و موارد بسیار دیگر مورد استفاده قرار گرفته اند.اولین نسل کامپیوترها در هیبتی غول آسا با قابلیت های محاسباتی پایین وارد زندگی مردم شد.با گذشت زمان این ماشین غول پیکر که جزء اصلی آن لامپ خلاء بود دستخوش دگرگونی های زیاد شد که مهمترین آنها جایگزینی ترانزیستور بجای لامپ خلاء بود. با ورود ترانزیستور در ساختار کامپیوتر، این ماشین محاسباتی ازیک طرف روزبه روزکوچکتر شد،بطوری که پردازش- گرهای امروزی بقدری کوچک شدند که قادرند از سوراخ یک سوزن در حدود ٦ میلی متر عبور کنند،از طرف دیگر،قابلیت انجام محاسبات آنها بطورخارق العاده ای زیادشده تا جائیکه ابرکامپیو ترهای

امروزی قادر به انجام ۱۰۰ میلیون محاسبه در ثانیه شدند . سوالی که برای دانشمندان امروزی علم کامپیوتر مطرح است این است که آیا کوچکتر شدن کامپیوترها در طول این چند دهه گذشته و در آینده از قانون خاصی پیروی می کند ؟

جواب این چند سوال از نظر این دانشمندان مثبت است بطوریکه آنهادریافتندتاکنون روند کوچک شدن کامپیوترها یا به عبارتی تراشه ها از یک قانون تجربی بنام قانون مور[۱] پیروی می کند طبق قانون مور، قدرت ذخیره سازی سلول حافظه به ازای هر دو سال دو برابر می شود، و اگر این روند ادامه یابد، طبق این قانون در سال ۲۰۲۸ میلادی سلولهای حافظه این قدر کوچک خواهند شد که می توان ۱۶ هزار CD فعلی را روی یک CD آن زمان ذخیره کرد واین یک تحول اعجاب انگیز درنوع خود می باشد.سئوالی که اینجا پیش روی دانشمندان است،این است که آیا با این روندکوچک شدن کامپیوتر به همراه بالا رفتن سرعت انجام محاسبات آن در دهه های آینده می توان تمام مسائل سخت[۱]،[۲]،[۳]،[٤]علوم مختلف از جمله علم فیزیک ، ریاضی و بیو لوژیک و .... را بوسیله کامپیوترهای قدرتمند حل کرد ؟

جواب این سئوال منوط به معیاری است که مسائل سخت و آسان را تعریف می کند[٥]،[٦]. این معیار از نظر دانشمندان کامپیوتر به نام پیچیدگی زمانی معروف است .برای حل یک مسئله با برنامه نویسی یک الگوریتم و یک سایز داریم ،آن دسته از مسائل که زمان حل آنها نسبت به

۱- Moor's Law

سایز مسئله نسبت توانی باشد، مسائل آسان یا مسائل نوع P[۱] نامیده می شوند، مانند:

معکوس کردن یک ماتریس n×n که سایز آن n است و زمان لازم برای حل آن $T(n)=n^3$ است. درمقابل مسائلی که زمان حل آنها نسبت به سایزمسئله بطورنمایی رشدکند(مانند، $T(n)=2^n$)مسائل سخت یامسائل نوع NP[۲]نامیده می شوند. نمونه ای این نوع مسائل سخت پیدا کردن فاکتور های اول یک عدد خیلی بزرگ می باشد.

با ادامه روند کوچک شدن کامپیوتر ها طبق قانون مور، پیش بینی می شود،در سال ۲۰۲۰ میلادی فاصله بین دو تا از سلول های حافظه اینقدر کوچک خواهد شد، که برای توصیف رفتار این دو سلول حافظه بایستی از قوانین مکانیک کوانتومی استفاده کنیم[۷]،[۸]،[۹]،[۱۰].بنابراین، بعد از اعمال قوانین مکانیک کوانتومی، باید ثبت اطلاعات ، خواندن اطلاعات نحوه محاسبه و الگوریتم ها[۱۱]،[۱۲]،[۱۳]،[۱٤] را با نحوه رفتار مکانیک کوانتومی سازگار کنیم[۱۵]،[۱٦] .

پیامد این پدیده جایگزین شدن کامپیوترهای کوانتومی $(Q.C)^3$ با کامپیوترهای کلاسیک می باشد [۱۷] ،[۱۸] .

در کامپیوترهای کلاسیک، عنصر اصلی حافظه یعنی بیت کلاسیکی (bit) ،در یکی ازحالتهای ۰ یا ۱ است .

۱- Polynomial

۲- Nonpolynomial

۳- Quantum computer

در کامپیوترهای کوانتومی عنصر اصلی حافظه کیوبیت(qubit) است،که یک سیستم کوانتومی دو بعدی در فضای هیلبرت می باشد.کیوبیت بر خلاف بیت کلاسیکی علاوه بر انتخاب یکی از حالت های کوانتومی $|0\rangle$ یا $|1\rangle$می تواند در ترکیبی از دو حالت $|0\rangle$و$|1\rangle$قرار گیرد.سلول حافظه ممکن است آنقدر کوچک شد ه باشد که نقش آن را یک اتم یا فوتون یا اسپین هسته ایفا کند [۱۹]،[۲۰]، در حالیکه امروزه در کامپیوتر های کلاسیکی تعداد بی شماری ازاتم ها این کار را انجام می دهند.

کیو بیت یک حالت کوانتومی است و برای تغییر آن دروازه ی کوانتومی[۱] مورد نیاز است،اما بنابر قوانین مکانیک کوانتومی تحول حالتهای کوانتومی توسط عملگر های یکایی صورت می گیرد.بنابراین،باید دروازه های کلاسیکی برگشت ناپذیر همچون NAND ، OR وAND به عملگر های یکایی تبدیل شوند [۲۱]،[۲۲] .

شگفتی کامپیوتر های کوانتومی در خلق ترکیب خطی حالتها به همراه عنصر احتمال است.بنابراین، کامپیوتر کوانتومی قادر به تحول دو حالت یا بیشتر به طور هم زمان می باشد ،که این پدیده به نام توازی کوانتومی[۲] معروف است. توازی کوانتومی که خود نقش اساسی در طرح الگوریتم های کوانتومی[۳] ایفا می کند، رایانه های کوانتومی را قادر می سازد، تا با پذیرفتن تعداد زیادی ورودی

---

۱) Quantum gate

۲) Quantum paralleism

۳) Quantum algorithms

در قالب یک حالت ، فقط با یک مرتبه عمل کردن خروجی های متناظر با این ورودیها را ، در اختیار ما قرار دهد . به این ترتیب رایانه های کوانتومی با سرعت و قابلیت فوق العاده ی خود چشم اندازهای جدیدی را به روی دانشمندان می گشایند.

در سالهای اخیرامکان ساخت یک کیو بیت و حتی هفت کیوبیت و یک دروازه کوانتومی در آزمایشگاه ، توسط پژوهشگران تجربی فراهم شده است . واز لحاظ تئوری تا کنون دوکشف مهم صورت گرفته است .

کشف اول ،الگوریتم شور[۱] (۱۹۹٤)است که یک الگوریتم کوانتومی نوعP برای تجزیه اعداد صحیح وپیدا کردن لگاریتم روی یک میدان متناهی می باشد[۲۳] .برای این دو مسئله بهترین الگوریتم های کلاسیکی شناخته شده ازنوعNP می باشد.نتایج الگوریتم شور توجه فوق العاده ای در میان دانشمندان نظری وتجربی همراه خود ساخت،چراکه مسئله سخت تجزیه اعدادبزرگ تا آن روز در شمارمسائل نوعNP بودوقلب سیستم های رمزنگاری همچون RSA [۲٤]،[۲۵] به شمار می رفت.

کشف دوم،الگوریتم جستجوی گرور[۲]می باشد.گروردرسال۱۹۹۵یک الگوریتم جستجوی کوانتومی ارائه کرد[۲٦]،که قادر بود یک داده را درمیان پایگاهی بهم ریخته از داده هابه اندازه N[کهN خیلی بزرگ است] با $\sqrt{N}$ مرتبه عملیات پیدا کند،در حالیکه این جستجو بابهترین

---

۱) Shor's Algorithm

۲) Grover's Search Algorithm