
بسم الله الرحمن الرحیم

پایان‌نامه دکترای مهندسی برق

تحقق‌پذیری کارآمد کدهای کانولوشنال کوانتومی

منیره هوشمند

استاد راهنما: دکتر سعید حسینی خیاط

بهار ۱۳۹۰

تقدیم به مادر

و پدرم

و تقدیم به همسرم

من به سر چشمه خورشید نه به خود بردم راه ذره‌ای بودم و مهر تو مرا بالا برد

تشکر و قدردانی

منت خدای را عزّ و جل که طاعتش موجب قربت است و به شکر اندرش مزید نعمت

در اینجا لازم می‌دانم از راهنمایی‌ها و حمایت‌های استاد بزرگوارم، جناب آقای دکتر سعید حسینی خیاط قدردانی و تشکر نمایم. این رساله جز در سایه آموخته‌های ایشان هرگز میسر نمی‌شد. همچنین از جناب آقای دکتر محسن سربیشه‌ای، جناب آقای دکتر علی پیروی، جناب آقای دکتر مرتضی صاحب‌الزمانی، جناب آقای دکتر مهدی صدیقی و جناب آقای دکتر کیوان ناوی که داوری این رساله را قبول کردند، سپاسگزاری می‌نمایم.

از همراهان همیشگی‌ام در طول زندگی، پدر، مادر، برادر و خواهرم، به دلیل حمایت‌ها و محبت-های بی‌دریغشان، تشکر می‌کنم. از پدر و مادر همسرم که راهنمایی‌ها و دعای خیرشان همواره بدرقه راهم بوده است، قدردانی می‌نمایم. از همسر عزیزم که در طول دوره دکتری، مشوق و حامی اینجانب بوده و موفقیت من را همچون موفقیت خود می‌دانست، صمیمانه تشکر می‌کنم.

در انتها از مرکز تحقیقات مخابرات ایران به دلیل حمایت این رساله تشکر می‌نمایم.

چکیده

علی‌رغم قدرت نظری سیستم‌های کوانتومی در زمینه پردازش و ارسال اطلاعات، یک مانع بزرگ در مسیر تحقق عملی آن‌ها وجود دارد و آن برهم‌کنش سیستم کوانتومی با محیط بیرون است که منجر به تغییر ناخواسته اطلاعات می‌شود. برای غلبه بر مشکل مذکور، کدهای تصحیح خطای کوانتومی طراحی شده‌اند. یک دسته خاص از این کدها، کدهای کانولوشنال کوانتومی می‌باشند که بر حسب نحوه طراحی به دو دسته کدهای CSS (Calderbank-Shor-Steane) و non-CSS تقسیم می‌شوند. علیرغم اهمیت فراوان کدهای کانولوشنال در تصحیح خطا، فقدان یک مدار کدگذار با قابلیت تحقق‌پذیری عملی، مانعی جدی در بهره‌گیری از این کدها می‌باشد. سه پارامتر در طراحی مدارهای کدگذار کانولوشنال اهمیت دارد: پارامتر اول، میزان حافظه مصرفی کدگذار است؛ زیرا کاهش حافظه باعث کاهش سربار سخت‌افزاری و افزایش سرعت الگوریتم کدبرداری می‌شود. پارامتر دوم غیرمخرب بودن کدگذار است، تا تعداد محدودی از خطاهای تصحیح نشده به تعداد نامحدودی از کیوبیت‌های اطلاعات منتقل نشود و آخرین پارامتر تعداد سطوح مدار است که با زمان تاخیر کدگذاری کیوبیت‌ها ارتباط مستقیم دارد.

از دیدگاه نظری، دو نوع ساختار برای کدگذارهای کدهای کانولوشنال وجود دارد که به ساختارهای استاندارد و ساختارهای pearl-necklace موسوم می‌باشند. اما کدگذارهای pearl-necklace قابلیت تحقق‌پذیری عملی را ندارند؛ زیرا به منابع نامحدود حافظه نیاز دارند. Grassl و Rotteler الگوریتمی برای کدگذاریِ کدهای کانولوشنال ارائه داده‌اند. این الگوریتم در ابتدا فقط برای کدگذاری کدهای CSS طراحی شده بود، ولی در ادامه الگوریتم دیگری برای کدگذاری کدهای non-CSS نیز، توسط Grassl و Rotteler پیشنهاد گردید. کدگذار حاصل از هر دو الگوریتم در ساختار pearl-necklace بوده که قابلیت تحقق‌پذیری عملی را ندارد. در این رساله، برآنیم که شکاف بین نمایش نظری و پیاده‌سازی عملی این کدگذارها را بیابیم. به این منظور، ابتدا الگوریتمی

برای تغییر ساختار کدگذارهای pearl-necklace برای کدهای CSS به کدگذارهای استاندارد ارائه می‌دهیم. سپس الگوریتم را توسعه داده تا بتوان پیاده‌سازی عملی کدگذارهای پیچیده‌تر pearl-necklace برای کدهای non-CSS را نیز به دست آورد. بررسی‌های انجام شده در این رساله نشان می‌دهد که چندین تحقق عملی با میزان حافظه مصرفی متفاوت برای یک کدگذار pearl-necklace مشخص وجود دارد، که الگوریتم ارائه شده در این رساله تحقق عملی با کمینه حافظه را می‌یابد. لازم به ذکر است که پیچیدگی این الگوریتم، بر حسب پارامترهای کد، چند جمله‌ای است.

از طرف دیگر، برای یک کد کانولوشنال مشخص، چندین کدگذار وجود دارد که الگوریتم Grassl-Rotteler تنها یکی از آنها را می‌یابد. شروع از یک کدگذارِ حاصل از الگوریتم Grassl-Rotteler و یافتن تحقق عملی آن کدگذار با کمینه حافظه به کمک الگوریتم ارائه شده در این رساله، لزوماً منجر به کدگذار با کمینه حافظه برای کد مفروض نمی‌شود؛ زیرا ممکن است کدگذارهای دیگر میزان حافظه کمتری نیاز داشته باشند. از طرف دیگر پیچیدگی نمایی الگوریتم Grassl-Rotteler برای کدهای non-CSS منجر به تعداد نمایی سطوح کدگذار بر حسب پارامترهای کد می‌شود. در ادامه رساله، الگوریتم نوینی برای کدگذاری غیرمخرب کدهای کانولوشنال ارائه می‌شود که بر مشکلات ذکر شده غلبه می‌کند. رهیافت به کار گرفته شده در این الگوریتم، کاملاً متفاوت از الگوریتم Grassl-Rotteler بوده و کدگذار حاصل، مستقیماً در ساختار استاندارد است و در بین تمامی کدگذارهای کد مفروض، میزان کمینه حافظه را مصرف می‌کند. تعداد سطوح مدار بر حسب پارامترهای کد دارای پیچیدگی چند جمله‌ای است.

کلمات کلیدی: محاسبات کوانتومی، کدهای کانولوشنال کوانتومی، مدارهای کدگذار با کمینه حافظه.

فهرست مطالب

فهرست جداول

فهرست اشکال

فصل ۱-

مقدمه

افزایش روزافزون نیازهای بشر برای پردازش اطلاعات با سرعت بالاتر منجر به ساخت تراشه‌های (پردازنده‌های) سریع‌تر و پیچیده‌تر شده است. برای ایجاد این تراشه‌ها، لازم است که تعداد ترانزیستورهای بیشتری بر روی تراشه تعبیه شود. طبق قانون Moore [۱]، تعداد ترانزیستورهای روی یک تراشه (با مساحت ثابت) تقریباً هر دو سال، دو برابر خواهد شد. این رشد نمایی که در سال ۱۹۶۵ پیش‌بینی شده بود تاکنون ادامه داشته است. با برون‌یابی قانون Moore، در سال ۲۰۲۰ اندازه ترانزیستوری که بر روی تراشه‌های سیلیکونی می‌بایست تعبیه شود، به اندازه یک اتم خواهد رسید [۲, ۳]. چالشی که در آن زمان رخ خواهد داد این است که در ابعاد اتمی، قوانین فیزیکی که بر رفتار اتم‌ها حاکم هستند، قوانین مکانیک کوانتومی هستند و نه قوانین مکانیک کلاسیک. در این صورت پیش‌بینی‌های کلاسیک، در اثر رفتار کوانتومی ذرات، نامعتبر خواهند شد. در صورتی که برای کنترل این مشکل تدبیری اندیشیده نشود، قطعات تولید شده به درستی عمل نخواهند کرد [۴]. مانع دیگر در دستیابی به کاهش نمایی اندازه ترانزیستور، موانع اقتصادی می‌باشد. طبق قانون دوم Moore، هزینه ساخت تراشه‌ها نیز با زمان رشد نمایی خواهد داشت [۴].

بنابراین بسیاری از متخصصان در زمینه‌های مختلف پیشاپیش به فکر رفع این مشکل افتادند. به این ترتیب بود که در سال ۱۸۹۲، دانشمندان پیشنهاد کردند که باید محاسبات را از دنیای کلاسیک کنونی وارد دنیای جدید کوانتومی کرد که بسیار متفاوت از قبلی بوده و نه تنها مشکلات گذشته و محدودیت‌های موجود را بر طرف می‌سازد، بلکه افق‌های جدیدی را نیز به این مجموعه اضافه می‌کند [۵]. در واقع، هدف محاسبات کوانتومی یافتن روش‌هایی برای طراحی مجدد قطعات به گونه‌ای است که بتوانند تحت اثرات کوانتومی، که در محدوده ابعاد نانومتری و کوچک‌تر بروز می کنند، به خوبی کار کنند [۶-۸]. پس از کشف الگوریتم‌های کوانتومی که قادر هستند مسائل محاسباتی سنگین را بسیار سریع‌تر از الگوریتم‌های کلاسیک حل کنند، توجه ویژه‌ی دانشگاه‌ها و سرمایه‌گذاری‌های کلان

صنایع به این زمینه نوظهور جلب شد. به عنوان نمونه‌ای از این الگوریتم‌ها، می‌توان به امکان تجزیه سریع اعداد بزرگ [۹] و جستجوی سریع در یک مجموعه تصادفی [۱۰] اشاره کرد.

علی‌رغم قدرت نظری سیستم‌های کوانتومی، یک مانع بزرگ در مسیر تحقق عملی آن‌ها وجود دارد و آن برهم‌کنش سیستم کوانتومی با محیط بیرون است که منجر به تغییر ناخواسته اطلاعات می‌شود. در ابتدا پژوهشگران بر این باور بودند که سیستم‌های قابل اطمینانی برای محاسبه و ارسال کوانتومی محقق نخواهند شد؛ زیرا خطاهای کوچک کوانتومی در خلال یک محاسبه کوانتومی انباشته شده و همچنین نویز کانال، اطلاعات کوانتومی ارسالی را تخریب خواهد کرد [۱۱]. قضیه عدم کپیِ اطلاعات کوانتومی [۱۲] و از دست رفتن اطلاعات پس از اندازه‌گیری کیوبیت‌ها [۲, ۳]، موانع بزرگی بر سر راه طراحی کدهای کوانتومی به نظر می‌رسیدند.

علی‌رغم موانع مذکور، در سال ۱۹۸۴، Shor توانست اولین کد تصحیح خطا برای محافظت از یک کیوبیت [۱۳] را طراحی کند. کد Shor بر تمام موانع بالا غلبه کرده و از بسیاری از اصول مکانیک کوانتومی همانند برهم‌نهی[1]، درهم‌تنیدگی[2]، عملگر یکانی[3] و اندازه‌گیری[4]، برای تصحیح خطا بهره می‌گیرد. پس از آن به سرعت، نظریه تصحیح خطای کوانتومی، زمینه مهمی برای پژوهش شد. در سال ۱۹۹۷، با کشف کدهای تثبیت‌گر کوانتومی[5] [۱۴]، تحولی شگرف در زمینه نظریه تصحیح خطای کوانتومی رخ داد. به کمک نظریه تثبیت‌گر، می‌توان از دو کد کلاسیک، برای طراحی یک کد کوانتومی بهره گرفت. این دسته خاص از کدهای تثبیت‌گر، به کدهای CSS[6] موسوم می‌باشند.

---

[1] Superposition
[2] Entanglement
[3] Unitary Transformation
[4] Measurement
[5] Quantum Stabilizer Codes
[6] Calderbank-Shor-Steane

از نقطه نظر روش کلی کدگذاری[۱]، کدهای تصحیح خطای تثبیت‌گر، به دو دسته کدهای بلوکی[۲] و کدهای کانولوشنال[۳] تقسیم می‌شوند [۱۴, ۱۵]. در کدهای بلوکی، رشته کیوبیت ارسالی به دسته‌هایی با طول یکسان تقسیم می‌شود. سپس هر دسته به طور مستقل از سایر دسته‌ها کدگذاری می‌شود؛ بنابراین کدهای بلوکی کدهای بدون حافظه هستند. در مقابل، کدهای کانولوشنال کدهای حافظه‌دار هستند. بدین معنا که خروجی در هر لحظه از زمان نه تنها به ورودی‌های در همان لحظه از زمان، بلکه به ورودی‌های قبلی نیز وابسته می‌باشد. کدهای کانولوشنال نرخ کد بهتری نسبت به کدهای بلوکی دارند؛ یعنی برای محافظت تعداد کیوبیت یکسان اطلاعات، کدهای کانولوشنال کوانتومی تعداد کیوبیت کدشده کمتری نسبت به کد بلوکی کوانتومی احتیاج دارند [۱۶]. همچنین الگوریتم کدبرداری کدهای کانولوشنال نسبت به تعداد کیوبیت‌های کدشده، پیچیدگی[۴] خطی دارد [۱۵, ۱۷]، در حالی‌که الگوریتم کدبرداری کدهای بلوکی پیچیدگی نمایی دارد [۱۴].

علیرغم برتری‌های کدهای کانولوشنال، چالش اصلی در بهره‌گیری از این دسته کدها، فقدان مدار کدگذاری[۵] مناسب برای آنها است. سه پارامتر در طراحی مدارهای کدگذار کانولوشنال اهمیت دارد: پارامتر اول، میزان حافظه[۶] مصرفی کدگذار است؛ زیرا کاهش حافظه باعث کاهش سربار سخت-افزاری و افزایش سرعت الگوریتم کدبرداری[۷] می‌شود. پارامتر دوم غیرمخرب بودن[۸] کدگذار است، تا تا تعداد محدودی از خطاهای تصحیح نشده به تعداد نامحدودی از کیوبیت‌های اطلاعات منتقل نشود و آخرین پارامتر تعداد سطوح[۹] مدار است که با زمان تاخیر کدگذاری کیوبیت‌ها ارتباط مستقیم دارد. از دیدگاه نظری، دو نوع ساختار برای کدگذارهای کانولوشنال وجود دارد که به ساختارهای استاندارد

---

1 Encoding
2 Block Code
3 Convolutional Code
4 Complexity
5 Encoding Circuit
6 Memory
7 Decoding
8 Non-catastrophicity
9 Level

و ساختارهای pearl-necklace موسوم می‌باشند. اما کدگذارهای pearl-necklace قابلیت تحقق‌پذیری عملی را ندارند؛ زیرا به منابع نامحدود حافظه نیاز دارند. در مراجع [۱۸] و [۱۹]، Grassl و Rotteler به ترتیب الگوریتم‌هایی برای کدگذاری کدهای کانولوشنال CSS و non-CSS ارائه داده‌اند. کدگذار حاصل از الگوریتم Grassl-Rotteler، از نوع ساختار pearl-necklace است و بنا به توضیحات ذکر شده، در عمل قابل پیاده‌سازی نمی‌باشد. در این رساله، به کمک نظریه گراف‌ها، الگوریتم کارآمدی[1] برای پرکردن شکاف بین نمایش نظری و پیاده‌سازی عملی کدگذارهای pearl-necklace در دو حالت کدهای CSS و non-CSS ارائه می‌شود. در الگوریتم‌های ارائه شده، ساختار کدگذار pearl-necklace را به گونه‌ای تغییر می‌دهیم تا به ساختار استاندارد تبدیل شود و بتوان آن را با منابع محدود حافظه پیاده‌سازی کرد. بررسی‌های انجام شده در این رساله نشان می‌دهد که در ازای یک کدگذار pearl-necklace مشخص کدگذارهای استاندارد بسیاری وجود دارند که همان کد را محقق می‌کنند. الگوریتم ارائه شده در این رساله، کدگذار استاندارد با حافظه کمینه را می‌یابد.

برای یک کد کانولوشنال مشخص، کدگذارهای متعددی وجود دارند. اما الگوریتم Grassl-Rotteler تنها یکی از آنها را می‌یابد. شروع از یک کدگذارِ حاصل از الگوریتم Grassl-Rotteler و یافتن تحقق عملی آن کدگذار با حافظه کمینه، لزوماً منجر به کدگذار با کمینه حافظه برای کد مفروض نمی‌شود؛ زیرا ممکن است کدگذارهای دیگر میزان حافظه کمتری نیاز داشته باشند. از طرف دیگر الگوریتم Grassl-Rotteler دارای پیچیدگی نمایی بر حسب پارامترهای کد است که منجر به تعداد نمایی سطوح در کدگذار می‌شود [۱۹]. در ادامه رساله، برای حل دو مشکل مذکور با نگرشی کاملاً متفاوت از الگوریتم Grassl-Rotteler، الگوریتم نوینی برای کدگذاری کدهای کانولوشنال ارائه می‌شود. کدگذار حاصل از این الگوریتم دارای ساختار استاندارد است و در بین تمامی

[1] Efficient

کدگذارهای یک کد مشخص، میزان حافظه کمینه را مصرف می‌کند. پیچیدگی این الگوریتم بر حسب پارامترهای کد، پیچیدگی چندجمله‌ای است.

ساختار این رساله بدین قرار است: در فصل دوم، مفاهیم مقدماتی در محاسبات کوانتومی و نظریه کدگذاری به اختصار بیان شده است. در فصل سوم دو ساختار مدارهای کدگذار برای کدهای کانولوشنال معرفی می‌شوند که به ساختارهای pearl-necklace و استاندارد موسوم هستند. سپس الگوریتم کدگذاری Grassl-Rotteler برای کدهای CSS کانولوشنال کوانتومی و کدهای non-CSS به تفصیل بیان می‌شود. در فصل چهارم، مسائل حل شده در این رساله و دلایل اهمیت آنها ذکر می‌شود. فصول پنجم، ششم و هفتم نیز دربردارنده روش‌های پیشنهادی این رساله برای حل مسائل مطرح شده در فصل چهارم است، به این ترتیب که در فصول پنجم و ششم، الگوریتمی برای پیاده-سازی عملی کدگذارهای Grassl-Rotteler با کمینه حافظه به ترتیب برای کدهای CSS و non-CSS پیشنهاد می‌شود؛ و در فصل هفتم، الگوریتم متفاوتی برای کدگذاری کدهای کانولوشنال پیشنهاد شده است که نقائص الگوریتم کدگذاری Grassl-Rotteler را ندارد. جمع‌بندی رساله و پیشنهاد کارهای آتی در فصل هشتم ارائه می‌گردد.

فصل ۲-

مفاهیم مقدماتی

محاسبات کوانتومی[1] که به عنوان زمینه تحقیقاتی جدید در هزاره سوم مطرح شده است، حاصل ترکیب مکانیک کوانتومی[2]، علوم کامپیوتر و نظریه اطلاعات کلاسیک است و منجر به پیشرفت‌های شگفت‌انگیز در زمینه‌های مختلف پردازش و ارسال اطلاعات شده و خواهد شد.

هرچند هنوز کامپیوترهای کوانتومی کاملاً عملی، ساخته نشده‌اند، اما آینده کامپیوترهای کوانتومی بسیار امیدوار کننده به نظر می‌رسد. مهم‌ترین مانع در ساخت سیستم‌های کوانتومی، *ناهمدوسی*[3] (به معنای به هم ریختگی حالت کوانتومی در نتیجه برهم‌کنش با محیط) است. برای حل این مشکل، کدهای تصحیح خطای کوانتومی طراحی شده‌اند. هرچند روش‌های کدگذاری کلاسیک را نمی‌توان به طور مستقیم به نظریه کدهای تصحیح خطای کوانتومی منتقل کرد، اما از خواص کدهای کلاسیک می‌توان برای طراحی دسته خاصی از کدهای کوانتومی موسوم به کدهای CSS بهره برد. برای واضح‌تر شدن مباحث بعدی رساله، در این فصل مفاهیم مقدماتی نظریه محاسبات کوانتومی، نظریه کدگذاری کلاسیک و نظریه کدگذاری کوانتومی بیان می‌گردند.

۲-۱- کیوبیت‌ها و گیت‌های کوانتومی

حالات کوانتومی را می‌توان بر حسب بردارها و یا با نماد معروف‌تر Bra/Ket نمایش داد. حالت Ket (که با نماد $|.\rangle$ نمایش داده می‌شود) نمایش دهنده یک بردار ستونی است. حالت Bra (که با نماد $\langle.|$ نمایش داده می‌شود) نمایش دهنده ترانهاده مزدوج[4] $|.\rangle$ است. از نمادهای $|0\rangle$ و $|1\rangle$ برای نمایش حالات پایه $(1,0)^T$ و $(0,1)^T$ استفاده می‌شود.

هر ترکیبی از $|0\rangle$ و $|1\rangle$، $\alpha|0\rangle + \beta|1\rangle$ را می‌توان به صورت $(\alpha, \beta)^T$ نشان داد.

---

[1] Quantum Computation
[2] Quantum Mechanics
[3] Decoherence
[4] Transpose Conjugate

محاسبات کوانتومی براساس مفهومی معادل بیت در دنیای کلاسیک، پایه‌گذاری شده است که به آن بیت کوانتومی یا کیوبیت[1] گفته می‌شود. یک *کیوبیت*، یک بردار یکه در فضای هیلبرت[2] دو بعدی است که برای این فضا بردارهای پایه مشخص که با نماد $|0\rangle$ و $|1\rangle$ نمایش داده می‌شوند، انتخاب شده‌اند. بردارهای پایه $|0\rangle$ و $|1\rangle$ به ترتیب همتای کوانتومی بیت‌های کلاسیک 0 و 1 می‌باشند. بر خلاف بیت‌های کلاسیک، کیوبیت‌ها می‌توانند در هر *برهم‌نهی* از $|0\rangle$ و $|1\rangle$ همانند $\alpha|0\rangle + \beta|1\rangle$ قرار بگیرند که α و β اعداد مختلطی هستند که $|\alpha|^2 + |\beta|^2 = 1$ است. اگر چنین ترکیبی نسبت به پایه‌های $|0\rangle$ و $|1\rangle$ اندازه‌گیری شود، آنگاه 0 با احتمال $|\alpha|^2$ و 1 با احتمال $|\beta|^2$ مشاهده می‌شود.

یک رجیستر[3] n *کیوبیتی*، یک حالت کوانتومی است که فضای حالت آن فضای هیلبرت 2^n بعدی می‌باشد. با فرض بردارهای پایه $\{|0\rangle, |1\rangle\}$ برای فضای هیلبرت یک کیوبیتی، بردارهای پایه فضای هیلبرت 2^n بعدی مجموعه زیر می‌باشد:

$$\{|i_1\rangle \otimes |i_2\rangle \otimes \dots \otimes |i_n\rangle ; i_1, i_2, \dots, i_n = 0,1\}$$

که به صورت زیر نیز نمایش داده می‌شود:

$$\{|i_1 i_2 \dots i_n\rangle ; i_1, i_2, \dots, i_n = 0,1\}$$

حالت یک رجیستر n کیوبیتی را می‌توان به صورت جمع خطی بردارهای پایه نوشت:

$$|\varphi\rangle = \sum_{i_1, i_2, \dots, i_n = 0,1} a_{i_1, i_2, \dots, i_n} |i_1\rangle \otimes |i_2\rangle \otimes \dots \otimes |i_n\rangle, \qquad (۱-۲)$$

که

$$\sum_{i_1, i_2, \dots, i_n = 0,1,} \left| a_{i_1, i_2, \dots, i_n} \right|^2 = 1.$$

---

[1] Qubit
[2] Hilbert
[3] Register