



دانشگاه صنعتی شریف
دانشکده علوم ریاضی

پایان نامه کارشناسی

با عنوان

اثبات‌های غیرتعاملی کوانتومی

نگارنده:

علی الماسی

استاد راهنما:

دکتر شهرام خزایی

چکیده

این پایان‌نامه با هدف معرفی مفهوم اثبات‌های غیرتعاملی کوانتومی نوشته شده است. این سیستم‌های اثبات، رده‌ای از مسائل را مشخص می‌کنند که به آن، کلاس QMA گفته می‌شود. مطالعه‌ی QMA از دو جهت حائز اهمیت است. نخست آن‌که این کلاس، همتای کوانتومی کلاس NP است؛ و می‌توان معادل کوانتومی بسیاری از نتایجی که تاکنون در مورد NP یا همتای تصادفی آن MA ، یافت شده است را در چهارچوب محاسبات کوانتومی نیز جست‌وجو کرد. خواهیم دید برخی از سوالات که در مورد NP یا MA به سادگی پاسخ داده می‌شوند، درباره‌ی QMA می‌توانند بسیار دشوار باشند؛ و همین سبب می‌شود تلاش برای پاسخ‌دادن به آن‌ها، به حصول درکی عمیق‌تر از محاسبات کوانتومی انجامد. وجه دیگر اهمیت مطالعه‌ی QMA ، ارتباط عمیق آن با مسائل فیزیک ماده‌ی چگال است. چه آن‌که یکی از مسائل کامل این کلاس، مسأله‌ی همیلتنی‌های موضعی است که یافتن پاسخ تقریبی خوبی برای آن، مسأله‌ای مرکزی در فیزیک ماده‌ی چگال است. به همین دلیل است که بخشی از پیشرفت‌های فعلی نظریه‌ی پیچیدگی محاسبات کوانتومی بر یافتن روش‌هایی کارا برای پاسخ به این مسأله، یا پیدا کردن شواهدی برای سختی آن متمرکز است. در این پایان‌نامه، پس از ساختن مدلی دقیق برای محاسبات کوانتومی، سیستم‌های اثبات غیرتعاملی کوانتومی را معرفی خواهیم کرد و به بررسی کلاس QMA از هر دو وجه فوق خواهیم پرداخت.

فهرست مطالب

۲	۱	مقدمه
۴	۲	پیش‌نیازها
۴	۱.۲	پیش‌نیازهای ریاضی
۴	۱.۱.۲	نمادگذاری دیراک
۶	۲.۱.۲	ضرب تنسوری
۷	۲.۲	پیش‌نیازهای مکانیک کوانتومی
۸	۱.۲.۲	مکانیک کلاسیک
۸	۲.۲.۲	اصول موضوعه‌ی مکانیک کوانتومی
۱۲	۳.۲.۲	قضیه‌ی عدم امکان شبیه‌سازی و درهم‌تنیدگی
۱۳	۴.۲.۲	فرمول‌بندی حالت‌های مخلوط
۱۵	۳.۲	پیش‌نیازهای علوم کامپیوتر
۱۷	۳	مدل محاسبات مداری کوانتومی
۱۷	۱.۳	الگوریتم‌های کوانتومی
۱۹	۲.۳	منال‌هایی از الگوریتم‌های کوانتومی
۱۹	۱.۲.۳	الگوریتم دوچ-جوزا
۲۱	۲.۲.۳	الگوریتم سایمون
۲۳	۳.۲.۳	الگوریتم جست‌وجوی گروور
۲۵	۳.۳	شبیه‌سازی کوانتومی محاسبات کلاسیک
۲۷	۴.۳	گیت‌های جهانی کوانتومی
۳۰	۵.۳	محاسبات کوانتومی کارا
۳۳	۴	اثبات‌های غیرتعاملی کوانتومی
۳۳	۱.۴	کلاس پیچیدگی QMA
۳۷	۲.۴	نسخه‌هایی دیگر از QMA
۳۸	۳.۴	مسئله‌هایی در QMA
۴۱	۵	پیچیدگی همیلتنی کوانتومی
۴۱	۱.۵	همیلتنی‌های موضعی
۴۴	۲.۵	قضیه‌ی کوک-لوین کوانتومی
۴۹	۳.۵	اثبات‌های قابل بررسی احتمالاتی کوانتومی
۴۹	۱.۳.۵	قضیه‌ی PCP کلاسیک
۵۲	۲.۳.۵	حدس PCP کوانتومی
۵۴	۶	مؤخره: پیشرفت‌های جدیدتر و زمینه‌های پژوهش
۵۵		مراجع

۱ مقدمه

محاسبات کوانتومی حوزه‌ای است که در نیمه‌ی دوم قرن بیستم، در پی پیدایش مکانیک کوانتومی و نیز به وجود آمدن نظریه‌ی مناسبی برای محاسبه‌پذیری، با انگیزه‌ی معرفی الگوریتم‌هایی کارا تر برای مطالعه‌ی سیستم‌های فیزیکی کوانتومی شکل گرفته است. از نظر تاریخی، اولین پیشنهاد برای ساختن ماشین محاسبه‌ای که بر اساس فیزیک کوانتوم کار می‌کند را می‌توان مربوط به پاول بنیوف دانست [۲۰]. با این وجود، معمولاً از ریچارد فاینمن به عنوان آغازکننده‌ی راه محاسبات کوانتومی یاد می‌شود. در حقیقت فاینمن در [۴۷]، با توجه به این که شبیه‌سازی برخی پدیده‌های فیزیکی کوانتومی بر روی کامپیوترهای کلاسیک غیرممکن به نظر می‌رسد، پیشنهاد داد از کامپیوترهایی که خود بر اساس فیزیک کوانتوم کار می‌کنند برای چنین شبیه‌سازی‌هایی استفاده شود.

بدون شک دعوت فاینمن، که فیزیکدان برجسته و شناخته‌شده‌ای در آن زمان بود، در جلب توجه فیزیکدانان به این مسأله تأثیر زیادی داشت. از جمله‌ی این افراد، دیوید دویچ بود که سه سال پس از مقاله‌ی فاینمن، مدل محاسبه‌ی ماشین تورینگ کوانتومی^۱ و در سال ۱۹۸۸ مدل محاسبات مداری کوانتومی^۲ را معرفی کرد. به این ترتیب، با داشتن مدل محاسبه‌ای که به طور دقیق تعریف شده باشد و بر اساس قوانین فیزیک کوانتوم کار کند، تلاش‌ها برای مطالعه‌ی بیشتر این دو مدل و یافتن الگوریتم‌هایی بر اساس آن‌ها، آغاز شد. برای مثال، یائو در [۲۲] نشان داد که هر دو مدل قدرت محاسباتی یکسان دارند. این نتیجه، از این نظر تأثیرگذار بود که پیاده‌سازی فیزیکی مدل ماشین تورینگ کوانتومی غیرممکن می‌نماید؛ حال آن‌که مدل مداری از نظر پیاده‌سازی عملی تا حدی امکان‌پذیر است؛ و این معادل بودن قدرت محاسباتی، امیدبخش پیاده‌سازی عملی الگوریتم‌های کوانتومی‌ای است که پیشتر بر اساس مدل ماشین تورینگ کوانتومی تعریف شده بودند.

در سوی دیگر، یافتن الگوریتم‌هایی در این مدل محاسباتی جدید به عنوان راهی برای شناخت بهتر آن، دنبال می‌شد. برنشتاین و وزیرانی با ارائه‌ی الگوریتمی در [۲۳]، نشان دادند اوراکلی وجود دارد که نسبت به آن، محاسبات کارای کوانتومی به طور اکید شامل محاسبات کارای تصادفی کلاسیک است. این نتیجه اولین نشانه را از این‌که مدل کوانتومی ممکن است به نقض تز توسعه‌یافته‌ی چرچ-تورینگ منتج شود، نمایان کرد. سایمون با ارائه‌ی الگوریتمی در [۸۰] نشان داد که محاسبات کوانتومی

کارا مشمول در محاسبات زیرنامی^۳ تصادفی نیست؛ و گروور در [۵۵] ثابت کرد که مسأله‌ی جست‌وجو را با الگوریتم‌های کوانتومی می‌توان به صورت کارتری حل کرد. گرچه برنشتاین و وزیرانی در [۲۳] ثابت کرده بودند که محاسبات کلاسیک و محاسبات کوانتومی از نظر قدرت محاسبه‌پذیری یکسانند، آن‌طور که از نتایج بالا برمی‌آید، محاسبات کوانتومی در مواردی از نظر کارایی می‌تواند بهتر از همتای کلاسیک خود باشد. قوی‌ترین مؤید این مطلب، الگوریتم‌هایی کارایی است که شور در [۷۹] برای حل مسأله‌های تجزیه‌ی اعداد و لگاریتم گسسته ارائه کرده است. ارائه‌ی این الگوریتم‌ها، توجه جامعه‌ی علمی را به قدرت و تأثیرات بالقوه‌ی محاسبات کوانتومی بر زمینه‌های متعددی از علوم کامپیوتر جلب کرد. بالاخص که با پیاده‌سازی الگوریتم شور، شکستن برخی سیستم‌های رایج رمزنگاری همچون DH, RSA, ECC و امکان‌پذیر می‌گردید.

محاسبات کوانتومی از زمان ارائه‌ی الگوریتم‌های شور تا کنون، در کمتر از چهل سال، رشد و پیشرفتی بسیار سریع داشته است. در هزاره‌ی جدید، با پیشرفت تکنولوژی قادر هستیم در عمل کامپیوترهای کوانتومی بسازیم و با آن‌ها محاسبه انجام دهیم [۱۴]. از سوی دیگر، امروزه به طور نظری بسیاری از حوزه‌های علوم کامپیوتر همتای کوانتومی دارند و نتایج امیدبخشی در این حوزه‌ها به دست آمده است. این نویدبخش آن است که در آینده‌ای نه چندان دور، می‌توان از محاسبات کوانتومی به طور گسترده‌ای بهره گرفت؛ و همین سبب شده است که توجه ویژه‌ای از سوی بسیاری از دولت‌ها و سرمایه‌گذاران بخش خصوصی به توسعه‌ی فناوری‌ها و علوم کوانتومی روانه شود [۵۸، ۷۲، ۸۴]. یک نتیجه‌ی توسعه‌ی محاسبات کوانتومی آن است که با پیدا شدن الگوریتم‌های کوانتومی جدید، رده‌بندی مسائل از نظر کیفیت کارایی الگوریتم‌هایی که آن‌ها را حل می‌کنند، ضرورت می‌یابد. نظریه‌ی پیچیدگی محاسبات کوانتومی چهارچوبی است که در آن، این برنامه را دنبال می‌کنیم.

در این پایان‌نامه، تمرکز ما بر مطالعه‌ی سیستم‌های اثبات غیرتعاملی کوانتومی است. سیستم‌های اثبات در پیچیدگی کلاسیک به طور مشروحی مورد مطالعه قرار گرفته‌اند [۱۵، ۷۷، ۸۱]؛ و موارد متعددی از نتایج درخشان پیچیدگی کلاسیک را می‌توان در رابطه با آن‌ها دانست. در چهارچوب محاسبات کوانتومی، مطالعه‌ی اثبات‌ها با کارهای نیل در [۶۷] و کیتاف در [۶۶] آغاز می‌شود. در تشابه با کلاس NP در پیچیدگی کلاسیک، می‌توان کلاسی از مجموعه‌ی ویژگی‌هایی مانند P که تصدیق $x \in P$ با اثبات کوانتومی کوتاهی مانند y و با استفاده از الگوریتمی کوانتومی و کارا امکان‌پذیر است، تعریف کرد. مطالعه‌ی این کلاس، که همتای کوانتومی کلاس NP است، موضوع اصلی این پایان‌نامه است.

در جریان بررسی این کلاس، خواهیم دید مسأله‌ی همپنتی‌های موضعی، که تعمیمی از مسأله‌ی SAT است، مسأله‌ای کامل برای آن است. مطالعه‌ی روش‌هایی برای حل این مسأله و پیچیدگی این روش‌ها، شاخه‌ای از محاسبات کوانتومی به نام پیچیدگی همپنتی کوانتومی را تشکیل می‌دهد. این حوزه ارتباطی عمیق میان نظریه‌ی پیچیدگی محاسبه و نظریه‌ی سیستم‌های چندپیکره در فیزیک ماده‌ی چگال برقرار می‌کند. بالاخص، یکی از زمینه‌های فعال در این حوزه، تلاش برای یافتن همتایی کوانتومی برای قضیه‌ی PCP کلاسیک است. قضیه‌ی PCP، یکی از درخشان‌ترین دستاوردهای نظریه‌ی پیچیدگی محاسبه است که ارتباطی بین نوع خاصی از سیستم‌های اثبات کارا - که به آن‌ها اثبات‌های قابل بررسی احتمالاتی

¹quantum Turing machine

²quantum circuit model

³subexponential

می‌گویند. و سختی یافتن الگوریتم‌های تقریبی کارا برای دسته‌ای از مسائل \mathcal{NP} -سخت برقرار می‌کند. معادل کوانتومی این قضیه، که به عنوان حدس PCP کوانتومی شناخته می‌شود، در صورت درستی، نتایجی خلاف شهود فیزیکی رایج درباره‌ی سیستم‌های کوانتومی خواهد داشت. در حال حاضر فیزیکدانان و متخصصین علوم کامپیوتر، هر یک به روش‌های خود، در تلاش برای یافتن نتایجی در تایید یا رد این حدس هستند؛ و این مسیر هم‌چنان ادامه دارد.

ساختار این پایان‌نامه: در فصل ۲ به بیان پیشینه‌هایی از ریاضی، فیزیک و علوم کامپیوتر خواهیم پرداخت. در بخش اول این فصل، به معرفی نمادگذاری دیراک که نمادگذاری رایجی در ادبیات محاسبات کوانتومی است می‌پردازیم؛ و برخی مباحث موردنیاز از جبرخطی را که معمولاً در یک درس استاندارد پوشش داده نمی‌شوند، مرور خواهیم کرد. در بخش دوم، به معرفی اصول موضوعه‌ی مکانیک کوانتومی و برخی نتایج آن‌ها خواهیم پرداخت؛ و نهایتاً فصل را با بخش کوتاهی درباره‌ی پیشینه‌های علوم کامپیوتری این پایان‌نامه به پایان خواهیم برد.

فصل ۳ به معرفی مدل محاسباتی مداری کوانتومی می‌پردازد؛ که همان مدل محاسباتی مورد استفاده در طول این پایان‌نامه است. پس از تعریف دقیق مدارهای کوانتومی در بخش ۱.۳، در بخش ۲.۳ سه الگوریتم کوانتومی شناخته‌شده را معرفی و بررسی خواهیم کرد. بخش ۳.۳ به این مطلب می‌پردازد که هر تابع محاسبه‌پذیر کلاسیک، به صورت کوانتومی نیز قابل محاسبه است. در ادامه، در بخش ۴.۳ مفهوم جهانی‌بودن یک مجموعه از گیت‌ها را برای مدارهای کوانتومی مورد بازنگری قرار خواهیم داد و به برخی ملاحظات پیچیدگی محاسباتی درباره‌ی سربار محاسباتی ساختن یک مجموعه‌ی جهانی با استفاده از مجموعه‌ی دیگر می‌پردازیم. نهایتاً در بخش ۵.۳، کلاس همه‌ی مسائل قابل حل با الگوریتم‌های کوانتومی کارا را معرفی و برخی ویژگی‌های آن را بیان خواهیم کرد.

بحث ما درباره‌ی اثبات‌های کوانتومی در فصل ۴ آغاز می‌شود. در بخش ۱.۴، کلاس QMA ، معادل کوانتومی کلاس NP ، معرفی می‌شود و امکان کاهش خطای آن مورد بررسی قرار می‌گیرد. علاوه، درباره‌ی برخی کران‌های بالا و پایین برای این کلاس بحث خواهیم کرد. بخش ۲.۴، به معرفی نسخه‌های مختلف کلاس QMA ، برخی ویژگی‌های آن‌ها و نیز روابطشان با یکدیگر اختصاص یافته است. نهایتاً فصل را با بخش ۳.۴، که به ذکر نمونه مسائلی در این کلاس می‌پردازد، به پایان خواهیم رساند.

فصل ۵ درباره‌ی پیچیدگی همیلتنی کوانتومی است. این فصل بر محور مسأله‌ی همیلتنی‌های موضعی که در بخش ۱.۵ معرفی می‌شود، شکل می‌گیرد. در بخش ۲.۵، پیچیدگی حل این مسأله را مورد بررسی قرار خواهیم داد؛ و خواهیم دید نسخه‌ی مشابه قضیه‌ی کوک-لوین، درباره‌ی همتای کوانتومی NP نیز برقرار است. پس از آن، در بخش ۳.۵ درباره‌ی صورت‌بندی دیگری از کلاس NP که با اثبات‌های قابل بررسی احتمالاتی انجام می‌شود، در هر دو چهارچوب کلاسیک و کوانتومی صحبت خواهیم کرد؛ و نهایتاً در مؤخره به برخی زمینه‌های فعلی پژوهش در اثبات‌های کوانتومی اشاره خواهیم کرد.

۲ پیش‌نیازها

هیچ دنیای کوانتومی‌ای وجود ندارد. تنها چیزی که وجود دارد یک توصیف مجرد کوانتومی است.

نیلز بور

۱.۲ پیش‌نیازهای ریاضی

مکانیک کوانتومی، که در ادامه با آن بیشتر آشنا خواهیم شد، چهارچوبی ریاضی است که قواعد ساختن نظریه‌های فیزیکی توصیف‌کننده پدیده‌های کوانتومی را تعیین می‌کند [۷۳]. در این چهارچوب، فضاهای خطی و نظریه‌ی احتمال از جایگاه ویژه‌ای برخوردارند و ضروری است که خواننده با مفاهیم اصلی این دو حوزه از ریاضیات آشنا باشد. در این پایان‌نامه به دلایل مختلفی از جمله اجتناب از جزئیات تکنیکی و نیز با توجه به این که توجه ما به کاربردهای «محاسباتی» فیزیک کوانتوم معطوف است، خود را به فضاهای خطی متناهی‌البعده محدود می‌کنیم. به این ترتیب، آشنایی با جبرخطی و احتمال، تنها پیش‌نیازهای مطالعه‌ی این پایان‌نامه خواهد بود.

در زیربخش نخست، نمادگذاری دیراک^۴، فرمول‌بندی ریاضیاتی رایجی که در مکانیک کوانتومی برای توصیف حالت سیستم‌های کوانتومی استفاده می‌شود را معرفی می‌کنیم. در زیربخش دوم، به معرفی مفهوم ضرب تنسوری فضاهای خطی خواهیم پرداخت و برخی از ویژگی‌های آن را که در ادامه مکرراً به کار خواهند رفت، بیان می‌کنیم.

۱.۱.۲ نمادگذاری دیراک

بسیاری از افرادی که با پیش‌زمینه‌ی غیر فیزیکی، به مطالعه‌ی محاسبات کوانتومی مبادرت می‌ورزند، معمولاً نمادگذاری دیراک را دشوار می‌یابند و گمان می‌کنند این دشواری، بازتابی از دشواری مفاهیم و اصول مکانیک کوانتومی است [۴۸]. با این همه، نباید از یاد برد زمانی که پاول دیراک این نمادگذاری را در اثر درخشانش، «اصول مکانیک کوانتومی [۴۴]»، به کار برد، در پی آن بود که این فرمول‌بندی به عنوان جایگزینی ساده‌تر برای فرمول‌بندی‌های رایج در آن زمان، یعنی مکانیک ماتریسی^۵ و توابع موج^۶ در جامعه‌ی علمی رواج یابد. این نمادگذاری گرچه در آغاز ممکن است پیچیده به نظر بیاید، اما همان‌گونه که خواهیم دید «به ما اجازه می‌دهد که محاسباتی صوری انجام دهیم که خود به خود ما را به نتایج درست رهنمون می‌کنند [۵۲]»؛ و به همین دلیل است که امروزه به طور گسترده‌ای در ادبیات محاسبات کوانتومی به کار برده می‌شود. پیش از معرفی این نمادگذاری، توجه کنید که در سراسر این پایان‌نامه، تمام فضاهای خطی روی میدان اعداد مختلط تعریف شده‌اند و متناهی‌البعده هستند، مگر آن که خلاف آن ذکر شود.

نمادگذاری ۱.۲ کت^۷ یک بردار: برای نمایش برداری مانند v که عضو فضایی خطی مانند V است، از نمادگذاری $|v\rangle$ استفاده می‌کنیم و آن را «کت بردار v » می‌خوانیم. □

نمادگذاری ۲.۲ برای یک بردار: اگر V یک فضای خطی ضرب داخلی و $|v\rangle$ برداری در این فضا باشد، $\langle v|$ $V \rightarrow \mathbb{C}$ ، که آن را «برای بردار v » می‌خوانیم، تابعکی خطی است که به صورت

$$\langle v|(|w\rangle) = (\langle v|, |w\rangle) \quad \forall |w\rangle \in V \quad (1)$$

تعریف شده است و در آن، مقصود از $(\langle v|, |w\rangle)$ ، ضرب داخلی بردارهای $|v\rangle$ و $|w\rangle$ است. □

یادداشت ۳.۲ چنانچه پایه‌ی $\{|v_0\rangle, \dots, |v_{n-1}\rangle\}$ را برای فضای خطی V داشته باشیم، می‌دانیم هر بردار $|v\rangle \in V$ نمایش یکتایی به صورت

$$|v\rangle = \sum_{i=0}^{n-1} \alpha_i |v_i\rangle \quad (2)$$

⁴Dirac Notation

⁵Matrix Mechanics

⁶Wave Functions

دارد. بردار $(\alpha_1 \cdots \alpha_{n-1})^t$ را بردار مختصات^۹ $|v\rangle$ در پایه‌ی داده‌شده می‌نامیم. به سادگی می‌توان دید که نگاشت

$$|v\rangle \mapsto \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} \quad (۳)$$

یک یکرختی بین V و \mathbb{C}^n است. بنابراین هر بردار $|v\rangle$ در یک فضای خطی n بعدی در تناظر یک به یک با یک بردار ستونی $1 \times n$ با درایه‌های مختلط است. به طور مشابه، چنانچه پایه‌ی متعامد یکه‌ای مانند $\{|v_0\rangle, \dots, |v_{n-1}\rangle\}$ برای فضای ضرب داخلی V موجود باشد، برای هر دو بردار دلخواه $|v\rangle = \sum_{i=0}^{n-1} \alpha_i |v_i\rangle$ و $|w\rangle = \sum_{i=0}^{n-1} \beta_i |v_i\rangle$ داریم:

$$(|v\rangle, |w\rangle) = \left(\sum_{i=0}^{n-1} \alpha_i |v_i\rangle, \sum_{i=0}^{n-1} \beta_i |v_i\rangle \right) \quad (۴)$$

$$= \sum_{i,j} \alpha_i^* \beta_j (|v_i\rangle, |v_j\rangle) \quad (۵)$$

$$= \sum_{i,j} \alpha_i^* \beta_j \delta_{i,j} \quad (۶)$$

$$= (\alpha_1^* \cdots \alpha_{n-1}^*) \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix}. \quad (۷)$$

بنابراین، می‌توان نتیجه گرفت که برای هر بردار دلخواه $|v\rangle = \sum_{i=0}^{n-1} \alpha_i |v_i\rangle$ متناظر با یک بردار $1 \times n$ با درایه‌های مختلط است که همان ترانهاده مزدوج بردار مختصات $|v\rangle$ در آن پایه می‌باشد. با توجه به مطلب فوق، در ادامه‌ی این پایان‌نامه، به جای فضاهای خطی دلخواه، خود را به \mathbb{C}^n محدود خواهیم کرد و تعبیرهای فوق را برای کت و برای یک بردار دلخواه به کار خواهیم گرفت.

نمادگذاری ۴.۲ دیگر قراردادها در نمادگذاری دیراک:

۱. با توجه به تعریف برا و کت، واضح است که برای دو بردار دلخواه $|v\rangle, |w\rangle \in V$ برابر با ضرب داخلی آن‌هاست. در نمادگذاری دیراک، ضرب داخلی این دو بردار با $\langle v|w\rangle$ نمایش داده می‌شود.

۲. می‌دانیم برای هر نگاشت خطی $T: V \rightarrow V$ ، نگاشت الحاقی T که آن را با $T^\dagger: V \rightarrow V$ نمایش می‌دهیم، نگاشتی است با این ویژگی که برای هر $|v\rangle, |w\rangle \in V$

$$(|v\rangle, T|w\rangle) = (T^\dagger|v\rangle, |w\rangle). \quad (۸)$$

در نمادگذاری دیراک برای هر $|v\rangle \in V$ و هر نگاشت خطی T روی فضای V تعریف می‌کنیم:

$$\langle v|^\dagger \stackrel{\text{def}}{=} |v\rangle, \quad (۹)$$

$$(T|v\rangle)^\dagger \stackrel{\text{def}}{=} \langle v| T^\dagger. \quad (۱۰)$$

۳. برای دو فضای ضرب داخلی V و W و دو بردار دلخواه $|v\rangle \in V$ و $|w\rangle \in W$ ، نگاشت خطی $|v\rangle\langle w|: W \rightarrow V$ به صورت زیر تعریف می‌شود:

$$|v\rangle\langle w|(|u\rangle) \stackrel{\text{def}}{=} \langle w|u\rangle |v\rangle \quad \forall |u\rangle \in W. \quad (۱۱)$$

به نگاشت فوق، ضرب خارجی^{۱۰} دو بردار $|v\rangle$ و $|w\rangle$ گویند.

^۹Coordinate Vector

^{۱۰}Outer Product

۴. پایه‌ی استاندارد \mathbb{C}^n ، که متشکل از n بردار

$$|0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, |n-1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \quad (12)$$

است، پایه‌ی محاسباتی نامیده می‌شود.

□

در پایان این زیربخش، شایان ذکر است که علاقه‌مندان به آشنایی بیشتر با نمادگذاری دیراک می‌توانند به مرجع [۷۳] مراجعه کنند.

۲.۱.۲ ضرب تنسوری

ضرب تنسوری^{۱۱} یکی از مفاهیمی است که در حوزه‌های مختلف ریاضیات و فیزیک، و بالاخص مکانیک کوانتومی، به طور گسترده‌ای به کار گرفته می‌شود. در این قسمت، به معرفی این مفهوم، و بیان برخی ویژگی‌های آن خواهیم پرداخت.

تعریف ۵.۲ فرض کنید V و W دو فضای برداری و $\{|v_0\rangle, \dots, |v_{n-1}\rangle\}$ و $\{|w_0\rangle, \dots, |w_{m-1}\rangle\}$ به ترتیب پایه‌هایی برای آن‌ها باشند. ضرب تنسوری دو فضای V و W ، که آن را با $V \otimes W$ نمایش می‌دهیم، یک فضای برداری با پایه‌ی صوری

$$\{|v_i\rangle \otimes |w_j\rangle : i = 0, 1, \dots, n-1, j = 0, 1, \dots, m-1\} \quad (13)$$

►

(روی میدان \mathbb{C}) است.

تعریف ۶.۲ برای دو فضای برداری V و W با پایه‌های $\{|v_0\rangle, \dots, |v_{n-1}\rangle\}$ و $\{|w_0\rangle, \dots, |w_{m-1}\rangle\}$ ، دو بردار $|v\rangle = \sum_{i=0}^{n-1} \alpha_i |v_i\rangle$ و $|w\rangle = \sum_{j=0}^{m-1} \beta_j |w_j\rangle$ ، حاصلضرب تنسوری دو بردار $|v\rangle$ و $|w\rangle$ ، که آن را با $|v\rangle \otimes |w\rangle$ نمایش می‌دهیم، به صورت

$$|v\rangle \otimes |w\rangle = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha_i \beta_j |v_i\rangle \otimes |w_j\rangle \quad (14)$$

►

تعریف می‌شود.

یادداشت ۷.۲ توجه کنید که در تعریف‌های فوق، ضرب تنسوری دو فضای برداری وابسته به پایه‌ای که برای دو فضا انتخاب می‌کنیم خواهد بود. شایان ذکر است که ضرب تنسوری را می‌توان به نحوی تعریف کرد که فضای $V \otimes W$ مستقل از انتخاب پایه باشد. خواننده‌ی علاقه‌مند می‌تواند برای آشنایی بیشتر با این تعریف، به مرجع [۵۶] مراجعه کند.

یادداشت ۸.۲ از تعریف ۵.۲ روشن است که حاصلضرب تنسوری دو فضای n و m بعدی، فضای nm بعدی است. بنابراین $\mathbb{C}^n \otimes \mathbb{C}^m \cong \mathbb{C}^{nm}$. به طور خاص، اگر $\{|i\rangle\}_{i=0}^{n-1}$ و $\{|j\rangle\}_{j=0}^{m-1}$ به ترتیب پایه‌های محاسباتی \mathbb{C}^n و \mathbb{C}^m باشند، نگاشت

$$|i\rangle \otimes |j\rangle \mapsto |mi + j\rangle \quad (15)$$

یک یکریختی بین $\mathbb{C}^n \otimes \mathbb{C}^m$ و \mathbb{C}^{nm} را مشخص می‌کند. در ادامه، ما نیز $|i\rangle \otimes |j\rangle$ و $|mi + j\rangle$ را یکی خواهیم گرفت.

►

نمادگذاری ۹.۲ در نمادگذاری دیراک، $|v\rangle \otimes |w\rangle$ معمولاً به صورت $|vw\rangle$ یا $|v\rangle |w\rangle$ خلاصه می‌شود.

تعریف ۱۰.۲ مقصود از ضرب تنسوری دو نگاشت خطی $L_1 : V \rightarrow V'$ و $L_2 : W \rightarrow W'$ ، نگاشتی خطی مانند $L_1 \otimes L_2 : V \otimes W \rightarrow V' \otimes W'$ است که عمل آن روی پایه‌ی $\{|v_i\rangle \otimes |w_j\rangle\}_{i,j}$ به صورت

$$L \otimes L'(|v_i\rangle \otimes |w_j\rangle) = (L|v_i\rangle) \otimes (L'|w_j\rangle) \quad (16)$$

¹¹Tensor Product

تعریف شده است. \blacktriangleright
 همان‌گونه که در یادداشت ۳.۲ دیدیم، در بسیاری از موارد ترجیح می‌دهیم به جای بردارهای دلخواه در یک فضای برداری، با بردارهای مختصات آن‌ها (در پایه‌ای دلخواه) کار کنیم. به طور مشابه، گاهی کار با نمایش ماتریسی یک نگاشت خطی (در پایه‌ای دلخواه) را ترجیح می‌دهیم. در چنین مواردی، که فضاهای برداری را به \mathbb{C}^n و نگاشت‌های خطی را به ماتریس‌هایی با درایه‌های مختلط تقلیل می‌دهیم، راحت‌تر است که ضرب تنسوری را با ضرب کرونکر^{۱۲} که ساده‌تر، ولی معادل با آن است، جایگزین کنیم. در واقع، تعریف بعد، تعمیمی از یکریختی یادشده در یادداشت ۸.۲ را ارائه می‌دهد.

تعریف ۱۱.۲ ضرب کرونکر دو ماتریس $A_{m \times n}$ و $B_{p \times q}$ ، که آن را با $A \otimes B$ نمایش می‌دهیم، ماتریسی با ابعاد $(mp) \times (nq)$ است که به صورت زیر تعریف می‌شود:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \quad (17)$$

\blacktriangleright **یادداشت ۱۲.۲** توجه کنید که اگر فضاهای V و W دو فضای ضرب داخلی باشند، فضای $V \otimes W$ را می‌توان به ضرب داخلی طبیعی

$$\left(\sum_i \alpha_i |v_i\rangle \otimes |w_i\rangle, \sum_j \beta_j |v_j\rangle \otimes |w_j\rangle \right) = \sum_{i,j} \alpha_i^* \beta_j \langle v_i | v_j \rangle \langle w_i | w_j \rangle \quad (18)$$

مجهز کرد. در ادامه، مقصودمان از ضرب داخلی روی فضای ضرب تنسوری، ضرب داخلی کانونی فوق خواهد بود. \blacktriangleright نهایتاً، این زیربخش را با گزاره‌ای به پایان خواهیم برد که برخی ویژگی‌های پرکاربرد ضرب تنسوری را بیان می‌کند.

گزاره ۱۳.۲ فرض کنید V و W دو فضای ضرب داخلی هستند؛ $|v\rangle, |v'\rangle \in V$ و $|w\rangle, |w'\rangle \in W$ ؛ c یک عدد مختلط دلخواه است و L و L' دو نگاشت خطی هستند که به ترتیب روی V و W تعریف شده‌اند. در این صورت، تساوی‌های زیر برقرارند:

$$1. (|v\rangle + |v'\rangle) \otimes |w\rangle = |vw\rangle + |v'w\rangle$$

$$2. |v\rangle \otimes (|w\rangle + |w'\rangle) = |vw\rangle + |vw'\rangle$$

$$3. c|vw\rangle = (c|v\rangle) \otimes |w\rangle = |v\rangle \otimes (c|w\rangle)$$

$$4. (L \otimes L')^\dagger = L^\dagger \otimes L'^\dagger$$

$$5. \text{tr}(L \otimes L') = \text{tr}(L)\text{tr}(L')$$

۲.۲ پیش‌نیازهای مکانیک کوانتومی

هر چند صحت تاریخی داستان سببی که بر سر نیوتن افتاد و الهام‌بخش او در تدوین نظریه‌اش شد، نظریه‌ای که در پی یافتن اصولی ریاضی برای فلسفه‌ی طبیعی بود [۳۸]، در حاله‌ای از ابهام است، اما این سبب الهام‌بخش مثال مناسبی است برای توضیح آن چه مکانیک (کلاسیک) در پی مطالعه‌ی آن است. در زیربخش ۱.۲.۲ با بهره‌گیری از این مثال، یادآوری خواهیم کرد که مکانیک کلاسیک چگونه سیستم‌های فیزیکی کلاسیک را به صورت ریاضی صورت‌بندی می‌کند؛ سپس در زیربخش ۲.۲.۲ به سراغ مکانیک کوانتومی و اصول موضوعه‌ی آن خواهیم رفت. زیربخش ۲.۲.۲ به دو مفهوم مهم که از وجوه تمایز فیزیک کلاسیک و فیزیک کوانتوم هستند خواهد پرداخت؛ و نهایتاً در زیربخش ۴.۲.۲ فرمول‌بندی دیگری برای توصیف سیستم‌های کوانتومی معرفی خواهیم کرد و با استفاده از این فرمول‌بندی، اصول بیان‌شده در بخش ۲.۲.۲ را بازنویسی خواهیم کرد.

¹²Kronecker Product

۱.۲.۲ مکانیک کلاسیک

سیستم فیزیکی مورد بحث در بالا، همان سببی که از درخت جدا شده و در حال افتادن بر زمین است، را در نظر بگیرید. برخی ویژگی‌های فیزیکی این سبب طی حرکتش به سمت زمین تغییر می‌کنند؛ مثلاً سرعت، ارتفاع آن از سطح زمین، انرژی جنبشی و پتانسیل آن. از سوی دیگر، برخی ویژگی‌های فیزیکی سبب نیز در طول این حرکت، ثابت باقی می‌مانند؛ برای مثال جرم سبب از جمله ویژگی‌های آن است که در این حرکت، ناوردا باقی می‌ماند. به خواص فیزیکی از نوع اول، خواص پویا، و به خواص نوع دوم، خواص ایستا می‌گوییم [۸۲].

به طور کلی، هدف مکانیک کلاسیک را می‌توان مطالعه‌ی خواص پویای سیستم‌های فیزیکی ماکروسکوپی که متشکل از اشیاء در حال حرکت هستند، دانست. برای نیل به این مقصود، یک کار طبیعی مدل‌سازی ریاضی خواص پویا با سیستم‌های دینامیکی زمان-پیوسته است. با این مدل‌سازی، بسیاری از مسائل فیزیکی را می‌توان به عنوان مسائلی در نظریه‌ی سیستم‌های دینامیکی صورت‌بندی کرد. به عنوان مثال، فرض کنید که در مثال سببی که از درخت افتاده است، می‌خواهیم رابطه‌ی بین ارتفاع اولیه‌ی سبب و سرعت آن در هنگام برخورد به زمین را پیدا کنیم. ترجمه‌ی این پرسش فیزیکی به زبان سیستم‌های دینامیکی می‌تواند به این صورت باشد: «چنانچه حالت اولیه‌ی یک سیستم دینامیکی را بدانیم، آیا می‌توانیم حالت سیستم را در یک زمان خاص پیش‌بینی کنیم؟»؛ مسأله‌ای که در قلب نظریه‌ی سیستم‌های دینامیکی قرار دارد.

از نظر تاریخی، صورت‌بندی سیستم‌های فیزیکی به عنوان سیستم‌های دینامیکی به انحاء مختلفی انجام شده است و منجر به شکل‌گیری فرمول‌بندی‌های متفاوتی مانند فرمول‌بندی‌های نیوتنی، لاگرانژی و همیلتنی برای مکانیک کلاسیک شده است. در ادامه، خود را به فرمول‌بندی نیوتنی محدود خواهیم کرد و توضیح خواهیم داد که ترجمه‌ی یک سیستم فیزیکی متشکل از یک ذره‌ی در حال حرکت در راستای عمودی (سبب افتان) به زبان سیستم‌های دینامیکی به چه صورت انجام خواهد شد. در مکانیک نیوتنی تنها دو خاصیت پویا، یعنی مکان و سرعت یک ذره، برای توصیف حالت سیستم در هر لحظه کافی هستند. حالت سیستم در لحظه‌ی t ، با زوج مرتب $(x(t), v(t))$ مشخص می‌شود؛ که $x(t)$ و $v(t)$ به ترتیب مکان و سرعت ذره را در زمان t مشخص می‌کنند. علاوه بر این، قانون انتقال سیستم، یا قاعده‌ای که حالت سیستم بر اساس آن در طول زمان تغییر می‌کند، با کمیت فیزیکی نیرویی که بر سیستم وارد می‌شود مشخص می‌شود؛ که بنابر قانون دوم نیوتن متناسب با مشتق دوم مکان ذره است. به عبارت دیگر، معادله‌ی دیفرانسیل

$$F = m \frac{d^2 x}{dt^2} \quad (19)$$

تحول زمانی سیستم را مشخص می‌کند؛ که در آن F و m به ترتیب نیروی کل وارد بر ذره و جرم آن هستند. سیستم دینامیکی فوق که برای یک ذره‌ی در حال حرکت تعریف شد، به سادگی قابل تعمیم برای سیستمی متشکل از چند ذره نیز هست. بدین منظور کافی است فضای حالت را مجموعه‌ی همه‌ی n تایی‌های مرتب که بیانگر مکان و سرعت هر یک از ذرات هستند، در نظر بگیریم؛ و معادله‌ی ۱۹ را نیز به صورت برداری بازنویسی کنیم. توجه کنید که اصول موضوعه‌ی مکانیک کوانتومی نیز، در روند مشابهی با آن چه در ارتباط با مکانیک کلاسیک گفتیم، نحوه‌ی نسبت دادن یک سیستم دینامیکی به سیستم‌های فیزیکی کوانتومی را مشخص می‌کنند؛ که در زیربخش بعد به تفصیل آن‌ها را بررسی خواهیم کرد.

۲.۲.۲ اصول موضوعه‌ی مکانیک کوانتومی

مکانیک کوانتومی چهارچوبی ریاضی است که جهان فیزیکی، به طور خاص پدیده‌هایی فیزیکی که در سطح اتمی و زیراتمی رخ می‌دهند، را به نظریات ریاضی پیوند می‌دهد. از نظر تاریخی، پیدایش فیزیک کوانتوم را می‌توان مربوط به اولین سال‌های قرن بیستم و ناکامی فیزیک کلاسیک در توضیح تعدادی از نتایج آزمایشگاهی حاصل شده در آن زمان دانست. معرفی مفهوم بسته‌های انرژی توسط مکس پلانک [۷۵] که بعدها انیشتین آن را توسعه داد و اثر فوتوالکتریک را به کمک این مفهوم توضیح داد [۴۵]، معرفی مدل اتمی بور برای توصیف طیف اتم هیدروژن [۲۵]، توسعه‌ی مکانیک ماتریسی توسط هایزنبرگ و توابع موج توسط شرودینگر برای توصیف ریاضی پدیده‌های کوانتومی و ارائه‌ی اصول موضوعه‌ی مکانیک کوانتومی توسط فون نویمان [۸۷] از جمله مهم‌ترین گام‌هایی است که در سه دهه‌ی اول قرن بیستم رخ داده و منجر به ساخته شدن این نظریه‌ی ارزشمند، و البته غامض، شده‌اند. نظریه‌ای که تأثیرات شگرفی بر زندگی بشر در عصر حاضر گذاشته و انتظار می‌رود که به زودی، بسیار بیشتر از امروز، وجوه مختلف زندگی ما را متأثر کند.

در این زیربخش، بررسی خواهیم کرد که اصول موضوعه‌ی مکانیک کوانتومی چگونه فضای حالت و تحول زمانی سیستم‌های فیزیکی کوانتومی را فرمول‌بندی می‌کنند. هم‌چنین خواهیم دید که چگونه این فرمول‌بندی‌ها قابل تعمیم به سیستم‌هایی متشکل از زیرسیستم‌های کوچکتر است. علاوه بر این، در اصلی که مشابه آن در مکانیک کلاسیک وجود ندارد، خواهیم دید که اندازه‌گیری یک سیستم کوانتومی، یکی از مفاهیم مناقشه‌برانگیز فیزیک کوانتوم، چگونه صورت‌بندی می‌شود.

اصل ۱۴.۲ (فضای حالت) به هر سیستم فیزیکی منزوی یک فضای هیلبرت نسبت داده می‌شود که به آن فضای حالت سیستم^a می‌گویند. بردار حالت^b سیستم (یا به طور خلاصه، حالت سیستم)، بردار یکه‌ای در فضای حالت آن است [۷۳].

^aState Space
^bState Vector

تعریف ۱۵.۲ یک کیوبیت^{۱۳}، یک سیستم کوانتومی است که فضای حالت آن، فضای هیلبرت دو بعدی \mathbb{C}^2 است. کیوبیت‌ها، همتای کوانتومی بیت‌های کلاسیک، اساسی‌ترین و ضروری‌ترین سیستم‌های فیزیکی هستند که در محاسبات و اطلاعات کوانتومی به کار گرفته می‌شوند. حالت یک کیوبیت می‌تواند به صورت

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (20)$$

نوشته شود که در آن، $\alpha, \beta \in \mathbb{C}$ ، $|\alpha|^2 + |\beta|^2 = 1$ ، و $|0\rangle$ و $|1\rangle$ بردارهای $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ و $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ را مشخص می‌کنند. برخلاف بیت‌های کلاسیک، که تنها می‌توانند یکی از دو مقدار ۰ یا ۱ را داشته باشند، یک کیوبیت می‌تواند (مانند معادله‌ی ۲۰) در یک برهم‌نهی^{۱۴} از $|0\rangle$ و $|1\rangle$ قرار گیرد. این یکی از تفاوت‌های اساسی میان محاسبات کلاسیک و محاسبات کوانتومی است. تفاوتی که می‌تواند در امکان ساختن الگوریتم‌هایی کوانتومی که بسیار بهتر از الگوریتم‌های کلاسیک عمل می‌کنند، نقش داشته باشد. در ادبیات محاسبات کوانتومی، نام‌های خاصی برای برخی حالت‌های یک کیوبیت وجود دارد. در نمادگذاری بعد، دو مورد از این حالات را معرفی می‌کنیم.

نمادگذاری ۱۶.۲ حالت‌های $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ و $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ به ترتیب با $|+\rangle$ و $|-\rangle$ نمایش داده می‌شوند. توجه کنید که $\{|+\rangle, |-\rangle\}$ پایه‌ای برای \mathbb{C}^2 است که به آن پایه‌ی X می‌گویند. همچنین پایه‌ی محاسباتی \mathbb{C}^2 پایه‌ی Z نامیده می‌شود.

اصل ۱۷.۲ (تحول زمانی سیستم) این اصل را می‌توان به دو صورت متفاوت بیان کرد؛ و البته می‌توان نشان داد که این دو صورت با یکدیگر معادلند [۷۳]:

• حالت یک سیستم بسته‌ی کوانتومی مطابق با معادله‌ی شرودینگر تحول می‌یابد. معادله‌ی شرودینگر به صورت زیر است:

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle,$$

که در آن $\psi(t)$ حالت سیستم در لحظه‌ی t ، عملگری هرمیتی که به آن همیلتنی^a سیستم می‌گویند، و \hbar ثابت پلانک است.

• اگر حالت یک سیستم بسته‌ی کوانتومی در لحظه‌ی t_1 ، $|\psi(t_1)\rangle$ باشد، حالت سیستم در لحظه‌ی $t_2 > t_1$ با

$$|\psi(t_2)\rangle = U|\psi(t_1)\rangle$$

مشخص می‌شود که U نگاشتی یکانی است که تنها به $t_2 - t_1$ وابسته است.









^aHamiltonian

از این به بعد، اصطلاح «گیت کوانتومی» را برای اشاره به عملگرهای یکانی که تحول سیستم را مشخص می‌کنند، به کار خواهیم برد. با وجود این که تعداد گیت‌های کوانتومی که قابل اعمال بر یک کیوبیت هستند نامتناهی است، به دلایل متعددی تنها تعدادی متناهی از این گیت‌ها مورد علاقه‌ی ما هستند. جدول ۱ شامل لیست مختصری از تعدادی از این گیت‌های کوانتومی و نمایش گرافیکی و ماتریسی آن‌هاست.

¹³Qubit

¹⁴Superposition


جدول ۱: برخی از مهم‌ترین گیت‌های تک‌کیوبیتی

نام گیت	نمایش ماتریسی	نمایش گرافیکی ^{۱۵}
Pauli-I	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	
Pauli-X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	
Pauli-Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	
Pauli-Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	
Hadamard	$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$	
T-gate	$\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$	
Phase (S-gate)	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	
Relative Phase Rotation	$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i\theta} \end{pmatrix}$	

اصل ۱۸.۲ (سیستم‌های مرکب) فضای حالت یک سیستم مرکب که متشکل از n زیرسیستم با فضاهای حالت V_1, \dots, V_n است، برابر است با $V_1 \otimes \dots \otimes V_n$. هم‌چنین اگر هر یک از زیرسیستم‌ها حالت $|v_i\rangle$ را داشته باشند، حالت سیستم مرکب برابر با $|v_1\rangle \otimes \dots \otimes |v_n\rangle$ خواهد بود [۷۳].

با توجه به اصول ۱۷.۲ و ۱۸.۲، تحول زمانی یک سیستم مرکب کوانتومی که متشکل از دو زیرسیستم با فضاهای حالت V و W است، با نگاهت‌های یکانی روی فضای $V \otimes W$ مشخص می‌شود. توجه کنید که زیرمجموعه‌ای از چنین نگاهت‌هایی، به صورت $L \otimes L'$ هستند، که L و L' به ترتیب نگاهت‌هایی یکانی روی فضاهای V و W هستند. با این وجود، باید توجه شود که این زیرمجموعه، زیرمجموعه‌ای سره از همه‌ی نگاهت‌های یکانی روی $V \otimes W$ است. بنا بر دلایلی، نظری و عملی، در محاسبات کوانتومی بیشتر علاقه‌مند به گیت‌هایی هستیم که حداکثر روی ۳ کیوبیت به طور نابديهی عمل می‌کنند. جدول ۲ تعدادی از این گیت‌ها، که روی بیش از یک کیوبیت به طور نابديهی عمل می‌کنند، نمایش ماتریسی و نمایش گرافیکی آن‌ها را لیست کرده است.

جدول ۲: برخی از مهم‌ترین گیت‌های چند کیوبیتی

نام گیت	نمایش ماتریسی	نمایش گرافیکی
CNOT	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	

^{۱۵}سیم‌ها نمایانگر کیوبیت‌ها هستند.

نمایش گرافیکی	نمایش ماتریسی	نام گیت
	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix}$	^{۱۶} Controlled- U
	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	Toffoli gate (CCNOT)

اصل ۱۹.۲ (اندازه‌گیری) مقصود از یک اندازه‌گیری با m نتیجه‌ی ممکن روی یک سیستم کوانتومی، خانواده‌ای از عملگرها مانند $M = \{M_1, \dots, M_m\}$ است (M_i متناظر با نتیجه‌ی i ام است) که روی فضای حالت آن سیستم عمل می‌کنند و شرط $\sum_{i=1}^m M_i^\dagger M_i = \mathbb{I}$ را نیز برآورده می‌کنند. هنگامی که این اندازه‌گیری روی سیستمی که در حالت $|\psi\rangle$ قرار دارد انجام می‌شود، نتیجه‌ی اندازه‌گیری با احتمال

$$p(i) = \langle \psi | M_i^\dagger M_i | \psi \rangle,$$

برابر با i خواهد بود؛ و در این صورت، حالت سیستم به حالت

$$\frac{M_i |\psi\rangle}{\sqrt{\langle \psi | M_i^\dagger M_i | \psi \rangle}}$$

فرو خواهد ریخت ^a[۷۳].

^aCollapse

در ادامه‌ی این پایان‌نامه، عموماً از حالت خاصی از اندازه‌گیری‌های معرفی شده در اصل ۱۹.۲ بهره خواهیم گرفت که در ادامه معرفی می‌شوند.

تعریف ۲۰.۲ یک اندازه‌گیری افکنشی یک اندازه‌گیری کوانتومی است که متشکل است از عملگرهای افکنشی دو به دو متعامد. یک عملگر افکنشی عملگری هرمیتی مانند $P: \mathbb{C}^n \rightarrow \mathbb{C}^n$ است به طوری که $P^2 = P$. به عبارت دیگر، یک اندازه‌گیری افکنشی خانواده‌ای مانند $M = \{P_1, \dots, P_m\}$ است به طوری که:

۱. هر P_i یک عملگر افکنشی است.

$$\sum_{i=1}^m P_i = \mathbb{I} \quad ۲.$$

$$\forall i, j \in \{1, \dots, m\}, \quad P_i P_j = \delta_{ij} P_i \quad ۳.$$

همچنین ممکن است در ادامه‌ی این تز، از اصطلاح اندازه‌گیری در پایه‌ی $\{|v_0\rangle, \dots, |v_{n-1}\rangle\}$ استفاده کنیم. در چنین مواردی، مقصودمان یک اندازه‌گیری افکنشی با عملگرهای اندازه‌گیری $|v_i\rangle\langle v_i|$ خواهد بود.

$$U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \text{ فرض کنید} \quad ۱۶.$$

نمادگذاری ۲۱.۲ در ادامه از نماد زیر برای نمایش گرافیکی اندازه‌گیری استفاده خواهیم کرد.



□

۳.۲.۲ قضیه‌ی عدم امکان شبیه‌سازی و درهم‌تیدگی

در این زیربخش، به دو مفهوم اساسی که نقشی کلیدی در علم اطلاعات کوانتومی دارند خواهیم پرداخت. مفاهیمی که ما را به دو مورد از اساسی‌ترین تفاوت‌های محاسبات کلاسیک و محاسبات کوانتومی رهنمون خواهند کرد. اولین مفهوم، قضیه‌ی عدم امکان شبیه‌سازی^{۱۷} است. بنا بر این قضیه، که نخستین بار در [۹۴] و [۴۲] بیان شده است، اگر یک نگاشت یکانی وجود داشته باشد که حالت مولفه‌ی اول یک سیستم مرکب دو مولفه‌ای کوانتومی را روی مولفه‌ی دوم کپی کند، در این صورت هر دو حالت قابل کپی کردن مولفه‌ی اول یا بر هم عمودند و یا باهم برابرند. به عبارت دیگر، با داشتن یک حالت کوانتومی نامعلوم، امکان کپی کردن آن بدون تغییر دادن حالتش وجود ندارد. این قضیه نتایج متعددی در محاسبات و اطلاعات کوانتومی دارد. به عنوان مثالی از یک نتیجه‌ی منفی، توجه کنید که برخلاف روش‌های کاهش خطای مبتنی بر تکرار که در مخابرات و اطلاعات کلاسیک به طور گسترده استفاده می‌شوند، در محاسبات کوانتومی به طور کلی نمی‌توان از روی یک پیام کوانتومی تعداد زیادی کپی درست کرد و از این طریق تأثیر نویز ایجاد شده در کانال مخابراتی را کاهش داد. به این ترتیب، راه‌های ممکن برای تصحیح خطای مخابره در ارتباطات کوانتومی بسیار محدودتر و توسعه‌ی این روش‌ها بسیار خلاقانه‌تر و سخت‌تر است. مفهوم دوم، مفهوم ساده و در عین حال مهمی به نام درهم‌تیدگی^{۱۸} است.

تعریف ۲۲.۲ به حالت $|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ (که حالت یک سیستم مرکب متشکل از دو زیرسیستم n و m بعدی است) درهم‌تیدگی می‌گوییم، هر گاه هیچ دو برداری مانند $|\phi_1\rangle \in \mathbb{C}^n$ و $|\phi_2\rangle \in \mathbb{C}^m$ وجود نداشته باشد چنان‌که

$$|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle.$$

▶ اگر یک حالت کوانتومی درهم‌تیدگی نباشد، به آن جداشدنی یا ضریبی می‌گوییم. توجه کنید که برخلاف آنچه در بالا بیان شد، حالات جداشدنی و حالات ضریبی در فرمول‌بندی حالت‌های مخلوط تعاریف متفاوتی دارند و با یکدیگر معادل نیستند. به این موضوع در زیربخش ۴.۲.۲ بیشتر خواهیم پرداخت.

تعریف ۲۳.۲ به چهار حالت زیر (که چهار حالت ممکن برای یک سیستم دوکیوبیتی هستند) حالت‌های بل^{۱۹} یا زوج‌های EPR^{۲۰} می‌گوییم.

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \end{aligned}$$

¹⁷No-cloning Theorem

¹⁸Entanglement

¹⁹Bell States

²⁰EPR Pairs

گزاره ۲۴.۲ حالت‌های بل درهم‌تنیده‌اند.

پس از معرفی مفهوم درهم‌تنیدگی، این سوال مطرح می‌شود که آیا می‌توان درهم‌تنیده بودن یک حالت دو بخشی را به صورت موثری تعیین کرد یا نه. قضیه‌ی بعد، که نتیجه‌ی مستقیمی از قضیه‌ی SVD است، ابزاری را برای این منظور در اختیار ما قرار می‌دهد.

قضیه ۲۵.۲ (تجزیه‌ی اشمیت) فرض کنید V و W دو فضای هیلبرت هستند و $|\psi\rangle \in V \otimes W$ مجموعه‌ای از بردارهای متعامد یکه‌ی V $\{|v_0\rangle, \dots, |v_{n-1}\rangle\} \subset V$ و مجموعه‌ای از بردارهای متعامد یکه‌ی W $\{|w_0\rangle, \dots, |w_{n-1}\rangle\} \subset W$ وجود دارد، چنانکه

$$|\psi\rangle = \sum_i \alpha_i |v_i\rangle \otimes |w_i\rangle,$$

که در آن $n = \min(\dim(V), \dim(W))$ ؛ و α_i ها اعداد حقیقی و نامنفی یکتایی هستند که ضرایب اشمیت^{۲۱} نامیده می‌شوند.

قضیه‌ی ۲۵.۲ روشی را برای اندازه‌گیری میزان درهم‌تنیدگی یک حالت کوانتومی دو بخشی در اختیار ما می‌گذارد. می‌توان نشان داد که یک حالت دو بخشی، درهم‌تنیده است اگر و فقط اگر در تجزیه‌ی اشمیتش، بیش از یک ضریب اشمیت ناصفر داشته باشد. بنابراین، با در اختیار داشتن توصیف حالت یک سیستم دو بخشی، برای چک کردن این که حالت سیستم درهم‌تنیده یا جداشدنی است، کافی است تجزیه‌ی اشمیت آن حالت را محاسبه کرده و سپس تعداد ضرایب اشمیت ناصفر آن را تعیین کنیم. این کار را در زمان چندجمله‌ای بر حسب بعد فضای حالت سیستم مرکب مورد نظر قابل انجام است. این بخش را با ذکر این نکته به پایان می‌رسانیم که درهم‌تنیدگی کوانتومی، همان‌گونه که شروینگر گفته است، «ویژگی بارز مکانیک کوانتومی است؛ آن چیزی که کل ماهیت آن را از خطوط فکری کلاسیک جدا می‌کند [۷۶]». تا کنون موارد متعددی از نتایج درهم‌تنیدگی کشف شده‌اند؛ و این مسیر هم‌چنان ادامه دارد. به طور ویژه، باور بر این است که درهم‌تنیدگی کوانتومی منبعی ضروری برای الگوریتم‌های کوانتومی است تا بتوانند به تسریعی نمایی نسبت به الگوریتم‌های کلاسیک دست یابند [۶۳]. افزون بر این، کاربردهای عدیده‌ی دیگری از وجود درهم‌تنیدگی کوانتومی در زمینه‌های دیگر علوم کامپیوتر نیز شناخته شده است. به عنوان چند مثال می‌توان به دورنوردی کوانتومی [۲۷، ۲۱]، کدگذاری فوق‌چگال کوانتومی [۲۲] و پروتکل‌های مبتنی بر درهم‌تنیدگی برای توزیع کلید کوانتومی [۷۸] اشاره کرد.

۴.۲.۲ فرمول‌بندی حالت‌های مخلوط

در این زیربخش به تعمیمی از فرمول‌بندی ارائه‌شده در زیربخش ۲.۲.۲، که به آن فرمول‌بندی حالت‌های خالص گفته می‌شود، خواهیم پرداخت. این فرمول‌بندی جدید، که به عنوان فرمالیزم حالت‌های مخلوط^{۲۲} شناخته می‌شود، روشی شهودی‌تر و مناسب‌تر برای فکر کردن به برخی سناریوهایی که در محاسبات کوانتومی با آن مواجه می‌شویم، فراهم می‌کند. به علاوه، محاسبات کوانتومی از طریق این فرمول‌بندی ارتباطات عمیقی با حوزه‌های دیگر ریاضیات، مانند نظریه‌ی ماتریس‌ها، آنالیز محذب و نظریه‌ی گروه‌ها پیدا خواهد کرد [۹۰].

تعریف ۲۶.۲ فرض کنید V یک فضای هیلبرت باشد. عملگر $\rho : V \rightarrow V$ را یک عملگر چگالی^{۲۳} می‌نامیم هرگاه مثبت نیمه معین باشد و $tr(\rho) = 1$.

تعریف ۲۷.۲ اگر حالت یک سیستم کوانتومی با احتمال $\{p_i\}_{i=0}^{k-1}$ بردار $\{|\psi_i\rangle\}_{i=0}^{k-1}$ باشد، در این صورت گفته می‌شود سیستم در حالت مخلوط^{۲۴} است. در این صورت مجموعه‌ی $\{(p_i, |\psi_i\rangle)\}_{i=0}^{k-1}$ یک هنگرد^{۲۵} نامیده می‌شود.

گزاره ۲۸.۲ برای هر هنگرد $\{(p_i, |\psi_i\rangle)\}_{i=0}^{k-1}$ ، عملگر

$$\rho = \sum_{i=0}^{k-1} p_i |\psi_i\rangle \langle \psi_i|$$

یک عملگر چگالی است.

در ادامه، اصول مکانیک کوانتومی را در فرمول‌بندی حالت‌های مخلوط بیان می‌کنیم.

²¹Schmidt coefficients

²²Mixed state formalism

²³Density operator

²⁴Mixed state

²⁵Ensemble

اصل ۲۹.۲ فضای حالت به هر سیستم فیزیکی منزوی یک فضای هیلبرت نسبت داده می‌شود که به آن فضای حالت سیستم^a می‌گویند. حالت^b سیستم، یک عملگر چگالی است که روی فضای حالت آن تعریف شده است. حالت یک هنگرد $\{(p_i, \rho_i)\}_{i=0}^{k-1}$ نیز برابر با عملگر چگالی $\rho = \sum_{i=0}^{k-1} p_i \rho_i$ است [۷۳].

اصل ۳۰.۲ تحول زمانی اگر حالت یک سیستم بسته‌ی کوانتومی در لحظه‌ی t_1 ، ρ_{t_1} باشد، حالت سیستم در لحظه‌ی $t_2 > t_1$ با

$$\rho_{t_2} = U \rho_{t_1} U^\dagger$$

مشخص می‌شود که U نگاشتی یکانی است که تنها به $t_2 - t_1$ وابسته است.

اصل ۳۱.۲ سیستم‌های مرکب فضای حالت یک سیستم مرکب که متشکل از n زیرسیستم با فضاهای حالت V_1, \dots, V_n است، برابر است با $V_1 \otimes \dots \otimes V_n$. همچنین اگر هر یک از زیرسیستم‌ها حالت ρ_i را داشته باشند، حالت سیستم مرکب برابر با $\rho_1 \otimes \dots \otimes \rho_n$ خواهد بود [۷۳].

اصل ۳۲.۲ اندازه‌گیری مقصود از یک اندازه‌گیری با m نتیجه‌ی ممکن روی یک سیستم کوانتومی، خانواده‌ای از عملگرها مانند $M = \{M_1, \dots, M_m\}$ است (M_i متناظر با نتیجه‌ی i ام است) که روی فضای حالت آن سیستم عمل می‌کنند و شرط $\sum_{i=1}^m M_i^\dagger M_i = \mathbb{I}$ را نیز برآورده می‌کنند. هنگامی که این اندازه‌گیری روی سیستمی که در حالت ρ قرار دارد انجام می‌شود، نتیجه‌ی اندازه‌گیری با احتمال

$$p(i) = \text{tr}(M_i^\dagger M_i \rho),$$

برابر با i خواهد بود؛ و در این صورت، حالت سیستم به حالت

$$\frac{M_i \rho M_i^\dagger}{\text{tr}(M_i^\dagger M_i \rho)}$$

فرو خواهد ریخت^c [۷۳].

^aState Space

^bState

^cCollapse

در این جا شایان ذکر است که می‌توان فرمالیسم فوق را بیش از این نیز تعمیم داد. این کار که توسط کراوس و چوی انجام شده است [۶۹]، منجر به تعریف نگاشت‌هایی می‌شود که به آن‌ها دینامیک کوانتومی^{۲۶} یا کانال‌های کوانتومی^{۲۷} می‌گویند. بر اساس این فرمول‌بندی، قادر خواهیم بود که مدلی برای محاسبات کوانتومی بسازیم که با مدلی که در بالا ارائه شد، معادل است، اما برخی دشواری‌های آن را ندارد [۹].

تعریف ۳۳.۲ فرض کنید ρ حالت یک سیستم مرکب باشد که از دو مولفه‌ی A و B تشکیل شده است. گوئیم ρ دارای حالت ضربی^{۲۸} است هرگاه حالت‌های ρ_A برای سیستم A و حالت ρ_B برای سیستم B وجود داشته باشد چنانکه

$$\rho = \rho_A \otimes \rho_B.$$

ρ را جداشدنی^{۲۹} نامیم هرگاه حالت‌های ضربی $\rho_A^k \otimes \rho_B^k, \dots, \rho_A^1 \otimes \rho_B^1$ و k عدد حقیقی نامنفی $\lambda_1, \dots, \lambda_k$ وجود داشته باشند به طوری که $\sum_{i=1}^k \lambda_i = 1$ و

$$\rho = \sum_{i=1}^k \lambda_i \rho_A^i \otimes \rho_B^i.$$



در غیر این صورت، ρ درهم‌تنیده^{۳۰} نامیده می‌شود.

²⁶quantum dynamic maps

²⁷quantum channels

²⁸product state

²⁹separable

³⁰entangled

در زیربخش ۳.۲.۲ به مسأله‌ی جداپذیری^{۳۱} اشاره کردیم؛ این مسأله که آیا می‌توان تعیین کرد که حالت یک سیستم دو بخشی (یا در حالت کلی‌تر یک سیستم چند بخشی) جداشدنی است یا نه. همان‌گونه که دیدیم، در فرمول‌بندی حالت خالص، الگوریتمی موثر برای پاسخ‌دادن به این مسأله وجود دارد. شایان ذکر است که وقتی از فرمول‌بندی حالت‌های خالص به فرمول‌بندی حالت‌های مخلوط کوچ می‌کنیم، چنین الگوریتمی دیگر شناخته شده نیست. گرویتس در [۵۷] نشان داده است که مسأله‌ی جداپذیری ماتریس‌های چگالی مسأله‌ای \mathcal{NP} -سخت است؛ نتیجه‌ای که نسخه‌های قوی‌تری از آن نیز توسط قریبان در [۴۹] اثبات شده است. این نشان می‌دهد که اگرچه فرمول‌بندی حالت‌های خالص و مخلوط از بسیاری جهات به یکدیگر شبیهند، اما از جهاتی نیز تفاوت‌های عمیقی با یکدیگر دارند. نهایتاً، این بخش را با اشاره به یکی از مزیت‌های فرمول‌بندی حالت‌های مخلوط به پایان می‌بریم؛ این که این فرمالیسم ما را قادر می‌سازد حالت یک زیرسیستم از یک سیستم مرکب درهم‌تنیده را توصیف کنیم. بدین منظور، ابتدا عملگر رد جزئی را معرفی می‌کنیم.

تعریف ۳۴.۲ فرض کنید که ρ حالت دلخواهی برای یک سیستم مرکب باشد که از دو زیرسیستم A و B با فضاهای حالت \mathbb{C}^m و \mathbb{C}^n تشکیل شده است. به عبارت دیگر $\rho \in \mathcal{L}(\mathbb{C}^n \otimes \mathbb{C}^m)$. رد جزئی نسبت به زیرسیستم B یک نگاشت خطی مانند $tr_B : \mathcal{L}(\mathbb{C}^n \otimes \mathbb{C}^m) \rightarrow \mathcal{L}(\mathbb{C}^n)$ است که به صورت

$$tr_B(\rho) = \sum_{j=0}^{m-1} (\mathbb{I}_n \otimes \langle w_j |) \rho (\mathbb{I}_n \otimes |w_j \rangle),$$

تعریف شده است، که در آن \mathbb{I}_n نگاشت همانی روی \mathbb{C}^n را مشخص می‌کند و $\{|w_j\rangle\}_{j=0}^{m-1}$ پایه‌ی متعامد یکه‌ای برای \mathbb{C}^m است. به طور مشابه، رد جزئی نسبت به زیرسیستم A نگاشت خطی $tr_A : \mathcal{L}(\mathbb{C}^n \otimes \mathbb{C}^m) \rightarrow \mathcal{L}(\mathbb{C}^m)$ است که به صورت

$$tr_A(\rho) = \sum_{i=0}^{n-1} (\langle v_i | \otimes \mathbb{I}_m) \rho (|v_i \rangle \otimes \mathbb{I}_m),$$

تعریف شده است که \mathbb{I}_m عملگر همانی روی \mathbb{C}^m ، و $\{|v_i\rangle\}_{i=0}^{n-1}$ پایه‌ای متعامد یکه برای \mathbb{C}^n هستند. ▶ با داشتن تعریف فوق در دست، حالت زیرسیستم A (یا B) از سیستمی که در حالت ρ قرار دارد برابر است با $tr_B(\rho)$ (یا $tr_A(\rho)$). به سادگی می‌توان دید که این توصیف از حالت یک زیرسیستم با آن چه در حالات ضربی در فرمالیسم حالت‌های خالص به دست می‌آید نیز تطابق دارد.

۳.۲ پیش‌نیازهای علوم کامپیوتر

در ادامه‌ی این پایان‌نامه، فرض می‌کنیم که خواننده با مفاهیم نظریه‌ی پیچیدگی محاسبه‌ی کلاسیک آشنایی دارد. خواننده می‌تواند برای آشنایی با این مفاهیم به مرجع [۱۷] مراجعه کند. یکی از مفاهیمی که در پیچیدگی محاسبات کوانتومی به صورت گسترده‌ای مورد استفاده قرار می‌گیرد، مفهوم مسأله‌ی قراردادی است. مسأله‌های قراردادی نخستین‌بار توسط ایون، سلمان و یاکوبی در [۴۶]، به عنوان تعمیمی از مفهوم مسأله‌های تصمیم‌گیری^{۳۲} معرفی شدند. در پیچیدگی محاسبات کلاسیک، کلاس‌های پیچیدگی معمولاً مجموعه‌هایی از مسأله‌های تصمیم‌گیری هستند؛ در حالی که در پیچیدگی محاسبات کوانتومی، بنا به دلایلی تعریف کلاس‌ها به عنوان مجموعه‌ای از مسأله‌های قراردادی رجحان یافته است.

تعریف ۳۵.۲ یک مسأله‌ی قراردادی^{۳۳} عبارت است از زوج مرتبی مانند $\Pi = (\Pi_{Yes}, \Pi_{No})$ ، به طوری که $\Pi_{Yes} \cap \Pi_{No} = \emptyset$ و $\Pi_{Yes}, \Pi_{No} \subseteq \{0, 1\}^*$. در حالتی که ورودی مسأله عضو $\Pi_{Yes} \cup \Pi_{No}$ باشد، می‌گوییم ورودی قرارداد مسأله را برآورده می‌کند. روشن است که اگر $\Pi_{Yes} \cup \Pi_{No} = \{0, 1\}^*$ ، Π یک مسأله‌ی تصمیم‌گیری خواهد بود. ▶

در ادامه، مقصودمان از این که الگوریتمی یک مسأله‌ی قراردادی $\Pi = (\Pi_{Yes}, \Pi_{No})$ را حل می‌کند این است که اگر ورودی عضو Π_{Yes} باشد، الگوریتم به ازای آن ورودی خروجی «بله» می‌دهد و اگر ورودی عضو Π_{No} باشد، خروجی الگوریتم به ازای آن ورودی «خیر» خواهد بود. به جز این، برای ورودی‌هایی که عضو $\Pi_{Yes} \cup \Pi_{No}$ نباشند، خروجی الگوریتم می‌تواند دلخواه باشد. حل کردن یک مسأله‌ی قراردادی را می‌توان در ساختار حل‌پذیری تصادفی نیز، کاملاً

³¹separability problem

³²decision problem

³³promise problem

مشابه با حل‌پذیری دقیق، تعریف کرد. کافی است حل مسأله را برای ورودی‌هایی که قرارداد مسأله را برآورده می‌کنند مشابه با حل یک مسأله‌ی تصمیم‌گیری تعریف کنیم؛ و برای ورودی‌هایی که قرارداد را برآورده نمی‌کنند، خروجی الگوریتم را دلخواه در نظر بگیریم.

یادداشت ۳۶.۲ به سادگی می‌توان دید که هر مسأله‌ی قراردادی معادل با یک تابع جزئی^{۳۴} روی $\{0, 1\}^*$ است که دامنه‌ی تعریف آن مجموعه‌ی $\Pi_{Yes} \cup \Pi_{No}$ می‌باشد. بعلاوه، مقدار تابع روی Π_{Yes} و Π_{No} به ترتیب برابر با ۱ و صفر است.

▷

مفهوم دیگری که در ادامه‌ی بحث به طور گسترده مورد استفاده قرار خواهد گرفت، مدل محاسبه‌ی مداری است. مدل محاسبه‌ی مداری، نوعی از مدل‌های غیریکنواخت محاسبه است. در این مدل‌ها، روشی که برای حل مسأله مورد استفاده قرار می‌گیرد، با توجه به طول ورودی مسأله می‌تواند تغییر کند. برای مثال در مدل مداری، برای هر n ، پاسخ مسأله برای ورودی‌های به طول n با یک مدار متفاوت تعیین می‌شود. به این ترتیب، یک مدل محاسبه‌ی مداری، خانواده‌ای نامتناهی از مدارها مانند (C_0, C_1, C_2, \dots) است که C_i مداری است که پاسخ مسأله را برای ورودی‌های به طول i تعیین می‌کند. در این‌جا ممکن است این مشکل به ذهن برسد که مدل‌های محاسبه‌ی مداری، در تضاد با روح محاسبه هستند؛ چه آن‌که محاسبه چیزی نیست جز ارائه‌ی توصیفی متناهی برای مجموعه‌های نامتناهی. برای رفع این مشکل، راه‌حل‌های متفاوتی وجود دارد. یک راه این است که این فرض را اضافه کنیم که توصیف مدل مداری، خود، توصیفی متناهی دارد. مثلاً، ماشین تورینگی وجود دارد که روی ورودی 1^n ، توصیف مدار C_n را خروجی می‌دهد. در این حالت، اصطلاحاً گوییم مدار مزبور یک مدار یکنواخت است. یک قضیه‌ی استاندارد در پیچیدگی محاسبه‌ی کلاسیک این است که اگر مدارهایی مانند (C_0, C_1, C_2, \dots) را در نظر بگیریم که ماشین تورینگی که توصیف C_n را با ورودی 1^n تولید می‌کند در زمان چندجمله‌ای کار کند، در این صورت کلاس زبان‌هایی که با چنین مدارهایی توصیف می‌شود، همان کلاس \mathcal{P} است.

³⁴partial function

۳ مدل محاسبات مداری کوانتومی

کامپیوترها اشیائی فیزیکی هستند؛ و محاسبه نیز فرایندی فیزیکی است. آنچه که کامپیوترها می‌توانند یا نمی‌توانند انجام دهند، تنها با قوانین فیزیک مشخص می‌شود؛ و نه با ریاضیات محض.

دیوید دویج

در این فصل به معرفی الگوریتم‌های کوانتومی و کلاس‌های مهمی مسائل قابل حل با الگوریتم‌های کوانتومی کارا خواهیم پرداخت. پیش از آن که به طور دقیق مقصودمان از یک الگوریتم کوانتومی را بیان کنیم، خالی از لطف نیست که توصیفی غیر دقیق، اما شهودبخش از یک الگوریتم کوانتومی داشته باشیم. این توضیحات، برگرفته از مرجع [۹۲] است.

یک الگوریتم را می‌توان یک سیستم دینامیکی با زمان گسسته دانست که فضای فاز آن نیز گسسته است. در واقع، فضای فاز چنین سیستم‌هایی عبارت است از مجموعه‌ای از رشته‌ها (در الفبایی دلخواه، که در ادامه برای راحتی فرض می‌کنیم مجموعه‌ای $\{0, 1\}$ است) که کد شده‌ی پیکربندی ماشین محاسبه در هر لحظه هستند. قانون انتقال حالت این سیستم دینامیکی، به این صورت است که در گذر هر لحظه، به طور موضعی رشته‌ای که متناظر با حالت فعلی سیستم است را تغییر داده و آن را به رشته‌ای دیگر، متناظر با حالتی دیگر در فضای فاز، تبدیل می‌کند. در ادامه برای سادگی بیشتر، فرض کنید که اعضای فضای فاز همگی رشته‌هایی به طول n هستند^{۳۵}. با چنین فرمالیسمی، محاسبه‌ی یک ورودی توسط یک ماشین محاسبه، در واقع معادل با یک مسیر^{۳۶} در سیستم دینامیکی متناظر با آن است.

با داشتن این ایده در ذهن، انواع مختلف مدل‌های محاسبه را می‌توان به این صورت، معادل با انواع مختلفی از سیستم‌های دینامیکی دانست. برای مثال، یک مدل محاسباتی احتمالاتی، عملاً همان مدل فوق است؛ با این تفاوت که هر حالت سیستم متناظر با آن برابر است با یک بردار 2^n تایی توزیع احتمال روی 2^n عضو متمایز $\{0, 1\}^n$ ؛ یا معادلاً، ترکیب محدبی مانند $\sum_{x \in \{0, 1\}^n} p_x x$. قانون انتقال حالت سیستم نیز متشکل از اعمالی موضعی است که در طول زمان این بردار حالت‌ها را تغییر می‌دهند.

با این مقدمه، محاسبات کوانتومی را می‌توان با استفاده از تعبیر سیستم دینامیکی فوق مورد بررسی قرار داد. در حقیقت، حالت سیستم در هر لحظه، برداری 2^n تایی مانند $(\alpha_x)_{x \in \{0, 1\}^n}$ است که هر درایه‌ی آن عددی مختلط است؛ و این بردار با نرم L_2 برداری یک‌ه است. حالت سیستم با استفاده از اعمالی موضعی تغییر می‌کند که نگاشت‌هایی خطی و یکانی روی بردار حالت اعمال می‌کنند. نهایتاً خروجی الگوریتم با اندازه‌گیری حالت سیستم مشخص می‌شود. برای سادگی فرض کنید نتیجه‌ی این اندازه‌گیری یک رشته‌ی n بیتی است. در این صورت نتیجه‌ی یک اندازه‌گیری به صورت کاملاً تصادفی یکی از رشته‌های 2^n $\{0, 1\}^n$ خواهد بود که با توزیع احتمال $(|\alpha_x|^2)_{x \in \{0, 1\}^n}$ مشخص می‌شود. به طور خلاصه، یک الگوریتم کوانتومی عبارت است از اعمال متناهی نگاشت موضعی نابدیبه‌ی یکانی بر بردار اولیه‌ای واقع در کره‌ی واحد فضای \mathbb{C}^{2^n} که در پایان الگوریتم، با استفاده از اندازه‌گیری، به یک بردار توزیع احتمال تبدیل می‌شوند.

گرچه توضیحات نادقیق فوق، شهودی از کارکرد و ساختار یک الگوریتم کوانتومی در اختیار ما می‌گذارد، دور از انتظار نیست که در تعریف کردن یک «الگوریتم کوانتومی» به صورت دقیق، به همان اندازه که تعریف کردن دقیق مفهوم «الگوریتم» در حالت کلاسیک چالش‌برانگیز است، با مشکل مواجه شویم. در حقیقت، مدل‌های مختلف محاسبات کوانتومی، نظیر مدل ماشین تورینگ کوانتومی یا مدل محاسبات مداری کوانتومی، تعاریف متفاوتی از الگوریتم‌های کوانتومی را در اختیار ما قرار می‌دهند. در این فصل، ما بر مدل محاسبات مداری کوانتومی تمرکز خواهیم کرد، و می‌توان نشان داد که با گذر از ماشین‌های تورینگ به مدل مداری، چیز زیادی را نیز از دست نخواهیم داد [۳۲].

۱.۳ الگوریتم‌های کوانتومی

تعریف ۱.۳ یک گیت کوانتومی k موضعی روی یک رجیستر n -کیوبیتی، نگاشتی یکانی است که به طور نابدیبه‌ی روی k کیوبیت از رجیستر عمل می‌کند؛ و عمل آن روی باقی کیوبیت‌ها نگاشت همانی است. ▶

فرض کنید $U \in \mathcal{L}((\mathbb{C}^2)^{\otimes k})$ نگاشتی یکانی و $(i_1, i_2, \dots, i_k) \in \llbracket n \rrbracket^k$ یک k تایی با درایه‌های متمایز باشد. در این صورت یک گیت کوانتومی k موضعی که نگاشت U را بر کیوبیت‌های i_1, i_2, \dots, i_k از یک رجیستر n کیوبیتی اعمال کرده و اثر آن بر باقی کیوبیت‌ها همانی است، نگاشتی مانند $U_{(i_1, \dots, i_k)}$ است که به صورت زیر تعریف می‌شود:

$$\bullet \text{ اگر } k = 1 :$$

^{۳۵} این فرض چندان دور از ذهن نیست. به عنوان مثال، سیستم دینامیکی متناظر با یک مدار محاسبه روی n بیت، مثالی از چنین سیستمی است.

^{۳۶} trajectory

$$U_{(i_1)} = I^{\otimes(i_1-1)} \otimes U \otimes I^{\otimes(n-i_1)}$$

• اگر $k > 1$: می‌دانیم که می‌توان نوشت:

$$U = \sum_j U^{1,j} \otimes \dots \otimes U^{k,j},$$

که هر $U^{i,j}$ نگاشتی یکانی روی \mathbb{C}^2 است. در این حالت:

$$U_{(i_1, \dots, i_k)} = \sum_j U_{(i_1)}^{1,j} \dots U_{(i_k)}^{k,j}.$$

در ادامه چنانچه از زمینه‌ی بحث روشن باشد که گیت‌های موضعی بر چه کیوبیت‌هایی به صورت نابديهی عمل می‌کنند، از نوشتن بانویس (i_1, \dots, i_k) برای $U_{(i_1, \dots, i_k)}$ اجتناب خواهیم کرد.

تعریف ۲.۳ فرض کنید B مجموعه‌ای ثابت از نگاشت‌های یکانی باشد. یک مدار کوانتومی روی n کیوبیت، نگاشتی مانند $U \in \mathcal{L}((\mathbb{C}^2)^{\otimes n})$ است که به صورت زیر تعریف شده است:

$$U = U_{\alpha_1} \otimes U_{\alpha_2} \dots \otimes U_{\alpha_s},$$

که در آن U_{α_i} ها گیت‌های کوانتومی k_i موضعی روی n کیوبیت هستند که از روی نگاشت‌های $U^i \in B$ ساخته شده‌اند، و $\alpha_i \in \llbracket n \rrbracket^{k_i}$. مجموعه‌ی B یک پایه برای مدار U نامیده می‌شود. هم‌چنین به عدد s اندازه‌ی مدار U گوئیم. ▶
تعریف کردن مفهوم الگوریتم، هدفی است که در قلب نظریه‌ی محاسبه قرار دارد و نیل به آن، نیازمند انتخاب مدل مناسبی برای محاسبه است. مدل محاسباتی رایج در ادبیات فعلی نظریه‌ی محاسبات کوانتومی، مدل محاسبات مداری است؛ گرچه از نظر تاریخی ماشین‌های تورینگ کوانتومی اولین مدلی هستند که برای مطالعه‌ی مفاهیم محاسبات کوانتومی مورد استفاده قرار گرفته‌اند [۱۱]. ما تا به این‌جا مفهوم مدار کوانتومی را به طور دقیقی تعریف کردیم. در ادامه، مختصراً سه سناریوی مختلف برای تعریف مفهوم الگوریتم کوانتومی را معرفی خواهیم کرد و خواهیم دید که هر یک از این سناریوها، ما را به منابع محاسباتی مختلفی که هر یک می‌توانند مبنای ساختن نظریه‌ای برای پیچیدگی محاسبات کوانتومی قرار گیرند، رهنمون خواهند کرد.

یادداشت ۳.۳ الگوریتم‌های کوانتومی را می‌توان به طرق مختلفی تعریف کرد. در ادامه، مطابق با مرجع [۳۴] به معرفی سه مورد از این روش‌ها خواهیم پرداخت. شایان ذکر است که هر یک از تعاریف زیر مزایای خاص خود را دارند؛ و گرچه هر یک از آن‌ها با دیگری متفاوت است، اما ارتباطاتی نیز میان آن‌ها وجود دارد که به طور مفصلی در ادبیات پیچیدگی محاسبه مورد مطالعه قرار گرفته است.

۱. سناریوی اول: پیچیدگی محاسباتی کوانتومی^{۳۷}

با فرض این‌که تابعی جزئی مانند $\{0, 1\}^m \rightarrow \{0, 1\}^n$: f داده شده باشد، یک الگوریتم که این تابع را محاسبه می‌کند عبارت است از یک مدار کوانتومی که برای هر $x \in \{0, 1\}^n$ ، بر حالت $|x\rangle$ اعمال می‌شود؛ و پس از آن m کیوبیت مشخص اندازه‌گیری می‌شود تا حالتی مانند $|f(x)\rangle$ به دست آید. در این الگوریتم‌ها، منبع محاسباتی مدنظر ما برای اندازه‌گیری پیچیدگی محاسبه، تعداد گیت‌های تشکیل‌دهنده‌ی مدار هستند.

۲. سناریوی دوم: پیچیدگی کوئری کوانتومی^{۳۸}

فرض کنید به عنوان ورودی مسأله، جعبه‌سیاهی به ما داده شده است که تابعی مانند $\{0, 1\}^m \rightarrow \{0, 1\}^n$: f را پیاده‌سازی می‌کند؛ و از ما خواسته شده است که اطلاعاتی درباره‌ی این تابع را با کوئری کردن از این جعبه‌سیاه (یا اوراکل) به دست آوریم. برای پرسیدن کوئری از اوراکلی که تابع f را پیاده‌سازی می‌کند، از نگاشت‌هایی یکانی موسوم به f -گیت بهره می‌گیریم. به این ترتیب، یک الگوریتم که چنین مسأله‌ای را حل می‌کند عبارت است از یک مدار کوانتومی که از گیت‌های استاندارد کوانتومی و f -گیت‌ها تشکیل شده است؛ و بر تعداد مناسبی کیوبیت ورودی اعمال می‌شود (معمولاً لازم است رجیستری که ورودی تابع f را در خود نگه می‌دارد را به یک رجیستر کمکی الحاق کنیم)؛ و پس از آن، تعدادی کیوبیت مشخص اندازه‌گیری می‌شوند و بر اساس نتایج اندازه‌گیری، اطلاعات مورد نظر درباره‌ی تابع f به دست می‌آید. در این الگوریتم‌ها منبع محاسباتی مورد نظر جهت اندازه‌گیری پیچیدگی محاسباتی، تعداد کوئری‌ها (یا تعداد f -گیت‌های استفاده شده در مدار) است.

³⁷quantum computational complexity

³⁸quantum query complexity

۳. سناریوی سوم: پیچیدگی ارتباطی کوانتومی^{۳۹}

فرض کنید آلیس و باب دو رجیستر کوانتومی $|x\rangle$ و $|y\rangle$ در اختیار دارند، که $x, y \in \{0, 1\}^n$ ؛ و از آن‌ها خواسته شده است تا مقدار تابعی مانند $f(x, y)$ را محاسبه کنند. یک الگوریتم برای حل این مسأله، که در این سناریو به آن پروتکل نیز گفته می‌شود، عبارت است از دو مدار کوانتومی، که هر یک در اختیار یکی از آلیس و باب است، و بر کیوبیت‌هایی که در اختیار هر یک از آن‌هاست اعمال می‌شود. این کیوبیت‌ها می‌توانند بین آلیس و باب انتقال یابند (به این معنی که هر یک برای دیگری کیوبیت‌هایی بفرستند)؛ و نهایتاً خروجی با اندازه‌گیری کیوبیت‌های مشخصی از رجیستری که در اختیار یکی از آن‌هاست (مثلاً باب)، تعیین می‌شود. در این سناریو، منبع محاسباتی مورد نظر ما تعداد کیوبیت‌های انتقال یافته میان طرفین است.

▷

با وجود آن‌که هدف این پایان‌نامه مطالعه‌ی کلاس‌های پیچیدگی‌ای است که در سناریوی پیچیدگی محاسباتی کوانتومی مورد مطالعه قرار می‌گیرند، در بخش بعد مثال‌هایی از الگوریتم‌هایی که در چهارچوب پیچیدگی کوئری معرفی شده‌اند را ارائه خواهیم کرد. انگیزه‌مان از ارائه‌ی مثال‌هایی که در این چهارچوب طراحی شده‌اند، چند چیز است: یکی این باور عمومی که مدل پیچیدگی کوئری، چهارچوبی طبیعی برای کشف الگوریتم‌های جدید کوانتومی است؛ و بسیاری از الگوریتم‌هایی که در این چهارچوب طراحی می‌شوند را می‌توان به الگوریتم‌هایی که در چهارچوب پیچیدگی محاسباتی کوانتومی تعریف شده‌اند تبدیل کرد [۳۴]. علاوه، در چهارچوب پیچیدگی کوئری می‌توان با اجتناب از بسیاری جزئیات تکنیکال، شهود خوبی از نحوه‌ی طراحی الگوریتم‌های کوانتومی به دست آورد؛ و به روشنی دید که چگونه الگوریتم‌های کوانتومی می‌توانند منجر به تسریع‌هایی نسبت به الگوریتم‌های کلاسیک می‌شوند. به همین دلیل، این چهارچوب می‌تواند نقطه‌ی شروع مناسبی برای افرادی که آشنایی پیشینی با محاسبات کوانتومی ندارند، باشد.

پیش از آن‌که به بیان مثال‌هایی از الگوریتم‌های کوانتومی بپردازیم، در خاتمه‌ی این بخش، به تعریف دقیق مفهوم کوئری‌زدن به یک اوراکل کوانتومی خواهیم پرداخت. برای پیاده‌سازی یک کوئری به اوراکلی که محقق‌کننده‌ی تابعی مانند $f: \{0, 1\}^m \rightarrow \{0, 1\}^n$ است، نیازمند گیتی هستیم که در ورودی، حالتی مانند $|x\rangle$ ، که $x \in \{0, 1\}^n$ ، دریافت کند و حالت $|f(x)\rangle$ را خروجی دهد. توجه کنید که نحوه‌ی پیاده‌سازی چنین گیتی (مثلاً با استفاده از گیت‌های استاندارد کوانتومی) نگرانی ما نیست؛ زیرا در مدل کوئری فرض می‌شود که چنین اوراکلی به عنوان ورودی مسأله به ما داده شده است. با این حال باید به این نکته توجه کرد که طبق اصل ۱۷.۲، هر گیت کوانتومی باید یک نگاشت یکانی باشد؛ و این در حالی است که تابع دلخواهی مانند f ، حتی ممکن است وارون‌پذیر نیز نباشد. به این ترتیب، ضروری است که برای توابع دلخواه، تعریف f -گیت‌ها را به طور مناسبی تغییر دهیم. بدین منظور، از یک رجیستر اضافی در کنار رجیستری که $|x\rangle$ در آن قرار می‌گیرد، استفاده می‌کنیم؛ و با توجه به کاربرد این رجیستر اضافی، به آن رجیستر کمکی می‌گوییم.

تعریف ۴.۲ برای تابعی دلخواه مانند $f: \{0, 1\}^n \rightarrow \{0, 1\}^m$ ، یک f -گیت عبارت است از نگاشتی یکانی مانند $U_f: (\mathbb{C}^2)^{\otimes m} \otimes (\mathbb{C}^2)^{\otimes n} \rightarrow (\mathbb{C}^2)^{\otimes m} \otimes (\mathbb{C}^2)^{\otimes n}$ که بر روی یک رجیستر n کیوبیتی اصلی و یک رجیستر m کیوبیتی کمکی عمل می‌کند و به صورت زیر تعریف شده است:

$$\forall |x\rangle \in (\mathbb{C}^2)^{\otimes n} \quad \forall |y\rangle \in (\mathbb{C}^2)^{\otimes m}, \quad U_f(|x\rangle |y\rangle) = |x\rangle |y \oplus f(x)\rangle,$$

►

که در آن، \oplus نمایانگر XOR بیت به بیت است. به سادگی می‌توان دید که نگاشت تعریف شده در بالا نگاشتی یکانی، و در نتیجه یک گیت کوانتومی است.

۲.۳ مثال‌هایی از الگوریتم‌های کوانتومی

در این بخش، به معرفی سه الگوریتم کوانتومی خواهیم پرداخت؛ آنالیزی برای درستی این الگوریتم‌ها ارائه خواهیم داد؛ و مقایسه‌ای اجمالی میان پیچیدگی الگوریتم‌های کوانتومی ارائه‌شده با الگوریتم‌های کلاسیک موجود برای مسأله ارائه خواهیم کرد.

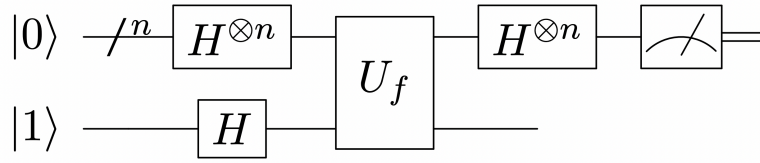
۱.۲.۳ الگوریتم دویچ-جوزا

الگوریتم دویچ-جوزا^{۴۰} اولین بار توسط دیوید دویچ و ریچارد جوزا در [۴۱] معرفی شد و سپس توسط موسکا و همکاران در [۳۳] بهبود یافت. هدف این الگوریتم حل مسأله‌ی زیر است:

³⁹quantum communication complexity

⁴⁰Deutsch-Jozsa algorithm

شکل ۱: شمایی از الگوریتم دویچ-جوزا. خط مورب با بالانویس n ، نمایش دهنده‌ی یک رجیستر n کیوبیتی و اندازه‌گیری‌ها در پایه‌ی محاسباتی است.



مسأله‌ی دویچ-جوزا

ورودی: دسترسی اوراکلی به تابعی مانند $f: \{0, 1\}^n \rightarrow \{0, 1\}$; که قرارداد شده است که یا تابعی ثابت و یا تابعی متوازن^a باشد.
سوال: مشخص کنید که f ثابت است یا متوازن.

^abalanced

توجه کنید که تابع بولی $f: \{0, 1\}^n \rightarrow \{0, 1\}$ را متوازن می‌نامیم، هرگاه

$$\text{card}(\{x \in \{0, 1\}^n : f(x) = 0\}) = \text{card}(\{x \in \{0, 1\}^n : f(x) = 1\}).$$

دویچ و جوزا برای حل مسأله‌ی فوق، الگوریتم زیر را پیشنهاد دادند:

الگوریتم

۱. روی رجیستر اصلی و کمکی تبدیل هادامارد $H^{\otimes(n+1)}$ را اعمال می‌کنیم.
۲. نگاشت U_f را بر هر دو رجیستر اعمال می‌کنیم.
۳. تبدیل هادامارد $H^{\otimes n}$ را بر رجیستر اصلی اعمال می‌کنیم.
۴. رجیستر اصلی را در پایه‌ی محاسباتی اندازه می‌گیریم. حالت سیستم پس از اندازه‌گیری $|0\rangle^{\otimes n}$ است اگر و تنها اگر f تابعی ثابت باشد.

نمایش گرافیکی مدار کوانتومی الگوریتم دویچ-جوزا در شکل ۱ نمایش داده شده است. برای آنالیز درستی الگوریتم از دولم زیر، که بدون اثبات ذکر شده‌اند، استفاده می‌کنیم.

لم ۵.۳ برای هر $x \in \{0, 1\}^n$ و هر تابع $f: \{0, 1\}^n \rightarrow \{0, 1\}$ ،

$$U_f(|x\rangle|-\rangle) = (-1)^{f(x)}|x\rangle|-\rangle.$$

لم ۶.۳ برای هر $x \in \{0, 1\}^n$ ،

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0, 1\}^n} (-1)^{x \cdot z} |z\rangle,$$

که در آن برای $x = x_1 x_2 \dots x_n$ و $z = z_1 z_2 \dots z_n$

$$x \cdot z = x_1 z_1 + x_2 z_2 + \dots + x_n z_n.$$

با استفاده از دولم فوق، می‌توان حالت رجیسترها را پس از اعمال گیت‌های کوانتومی و پیش از اندازه‌گیری نهایی به دست آورد. اگر این حالت را با $|\psi\rangle$ نمایش دهیم، داریم:

$$\begin{aligned} |\psi\rangle &= (H^{\otimes n} \otimes I) U_f H^{\otimes(n+1)} (|0\rangle^{\otimes n} |1\rangle) \\ &= (H^{\otimes n} \otimes I) U_f (|+\rangle^n |-\rangle) \\ &= (H^{\otimes n} \otimes I) U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |-\rangle \right) \\ &= (H^{\otimes n} \otimes I) \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes |-\rangle \right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \otimes |-\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x) + x \cdot z} |z\rangle \otimes |-\rangle \end{aligned}$$

حال توجه کنید که اگر تابع f ، تابعی ثابت باشد، ضریب جمله‌ی $|-\rangle \otimes |0\rangle^{\otimes n}$ در مجموع بالا برابر با ± 1 خواهد بود؛ و اگر f متوازن باشد، این ضریب برابر با صفر است. به این ترتیب با توجه به قرارداد مسأله، که تضمین شده تابع f یا ثابت و یا متوازن است، نتیجه خواهیم گرفت که حالت رجیستر n تایی پس از اندازه‌گیری نهایی برابر با $|0\rangle^{\otimes n}$ است، اگر و تنها اگر f تابعی ثابت باشد.

در بالا نشان دادیم که الگوریتم دویچ-جوزا مسأله را با تنها یک کوثری به اوراکل حل می‌کند. شایان توجه است که یک الگوریتم قطعی کلاسیک برای حل مسأله در بدترین حالت نیاز به پرسیدن $\theta(2^n)$ کوثری از اوراکل دارد. با این حال، الگوریتم‌های تصادفی کلاسیکی وجود دارند که مسأله را با احتمال خطای حداکثر $\frac{1}{q}$ ، با پرسیدن q کوثری، حل می‌کنند.

۲.۲.۳ الگوریتم سایمون

الگوریتم سایمون^{۴۱} نخستین بار توسط دانیل سایمون در [۸۰] ارائه شده است. مسأله‌ای که این الگوریتم آن را حل می‌کند به شرح زیر است:

مسأله‌ی سایمون

ورودی: دسترسی اوراکلی به تابع $f: \{0,1\}^n \rightarrow \{0,1\}^n$ با این ویژگی که قرارداد شده است که رشته‌ای مانند $s \in \{0,1\}^n$ وجود دارد به طوری که برای هر دو رشته‌ی $x, y \in \{0,1\}^n$ ، $f(x) = f(y)$ اگر و تنها اگر $x = y \oplus s$ یا $x = y$ خروجی: رشته‌ی s .

سایمون الگوریتم زیر را برای حل مسأله‌ی فوق ارائه داد:

الگوریتم

۱. با دو رجیستر n بیتی شروع می‌کنیم که هر یک در حالت $|0\rangle^{\otimes n}$ آماده‌سازی شده‌اند. به علاوه، قرار می‌دهیم $Y = \emptyset$.

۲. مراحل زیر را $\mathcal{O}(n)$ بار تکرار می‌کنیم:

- (آ) روی رجیستر اول تبدیل هادامارد $H^{\otimes n}$ را اعمال می‌کنیم.
- (ب) نگاشت U_f را روی رجیستر اول و دوم اعمال می‌کنیم.
- (ج) رجیستر دوم را در پایه‌ی محاسباتی اندازه‌گیری می‌کنیم.

⁴¹Simon's algorithm

(د) تبدیل هادامارد $H^{\otimes n}$ را روی رجیستر اول اعمال می‌کنیم.

(ه) رجیستر اول را اندازه می‌گیریم. فرض کنید حالت این رجیستر پس از اندازه‌گیری $|y\rangle$ باشد. در این صورت y را به Y اضافه می‌کنیم.

۳. اگر Y شامل n بردار مستقل خطی باشد، $s = 00\dots 0$.

۴. در غیر این صورت، اگر Y شامل $n-1$ بردار مستقل خطی باشد، بردار s برداری است که بر اعضای Y عمود است. (با حل یک دستگاه خطی، s را می‌یابیم).

۵. در غیر این صورت، خروجی می‌دهیم: «شکست!»

O:

آنالیز درستی الگوریتم فوق:

- پس از اعمال اولین سری از گیت‌های هادامارد حالت سیستم برابر با $|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^n\rangle$ است.
- سپس با اعمال گیت U_f ، خواهیم داشت:

$$U_f\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^n\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

- با اندازه‌گیری رجیستر دوم، حالت سیستم به حالت

$$\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle) |f(z)\rangle$$

فرو می‌ریزد.

- ابتدا توجه کنید که برای هر رشته‌ی $z \in \{0,1\}^n$

$$H^{\otimes n} |z\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot z} |x\rangle.$$

با توجه به این مطلب، با اعمال سری دوم عملگرهای هادامارد بر رجیستر اول، حالت این رجیستر به صورت زیر خواهد بود:

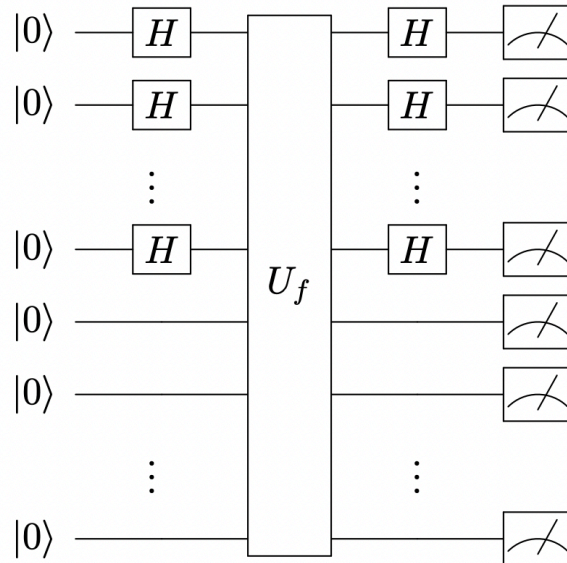
$$\begin{aligned} H^{\otimes n} \frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle) &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} ((-1)^{x \cdot z} + (-1)^{x \cdot (z \oplus s)}) |x\rangle \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} ((-1)^{x \cdot z} (1 + (-1)^{x \cdot s})) |x\rangle \end{aligned}$$

با توجه به این معادله، احتمال این که حالت رجیستر اول پس از اندازه‌گیری $|y\rangle$ باشد، که $y \cdot s \neq 0$ ، برابر با صفر است. بنابراین با اندازه‌گیری رجیستر اول، با احتمال ۱ حالت این رجیستر به $|y\rangle$ فرو می‌ریزد، به طوری که $y \cdot s = 0$.

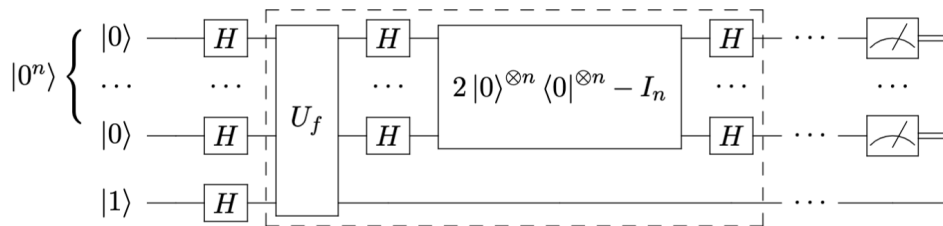
- حال با پیدا کردن $n-1$ بردار مستقل خطی مانند y_1, y_2, \dots, y_{n-1} می‌توان بردار s را به نحوی یافت که بر این $n-1$ بردار عمود باشد. به علاوه، به سادگی می‌توان نشان داد که به طور متوسط $O(n)$ بار اجرای حلقه‌ی سایمون برای یافتن $n-1$ بردار مستقل خطی کافی است.

شمایی از این الگوریتم در شکل ۲ نمایش داده شده است. روشن است که پیچیدگی زمانی اجرای الگوریتم سایمون چند جمله‌ای است. در این جا شایان ذکر است که الگوریتم‌های تصادفی کلاسیکی وجود دارند که مسأله‌ی سایمون را در $O(\sqrt{2^n})$ حل می‌کنند [۹۳]. با این وجود، سایمون در [۸۰] نشان داد که هر الگوریتم کلاسیکی که این مسأله را با احتمال بالا حل کند، نیاز به پرسیدن $\Omega(\sqrt{2^n})$ کوئری دارد؛ و این در حالی است که الگوریتم سایمون مسأله را در زمان $\text{poly}(n)$ حل می‌کند. بنابراین، الگوریتم سایمون نمونه‌ای از آن دسته از الگوریتم‌های کوانتومی است که به طور اثبات‌شده‌ای بر الگوریتم‌های کلاسیک برتری محاسباتی دارند.

شکل ۲: شمایی از الگوریتم سایمون



شکل ۳: شمایی از الگوریتم گروور. قسمتی که دور آن خط چین کشیده شده است، یک تکرار گروور نامیده می‌شود.



۳.۲.۳ الگوریتم جست‌وجوی گروور

الگوریتم گروور^{۴۲}، یکی از مشهورترین الگوریتم‌های کوانتومی (احتمالاً بعد از الگوریتم شور) است. این الگوریتم در سال ۱۹۹۶ توسط لادو گروور در [۵۵] ارائه شد و بعدها نسخه‌های متنوع‌تری از آن نیز توسعه یافت [۲۸]. الگوریتم گروور از مهم‌ترین الگوریتم‌های کوانتومی به دست آمده تا امروز است؛ و دلیل آن مسأله‌ی مهم و پرکاربردی است که این الگوریتم حل می‌کند. این مسأله همان‌گونه که در ادامه شرح خواهیم داد، مسأله‌ی جست‌وجو است.

مسأله‌ی جست‌وجوی بدون ساختار

ورودی: دسترسی اوراکلی به تابع $f: \{0, 1\}^n \rightarrow \{0, 1\}$ با این ویژگی که قرارداد شده است، تعداد اعضای مجموعه‌ی $\{x \in \{0, 1\}^n : f(x) = 1\}$ برابر با t است.
خروجی: رشته‌ای مانند $x \in \{0, 1\}^n$ چنانکه $f(x) = 1$.

گروور الگوریتم زیر را برای حل مسأله‌ی فوق پیشنهاد داد. شکل ۳ پیاده‌سازی این الگوریتم را نمایش می‌دهد. (در ادامه فرض کنید $N = 2^n$).

⁴²Grover's algorithm

الگوریتم

۱. با یک رجیستر n بیتی (رجیستر اول) و یک رجیستر ۱ بیتی (رجیستر دوم) شروع می‌کنیم که رجیستر اول در حالت $|0\rangle^{\otimes n}$ و رجیستر دوم در حالت $|1\rangle$ آماده‌سازی شده‌اند.

۲. نگاشت $H^{\otimes(n+1)}$ را بر رجیستر اول و دوم اعمال می‌کنیم.

۳. (تکرار گروور) مراحل زیر را $\mathcal{O}(\sqrt{N})$ بار تکرار می‌کنیم:

(آ) U_f را بر رجیستر اول و دوم اعمال می‌کنیم.

(ب) نگاشت $D = (D_{ij}) : \mathbb{C}^N \rightarrow \mathbb{C}^N$ را که به صورت زیر تعریف شده است بر رجیستر اول اعمال می‌کنیم.

$$D_{ij} = \begin{cases} \frac{1}{N}, & \text{اگر } i \neq j \\ -1 + \frac{1}{N}, & \text{اگر } i = j \end{cases} \quad (21)$$

۴. رجیستر اول را در پایه‌ی محاسباتی اندازه می‌گیریم.

آنالیز درستی الگوریتم فوق:

• نخست توجه کنید که پس از اعمال اولین مجموعه از گیت‌های هادامارد حالت سیستم برابر است با:

$$|\psi\rangle = |+\rangle^{\otimes n} |-\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |-\rangle.$$

• از طرفی، برای هر $x \in \{0,1\}^n$ داریم:

$$\begin{aligned} U_f(|x\rangle |-\rangle) &= \frac{1}{\sqrt{2}} U_f(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} U_f(|x\rangle |0\rangle + |x\rangle |1\rangle) = |x\rangle \frac{1}{\sqrt{2}} (|f(x)\rangle - |f(x) \oplus 1\rangle) \\ &= (-1)^{f(x)} |x\rangle |-\rangle \end{aligned}$$

بنابراین با اعمال گیت U_f بر حالت $|\psi\rangle$ خواهیم داشت:

$$U_f |\psi\rangle = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle |-\rangle \quad (22)$$

از اینجا به بعد، با توجه به این که حالت فعلی سیستم جداشدنی است (و با توجه به معادله‌ی فوق، با اعمال مجدد U_f جداشدنی باقی می‌ماند)، توجه خود را تنها به رجیستر اول معطوف خواهیم کرد. فرض کنید حالت رجیستر اول قبل از اولین تکرار گروور را $|\psi_0\rangle$ بنامیم. بنابراین:

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

$|\psi_0\rangle$ را به صورت زیر بازنویسی می‌کنیم:

$$|\psi_0\rangle = \sqrt{\frac{t}{N}} \left(\frac{1}{\sqrt{t}} \sum_{x:f(x)=1} |x\rangle \right) + \sqrt{\frac{N-t}{N}} \left(\frac{1}{\sqrt{N-t}} \sum_{x:f(x)=0} |x\rangle \right),$$

اگر تعریف کنیم:

$$|G\rangle = \frac{1}{\sqrt{t}} \sum_{x:f(x)=1} |x\rangle,$$

$$|B\rangle = \frac{1}{\sqrt{N-t}} \sum_{x:f(x)=0} |x\rangle,$$

$$\sin \theta = \sqrt{\frac{t}{N}},$$

در این صورت $|\psi_0\rangle$ را می‌توان به صورت زیر بازنویسی کرد:

$$|\psi_0\rangle = \sin \theta |G\rangle + \cos \theta |B\rangle.$$

روشن است که $|\psi_0\rangle$ در صفحه‌ی تولید شده توسط بردارهای متعامد $|G\rangle$ و $|B\rangle$ قرار دارد.

- حال اگر به نگاشت U_f توجه کنیم، از معادله‌ی ۲۲ متوجه می‌شویم که $U_f |G\rangle |-\rangle = -|G\rangle |-\rangle$ و $U_f |B\rangle |-\rangle = |B\rangle |-\rangle$. بنابراین، اگر عمل نگاشت U_f روی رجیستر اول را در نظر بگیریم، به این صورت است که هر بردار در صفحه‌ی تولید شده توسط $|G\rangle$ و $|B\rangle$ را نسبت به بردار $|B\rangle$ بازتاب می‌کند.
- از طرفی به سادگی می‌توان دید که:

$$D = H^{\otimes n} (\mathbb{2} |0^n\rangle \langle 0^n| - I) H^{\otimes n} = \mathbb{2} |\psi_0\rangle \langle \psi_0| - I.$$

مشابه بند قبل، می‌توان دید که $\mathbb{2} |\psi_0\rangle \langle \psi_0| - I$ یک بازتاب در صفحه‌ی دوبعدی تولیدشده توسط $|G\rangle$ و $|B\rangle$ ، حول بردار $|\psi_0\rangle$ را مشخص می‌کند.

- با توجه به دو بند قبل، می‌توان دید با هر بار اعمال یک تکرار گروور، زاویه‌ی بین بردار حاصل و بردار $|B\rangle$ به اندازه‌ی 2θ افزایش می‌یابد. به عبارت دیگر، پس از تکرار k ام گروور حالت رجیستر اول برابر است با:

$$|\psi_k\rangle = \sin(2k + 1)\theta |G\rangle + \cos(2k + 1)\theta |B\rangle.$$

بنابراین، چنانچه پس از تکرار k ام، حالت رجیستر اول را اندازه بگیریم، با احتمال $|\sin(2k + 1)\theta|^2$ حالت سیستم بعد از اندازه‌گیری برابر با $|z\rangle$ است که $f(z) = 1$.

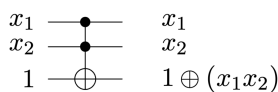
- می‌توان نشان داد برای مقادیر کوچک t ، با اعمال $O\left(\sqrt{\frac{N}{t}}\right)$ بار تکرار گروور، با احتمال خطای کمی، حالت رجیستر اول بعد از اندازه‌گیری برابر است با $|z\rangle$ که $f(z) = 1$. در واقع کافی است k را نزدیک‌ترین عدد صحیح به $\frac{1}{4} \sqrt{\frac{2N}{t}} - \frac{1}{4}$ قرار دهیم، در این صورت $\frac{t}{N}$ کران بالایی برای احتمال خطای الگوریتم خواهد بود، که برای t های به اندازه‌ی کافی کوچک، احتمال ناچیزی خواهد بود.

همان‌گونه که از آنالیز فوق بر می‌آید، الگوریتم گروور پیچیدگی زمانی جست‌وجو را به صورت مربعی تسریع می‌کند.

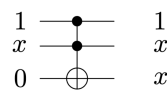
۳.۳ شبیه‌سازی کوانتومی محاسبات کلاسیک

مطالعه‌ی رابطه‌ی بین مدل‌های مختلف محاسبه را می‌توان یکی از مهم‌ترین اهدافی دانست که در نظریه‌ی محاسبه دنبال می‌شود. با توجه به این‌که در این پایان‌نامه، تمرکز خود را بر مدل محاسبات مداری کوانتومی گذاشته‌ایم، بررسی رابطه‌ی این مدل محاسبه با دیگر مدل‌های محاسبه‌ای که مورد استفاده‌ی ما هستند، بالاخص مدل محاسبات مداری کلاسیک، از اهمیت بالایی برخوردار است. این ارتباط می‌تواند از دو منظر محاسبه‌پذیری و پیچیدگی محاسباتی مورد بررسی قرار گیرد. در این بخش، اجمالاً به بررسی این رابطه خواهیم پرداخت؛ و نیز در فصل‌های آتی وجوه بیشتری از این ارتباطات را بررسی خواهیم کرد.

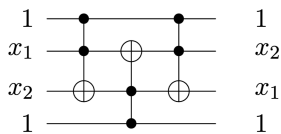
با توجه به تعریف گیت‌های کوانتومی، روشن است که گیت‌های کلاسیکی وجود دارند که نمی‌توان آن‌ها را یک گیت کوانتومی دانست؛ چه آن‌که بسیاری از گیت‌های پایه‌ای در محاسبات کلاسیک حتی وارون‌پذیر نیز نیستند. با این حال، همان‌گونه که از عنوان این بخش بر می‌آید، گیت‌های کلاسیک را می‌توان با گیت‌های کوانتومی شبیه‌سازی کرد. در ادامه به رفع مشکل



(ب) پیاده‌سازی گیت NAND با θ_2 .



(ت) پیاده‌سازی fan-out با θ_2 .



(ج) تعویض کردن دو بیت با یکدیگر با استفاده از θ_2 .

شکل ۴

حضور گیت‌های وارون‌ناپذیر در مدارهای کلاسیک خواهیم پرداخت؛ و نشان خواهیم داد که برای هر مدار کلاسیک، مداری کوانتومی وجود دارد که آن را شبیه‌سازی می‌کند.

تعریف ۷.۲ یک گیت (کلاسیک) برگشت‌پذیر n روی $\{0, 1\}^n$ تابعی وارون‌پذیر مانند $g : \{0, 1\}^n \rightarrow \{0, 1\}^n$ است. یک مدار برگشت‌پذیر، مداری است که فقط از گیت‌های برگشت‌پذیر ساخته شده است و هیچ fan-out ای ندارد.

به سادگی می‌توان دید که هر گیت برگشت‌پذیر مانند $g : \{0, 1\}^n \rightarrow \{0, 1\}^n$ را می‌توان به گیتی کوانتومی مانند $G : (\mathbb{C}^2)^{\otimes n} \rightarrow (\mathbb{C}^2)^{\otimes n}$ گسترش داد؛ به این ترتیب که G را روی بردارهای پایه‌ی محاسباتی به صورت زیر تعریف کنیم:

$$\forall x \in \{0, 1\}^n, \quad G|x\rangle = |g(x)\rangle$$

بنابراین، هر گیت برگشت‌پذیر را می‌توان به جای جدول ارزشش، با نمایش ماتریسی گسترش‌یافته‌ی کوانتومی آن مشخص کرد.

مثال ۸.۳ گیت کلاسیک $\theta_2 : \{0, 1\}^2 \rightarrow \{0, 1\}^2$ که به صورت

$$\forall x_1, x_2, x_3 \in \{0, 1\}, \quad \theta_2(x_1, x_2, x_3) = (x_1, x_2, x_3 \oplus x_1x_2)$$

تعریف شده است، مثالی از یک گیت برگشت‌پذیر است. گسترش‌یافته‌ی کوانتومی این گیت، که با نام گیت توفولی ^{۴۴} شناخته شده و با CCNOT نمایش داده می‌شود، در جدول ۲ معرفی شد.

◇

توفولی نشان داد که $\{\theta_2\}$ یک مجموعه‌ی جهانی از گیت‌ها برای محاسبات برگشت‌پذیر است. در این جا شایان ذکر است که می‌توان اثبات کرد که هیچ مجموعه‌ی جهانی‌ای از گیت‌های ۱ یا ۲ بیتی برای محاسبات برگشت‌پذیر وجود ندارد. دلیل این امر آن است که به سادگی می‌توان دید که نمایش ماتریسی هر گیت ۲ بیتی برگشت‌پذیر مانند $g(x)$ ، یک تبدیل آفین است. به عبارت دیگر،

$$g(x) = Ax + b,$$

که A ماتریس بولی ای 2×2 و وارون‌پذیر و b بردار بولی ای 1×2 است. با توجه به این که نگاشت‌های آفین تحت عمل ترکیب توابع، بسته هستند؛ و گیت‌هایی برگشت‌پذیر (مانند CNOT) وجود دارند که تبدیل آفین نیستند، بنابراین مجموعه‌ای جهانی از گیت‌های ۲ بیتی برگشت‌پذیر برای محاسبات برگشت‌پذیر کلاسیک وجود ندارد.

برای این که نشان دهیم هر مدار کلاسیک برگشت‌ناپذیر را می‌توان به مداری برگشت‌پذیر تبدیل کرد، نخست توجه کنید که هر مدار کلاسیک را می‌توان به مداری تبدیل کرد که فقط از گیت NAND و fan-out تشکیل شده باشد. این کار را می‌توان با استفاده از بیت‌هایی کمکی که مقادیر ثابتی دارند، انجام داد. بنابراین، کافی است نشان دهیم که می‌توان NAND و fan-out را با گیت‌های برگشت‌پذیر جایگزین کرد. این کار را نیز می‌توان با استفاده از گیت θ_2 و بهره گرفتن از بیت‌های کمکی با مقادیر ثابت انجام داد. شکل‌های **آ۴** و **ب۴** نحوه‌ی انجام پذیرفتن این تبدیل را نمایش می‌دهند. نحوه‌ی ساختی که در بالا ارائه کردیم، در کنار این مطلب که تعویض مقادیر دو بیت با یکدیگر با استفاده از گیت θ_2 امکان‌پذیر است (همان‌گونه که در شکل **ج۴** نمایش داده شده است)، قضیه‌ی زیر را نتیجه می‌دهد.

⁴³reversible

⁴⁴Toffoli

قضیه ۹.۳ فرض کنید C مدار کلاسیک برگشت‌ناپذیری است که تابع بولی $f: \{0, 1\}^n \rightarrow \{0, 1\}^m$ را محاسبه می‌کند. در این صورت مدار کلاسیک برگشت‌پذیری مانند C' وجود دارد که تابع $F: \{0, 1\}^{n+L} \rightarrow \{0, 1\}^{n+L}$ را محاسبه می‌کند؛ به طوری که برای مقادیر بولی ثابت $(c_{n+1}, c_{n+2}, \dots, c_{n+L})$ و برای هر $(x_1, x_2, \dots, x_n) \in \{0, 1\}^n$

$$F(x_1, x_2, \dots, x_n, c_{n+1}, c_{n+2}, \dots, c_{n+L}) = (y_1, y_2, \dots, y_m, d_1, d_2, \dots, d_{n+L-m}),$$

که در آن $(y_1, y_2, \dots, y_m) = f(x_1, x_2, \dots, x_n)$ و C' تنها از گیت θ_2 ساخته شده است [۶۱].

یادداشت ۱۰.۳ چنانچه مدار برگشت‌ناپذیری که در ابتدا با آن شروع می‌کنیم و تبدیل بالا را روی آن انجام می‌دهیم اندازه‌ی s ، و عمق d داشته باشد، مدار معادل برگشت‌پذیری که نهایتاً به دست می‌آید، اندازه‌ی $O(s + n + m)$ و عمق $O(d)$ خواهد داشت [۶۶]. این مطلب، در ملاحظات پیچیدگی محاسباتی مان در آینده کاربرد خواهد داشت. بالاخص توجه کنید که اگر مدار اولیه، اندازه‌ی چندجمله‌ای بر حسب طول ورودی مدار داشته باشد، مدار معادل برگشت‌پذیر نیز چنین خواهد بود.

با توجه به بحث بالا، هر مدار کلاسیک (نه لزوماً برگشت‌پذیر)، مداری معادل و برگشت‌پذیر دارد که فقط از گیت‌های θ_2 ساخته شده است. حال، برای به دست آوردن یک مدار معادل کوانتومی کافی است همه‌ی گیت‌های θ_2 را با گیت‌های CCNOT جایگزین کنیم.

۴.۳ گیت‌های جهانی کوانتومی

از محاسبات کلاسیک می‌دانیم که مجموعه‌هایی متناهی از گیت‌های کلاسیک وجود دارند که جهانی هستند؛ به این معنا که هر تابع بولی را می‌توان با مدارهایی که تنها از گیت‌هایی که عضو این مجموعه‌ها هستند، پیاده‌سازی کرد. در بخش قبل نشان دادیم که برای محاسبات برگشت‌پذیر، مجموعه‌ی $\{\theta_2\}$ یکی از چنین مجموعه‌هایی است؛ و نیز نشان دادیم که هیچ مجموعه‌ای از گیت‌های ۱ و ۲ بیتی وجود ندارد که مجموعه‌ای جهانی برای محاسبات برگشت‌پذیر باشد. در این بخش به طور اجمالی وجود چنین مجموعه‌های جهانی‌ای از گیت‌ها را برای محاسبات کوانتومی مورد بررسی قرار می‌دهیم. اولین مسأله‌ای که باید به آن توجه کرد این است که تعداد نامتناهی ناشمارایی گیت کوانتومی متمایز وجود دارد؛ و در نتیجه، هیچ مجموعه‌ی متناهی‌ای از گیت‌های کوانتومی نمی‌تواند به طور دقیق جهانی باشد. از سوی دیگر، بنا به دلایل نظری و عملی متعددی از جمله ممکن نبودن پیاده‌سازی فیزیکی هر نگاشت یکانی دلخواه، به صورت آزمایشگاهی تنها پیاده‌سازی تعداد متناهی‌ای از گیت‌های کوانتومی برای ما مقدور است. این دلایل، ما را به این رهنمون می‌کنند که مفهوم جهانی بودن را برای گیت‌های کوانتومی به دو صورت متفاوت تعریف کنیم: یکی جهانی بودن به صورت دقیق، و دیگری جهانی بودن به صورت تقریبی.

تعریف ۱۱.۳ مجموعه‌ای از گیت‌های کوانتومی مانند \mathcal{G} به طور دقیق جهانی است هر گاه برای هر گیت کوانتومی مانند U ، دنباله‌ای متناهی از گیت‌ها مانند $g_1, g_2, \dots, g_n \in \mathcal{G}$ وجود داشته باشند به طوری که:

$$U = g_1 g_2 \dots g_n.$$

توجه کنید که سمت راست تساوی فوق مختصر نوشته شده است و باید چنین تعبیر شود: ممکن است هر یک از گیت‌های g_i ، تنها روی تعدادی از کیوبیت‌هایی که U بر آن‌ها اثر می‌کند (و نه همه‌ی آن‌ها) به صورت نابدهی عمل کنند (با توجه به بعد فضایی که روی آن تعریف شده اند)؛ و اثرشان روی باقی کیوبیت‌ها نگاشت همانی باشد. بنابراین، تساوی فوق به این معنا نیست که بعد فضایی که U و گیت‌های g_i روی آن تعریف شده‌اند، یکسان است.

با یک استدلال ساده‌ی شمارشی می‌توان نشان داد که هیچ مجموعه‌ی متناهی‌ای از گیت‌ها وجود ندارد که به طور دقیق جهانی باشد. با این وجود، مجموعه‌های نامتناهی از گیت‌ها که به طور دقیق جهانی باشند وجود دارند. یکی از چنین مجموعه‌هایی، که شاید مشهورترین آن‌ها باشد، توسط بارنکو و همکاران در [۱۹] معرفی شده است. آن‌ها نشان دادند که مجموعه‌ی همه‌ی گیت‌های کوانتومی ۱ کیوبیتی به همراه گیت ۲ کیوبیتی CNOT، مجموعه‌ای به طور دقیق جهانی از گیت‌های کوانتومی است.

برای تعریف کردن مفهوم جهانی بودن تقریبی، نخست به این نیازمندیم که به طور دقیقی مشخص کنیم که منظور ما از «تقریب‌زدن» چیست. برای آن که بتوانیم گیتی را تقریب بزیم، ضروری است که مفهومی از فاصله را روی نگاشت‌های یکانی تعریف کنیم. تعریف زیر، دسته‌ای از کاندیدهای مناسب برای این منظور را به ما پیشنهاد می‌دهد.

تعریف ۱۲.۳ -نرم شاتن یک عملگر $T \in \mathcal{L}(\mathbb{C}^d)$ ، که در آن $p \in [1, \infty)$ ، به صورت زیر:

$$\|T\|_p = (tr((T^\dagger T)^{\frac{p}{2}}))^{\frac{1}{p}},$$

و برای $p = \infty$ نیز به شکل زیر:

$$\|T\|_\infty = \lim_{p \rightarrow \infty} \|T\|_p = \sup_{|\psi\rangle : \langle \psi | \psi \rangle = 1} \|T|\psi\rangle\|.$$

تعریف می‌شود. به ۱-نرم و ∞ -نرم شاتن به ترتیب نرم اثر^{۴۵} و نرم طیفی^{۴۶} گفته می‌شود.



گزاره ۱۳.۳ برای هر $p \in [1, \infty]$ ، p -نرم شاتن یکانی-ناورد است؛ به این معنی که برای نگاشت‌های یکانی دلخواه $U, V \in \mathcal{L}(\mathbb{C}^d)$

$$\|UTV\|_p = \|T\|_p.$$

برهان. با استفاده از تجزیه‌ی SVD می‌توانیم T را به صورت زیر بنویسیم:

$$T = \sum_{i=1}^d \sigma_i |u_i\rangle \langle v_i|,$$

که در آن σ_i ها اعداد حقیقی نامنفی و $\{|u_i\rangle\}$ و $\{|v_i\rangle\}$ به ترتیب بردارهای ویژه‌ی تکین چپ و راست T هستند. بنابراین:

$$\begin{aligned} \|T\|_p &= (tr((T^\dagger T)^{\frac{p}{2}}))^{\frac{1}{p}} \\ &= (tr((\sqrt{\sum_{i,j} \sigma_i \sigma_j |v_i\rangle \langle u_j| |u_j\rangle \langle v_i|})^p))^{\frac{1}{p}} \\ &= (tr((\sqrt{\sum_i \sigma_i^2 |v_i\rangle \langle v_i|})^p))^{\frac{1}{p}} \\ &= (tr(\sum_i \sigma_i^p |v_i\rangle \langle v_i|))^{\frac{1}{p}} \\ &= (\sum_i \sigma_i^p)^{\frac{1}{p}} \end{aligned}$$

به عبارت دیگر اگر $\sigma(T)$ را برابر با بردار $(\sigma_1 \ \sigma_2 \ \dots \ \sigma_d)^T$ تعریف کنیم؛ که در آن σ_i ها مقادیر تکین T هستند، p -نرم شاتن عملگر T برابر است با p -نرم بردار $\sigma(T)$. از آن جا که مقادیر تکین یک عملگر با ضرب کردن آن در یک نگاشت یکانی تغییر نمی‌کند، بنابراین

$$\|UTV\|_p = \|T\|_p.$$



در ادامه گزاره‌ای را درباره‌ی برخی ویژگی‌های پرکاربرد p -نرم‌های شاتن بیان می‌کنیم. به دلیل مفصل بودن اثبات، در این جا از بیان آن خودداری می‌کنیم.

گزاره ۱۴.۳ گزاره‌های زیر برای p -نرم‌های شاتن برقرار هستند [۹۱]:

۱. p -نرم‌های شاتن، یکنوا هستند؛ به این معنی که برای هر $p, q \in [1, \infty]$ که $p \leq q$ و $A \in \mathcal{L}(\mathbb{C}^d)$

$$\|A\|_p \geq \|A\|_q.$$

۲. p -نرم‌های شاتن در نامساوی هولدر صدق می‌کنند؛ به این معنی که برای هر $p, q \in [1, \infty]$ به طوری که $\frac{1}{p} + \frac{1}{q} = 1$ و $A, B \in \mathcal{L}(\mathbb{C}^d)$

$$|tr(B^\dagger A)| \leq \|B\|_p \|A\|_q.$$

⁴⁵trace norm

⁴⁶spectral norm

۳. p -نرم‌های شاتن زیرضربی هستند؛ به این معنی که برای هر $A, B \in \mathcal{L}(\mathbb{C}^d)$ و $p \in [1, \infty]$

$$\|AB\|_p \leq \|A\|_p \|B\|_p.$$

۴. برای هر $A \in \mathcal{L}(\mathbb{C}^d)$ و $p \in [1, \infty]$

$$\|A\|_p = \|A^\dagger\|_p = \|A^T\|_p$$

از میان خانواده‌ی نامتناهی‌ای از نرم‌ها که در بالا معرفی شد، ما نرم اثر را انتخاب می‌کنیم و فاصله‌ی میان دو نگاشت یکانی U و V را به صورت $\|U - V\|_1$ تعریف می‌کنیم. اکنون که متر مناسبی برای تعریف فاصله‌ی میان دو گیت داریم، یک سوال مهم این است که «خطای گیت‌ها تا چه اندازه بر نتیجه‌ی محاسبه اثرگذار است؟». گزاره‌ی زیر، پاسخی به این سوال است.

گزاره ۱۵.۳ فرض کنید که برای دو مدار کوانتومی U و V که بر n کیوبیت عمل می‌کنند، داشته باشیم:

$$\|U - V\|_1 < \varepsilon.$$

اگر Π یک عملگر اندازه‌گیری افکنشی و ρ یک ماتریس چگالی باشد که حالت ورودی مدار را نمایش دهد، آنگاه

$$|tr(\Pi U \rho U^\dagger) - tr(\Pi V \rho V^\dagger)| < 2\varepsilon.$$

برهان.

$$|tr(\Pi U \rho U^\dagger) - tr(\Pi V \rho V^\dagger)| = |tr(\Pi(U \rho U^\dagger - V \rho V^\dagger))| \quad (23)$$

$$\leq \|\Pi\|_\infty \|U \rho U^\dagger - V \rho V^\dagger\|_1 \quad (24)$$

$$\leq \|U \rho U^\dagger - V \rho V^\dagger\|_1 \quad (25)$$

$$= \|U \rho U^\dagger - V \rho U^\dagger + V \rho U^\dagger - V \rho V^\dagger\|_1 \quad (26)$$

$$\leq \|U \rho U^\dagger - V \rho U^\dagger\|_1 + \|V \rho U^\dagger - V \rho V^\dagger\|_1 \quad (27)$$

$$= \|(U - V) \rho U^\dagger\|_1 + \|V \rho (U^\dagger - V^\dagger)\|_1 \quad (28)$$

$$= \|(U - V) \rho\|_1 + \|\rho (U^\dagger - V^\dagger)\|_1 \quad (29)$$

$$\leq \|U - V\|_1 \|\rho\|_1 + \|\rho\|_1 \|U^\dagger - V^\dagger\|_1 \quad (30)$$

$$\leq \|U - V\|_1 + \|U^\dagger - V^\dagger\|_1 \quad (31)$$

$$\leq \varepsilon + \varepsilon = 2\varepsilon \quad (32)$$

خطوط ۲۴، ۲۷، ۲۹ و ۳۰ به ترتیب از نامساوی هولدر، نامساوی مثلث، یکانی-ناوردا بودن و زیرضربی بودن اثر نتیجه می‌شوند. خطوط ۲۵ و ۳۱ از این حقیقت استفاده می‌کنند که $\|\Pi\|_\infty \leq 1$ و $\|\rho\|_1 \leq 1$ ، که به سادگی می‌توان درستی آن را بررسی کرد.

■

حال به تعریف مفهوم جهانی بودن به طور تقریبی می‌پردازیم.

تعریف ۱۶.۳ مجموعه‌ای متناهی از گیت‌های کوانتومی مانند \mathcal{G} به طور تقریبی جهانی است هرگاه برای هر گیت کوانتومی مانند U و هر $\varepsilon > 0$ دنباله‌ای متناهی از گیت‌های $g_1, g_2, \dots, g_n \in \mathcal{G}$ وجود داشته باشد به طوری که

$$\|U - g_1 g_2 \dots g_n\|_1 < \varepsilon.$$

►

مجموعه‌های متنوعی از گیت‌های به طور تقریبی جهانی وجود دارد که در مثال بعد، تعدادی از آن‌ها را معرفی می‌کنیم.

مثال ۱۷.۳ هر یک از مجموعه‌های زیر از گیت‌های کوانتومی، به طور تقریبی جهانی هستند:

• گیت دویج [۳۹]

• گیت بارنکو [۱۸]

• $\{H, T, \text{CNOT}\}$ [۷۳]

• تقریباً هر گیت کوانتومی که روی حداقل ۲ کیوبیت اثر می‌کند [۴۰]. (به این معنی که گیت‌هایی که جهانی نیستند، مجموعه‌ای اندازه صفر را مشخص می‌کنند.)

◇

در خاتمه‌ی این بخش، به پرسش مهم دیگری می‌پردازیم که پاسخ آن در ملاحظات پیچیدگی محاسباتی ما تاثیرگذار است. تا به اینجا، نشان دادیم که مجموعه‌ی همه‌ی گیت‌های ۱ کیوبیتی به همراه گیت CNOT مجموعه‌ای به طور دقیق جهانی است. با این حال، سوال این جاست که «برای ساختن یک نگاشت یکانی دلخواه با استفاده از اعضای این مجموعه، به چند گیت نیاز است؟». می‌توان نشان داد که نگاشت‌هایی یکانی روی n کیوبیت وجود دارند که برای ساختن آن‌ها با استفاده از اعضای این مجموعه، به $\theta(n^2 4^n)$ گیت نیاز است [۷۳]. با این حال قضیه‌ای زیبا موسوم به قضیه‌ی سولووی-کیتائف، به ما این تضمین را می‌دهد که برای هر دو مجموعه از گیت‌های به طور تقریبی جهانی، می‌توان یکی را با دیگری به صورت کارایی تقریب زد. همان‌گونه که در بخش بعد خواهیم دید، چنین نتیجه‌ای برای ساختن یک نظریه‌ی پیچیدگی مناسب برای محاسبات کوانتومی، اهمیت زیادی دارد.

قضیه ۱۸.۳ (قضیه‌ی سولووی-کیتائف) فرض کنید \mathcal{G} مجموعه‌ای متناهی از گیت‌های کوانتومی ۱ کیوبیتی است که شامل وارون اعضایش نیز هست و گروهی که توسط اعضای \mathcal{G} تولید می‌شوند در $SU(2)$ با نرم اثر چگال است. در این صورت برای هر $\varepsilon > 0$ ، ثابت c موجود است چنان‌که برای هر $U \in SU(2)$ ، دنباله‌ای از اعضای \mathcal{G} مانند $g_1, g_2, \dots, g_n \in \mathcal{G}$ وجود دارد به طوری که $\|U - g_1 g_2 \dots g_n\|_1 < \varepsilon$ و $n \in O(\log^c(\frac{1}{\varepsilon}))$ [۳۷].
فرض کنید مداری کوانتومی داریم که شامل m گیت کوانتومی ۱ کیوبیتی است؛ و می‌خواهیم آن را به مداری که گیت‌هایش از یک مجموعه از گیت‌های ۱ کیوبیتی به طور تقریبی جهانی (برای گیت‌های ۱ کیوبیتی) می‌آید، تبدیل کنیم؛ به طوری که مدار دوم با دقت ε مدار نخست را تقریب بزند. لم زیر، که نتیجه‌ی مستقیم یکانی-ناوردا بودن نرم اثر است؛ نشان می‌دهد که بدین منظور کافی است هر گیت مدار اول را با دقت $\frac{\varepsilon}{m}$ تقریب بزنیم.

لم ۱۹.۳ فرض کنید $V = V_m V_{m-1} \dots V_1$ و $U = U_m U_{m-1} \dots U_1$ دو مدار کوانتومی باشند به طوری که برای هر $0 \leq i \leq m$ ، $\|U_i - V_i\|_1 < \varepsilon$ ، $\varepsilon > 0$ ، در این صورت $\|U - V\|_1 < m\varepsilon$.
لم ۱۹.۲، همراه با قضیه‌ی ۱۸.۳ نتیجه می‌دهد که اگر مداری کوانتومی مانند U که از m گیت ۱ کیوبیتی کوانتومی ساخته شده است داشته باشیم، می‌توان آن را به مداری مانند U' تبدیل کرد؛ چنان‌که مدار اخیر تنها از گیت‌های جهانی ساخته شده است؛ و U' در ε -همسایگی U قرار دارد؛ و ضمناً اندازه‌ی مدار اخیر $O(m \log^c(\frac{m}{\varepsilon}))$ است.

۵.۳ محاسبات کوانتومی کارا

در نظریه‌ی محاسبه‌ی کلاسیک، محاسبات کارا معمولاً به محاسباتی با زمان چندجمله‌ای تعبیر می‌شود؛ انتخابی که پیشنهاد آن را می‌توان مربوط به کارهای کابام در دهه‌ی ۶۰ دانست [۳۵]. گرچه انتخاب چندجمله‌ای‌ها برای این منظور تا حدی دلخواه به نظر می‌رسد، این انتخاب در طول سالیان از نقطه‌ی نظرهای مختلفی تایید شده است^{۴۷}؛ تا این حد که باور عمومی بر این است که محاسبات کارایی که اساساً توسط بشر، و با محدودیت‌های طبیعت و قوانین فیزیک قابل انجام است، محاسبات چندجمله‌ای است. این باور را در نسخه‌ی تعمیم‌یافته‌ی تر چرچ-تورینگ می‌توان دید:

«هر چیز که به صورت کارایی محاسبه‌پذیر باشد، با یک ماشین تورینگ احتمالاتی در زمان چندجمله‌ای قابل محاسبه است [۹۲]»

توجه کنید که در محاسبات کلاسیک، مدل تورینگ مدل محاسبه‌ی مرجع است، حال آن‌که در محاسبات کوانتومی بنا به دلایل متعددی (از جمله این‌که پیاده‌سازی فیزیکی ماشین‌های تورینگ کوانتومی با توجه به محدودیت‌های فعلی مهندسی سیستم‌های کوانتومی غیرممکن می‌نماید) مدل مداری را به مدل تورینگ ترجیح می‌دهیم. با این توصیف به نظر می‌رسد که ضروری است با توجه به این پارادایم، در تعبیرمان از مفهوم کارایی محاسبه تغییراتی ایجاد کنیم. در مدل مداری، انتخاب طبیعی برای منابع محاسباتی‌ای که پیچیدگیشان مورد مطالعه قرار گیرد، اندازه و عمق مدار است؛ که می‌توان ثابت کرد تناظری بین این دو، با مفاهیم زمان و حافظه در مدل تورینگ وجود دارد [۱۷]. با این وجود، اگر محاسبات کارا در مدل مداری را به عنوان وجود مداری با اندازه‌ی چندجمله‌ای برای یک مسأله تعبیر کنیم، در این صورت به سادگی می‌توان دید که بسیاری از مسائل محاسبه‌ناپذیر نیز تحت این تعبیر، کارا خواهند بود. برای رفع این مشکل، باید با گذاشتن شرایط مناسبی بر مدارها، به نوعی آن‌ها را ملزم به رفتاری «یکنواخت» کرد. در ادامه، یک انتخاب برای چنین کاری را بیان می‌کنیم.

^{۴۷} گرچه در سال‌های اخیر، با ظهور و توسعه‌ی حوزه‌هایی مثل تحلیل داده‌های حجیم، مناسب بودن این انتخاب برای برخی مقاصد محاسباتی مورد بازبینی قرار گرفته است.

تعریف ۲۰.۳ یک خانواده از مدارها مانند (C_1, C_2, C_3, \dots) ، یکنواخت-چندجمله‌ای نامیده می‌شود هرگاه یک ماشین تورینگ با زمان چندجمله‌ای وجود داشته باشد که با ورودی 1^n ، توصیفی برای مدار C_n خروجی دهد.

پیش از آن که به طور دقیق مجموعه‌ی همه‌ی مسائلی که به طور کارا توسط کامپیوترهای کوانتومی قابل حل هستند را تعریف کنیم، ذکر دو نکته خالی از لطف نیست.

- همان‌گونه که تا به این جا دیده‌ایم، الگوریتم‌های کوانتومی ذاتاً احتمالاتی هستند؛ بنابراین برای تعریف کلاس همه‌ی مسائل قابل حل با الگوریتم‌های کارای کوانتومی، تلاش برای تعریف همتای کوانتومی کلاس BPP نقطه‌ی شروع بهتری از همتای کوانتومی P است.

- با وجود آن که کلاس‌های پیچیدگی کلاسیک عمدتاً به عنوان مجموعه‌ای از «زبان»ها تعریف می‌شوند، به دلایلی در پیچیدگی محاسباتی کوانتومی تعریف کلاس‌ها بر اساس مسأله‌ی قراردادی برتری یافته است. گرچه در پیچیدگی کلاسیک رایج است که اگر کلاسی مانند C بر اساس مسأله‌های قراردادی تعریف شده باشد، از آن به عنوان Promise C یاد کنند؛ در پیچیدگی کوانتومی معمولاً از این کار عدول می‌شود. بنابراین توجه کنید که همه‌ی کلاس‌هایی که در ادامه تعریف خواهد شد کلاس‌های قراردادی هستند؛ مگر آن که خلاف آن ذکر شود.

تعریف ۲۱.۳ کلاس پیچیدگی BQP عبارت است از همه‌ی مسائل قراردادی مانند $\Pi = (\Pi_{Yes}, \Pi_{No})$ ، به طوری که مدار کوانتومی یکنواخت-چندجمله‌ای (C_0, C_1, C_2, \dots) و چندجمله‌ای $q(x)$ موجودند به نحوی که برای هر $n \in \mathbb{N}$ ، C_n یک مدار کوانتومی است که روی یک ورودی n کیوبیتی (رجیستر in) و $q(n)$ کیوبیت کمکی (رجیستر an) با حالت اولیه‌ی صفر، عمل می‌کند، به طوری که:

۱. برای هر ورودی $x \in \{0, 1\}^n$ ، حالت C_n ، $|x\rangle_{in} |0\rangle_{an}^{\otimes q(n)}$ را ورودی می‌گیرد و پس از اعمال شدن بر آن، یک کیوبیت خاص (مثلاً اولین کیوبیت رجیستر an) در پایه‌ی محاسباتی اندازه‌گیری می‌شود. فرض کنید حاصل اندازه‌گیری $\{0, 1\}$ باشد. در این صورت،

۲. اگر $x \in \Pi_{Yes}$ ، آنگاه $\Pr[b = 1] \geq \frac{2}{3}$.

۳. اگر $x \in \Pi_{No}$ ، در این صورت $\Pr[b = 1] \leq \frac{1}{3}$.

با توجه به تعریفی که پیشتر از گیت‌های کوانتومی ارائه کردیم، این که هر نگاشت یکانی یک گیت کوانتومی است، اگر بخواهیم هزینه‌ی محاسباتی یک مدار را تعداد گیت‌های آن تعریف کنیم، چنین هزینه‌ای خوش‌تعریف نخواهد بود؛ زیرا ترکیب چند گیت کوانتومی نیز خود، گیتی کوانتومی است. برای رفع این مشکل مجموعه‌ی گیت‌هایی که در مدارها ظاهر می‌شوند را به مجموعه‌ای گسسته از گیت‌ها محدود می‌کنیم. از وجود مجموعه‌های به طور تقریبی جهانی از گیت‌ها می‌دانیم که چنین کاری مشکلی در محاسبه‌پذیری ایجاد نخواهد کرد. بعلاوه، از قضیه‌ی سولووی-کیتائف نیز می‌توان نتیجه گرفت که انتخاب مجموعه‌های جهانی متفاوت، در حد یک سربار چندجمله‌ای تفاوت ایجاد خواهد کرد؛ که با توجه به تعریف فوق، قابل تحمل است. بنابراین در ادامه می‌توانیم فرض کنیم که تمام مدارها متشکل از گیت‌هایی از مجموعه‌ی $\{H, T, CNOT\}$ هستند.

یادداشت ۲۲.۳ مانند بسیاری دیگر از کلاس‌های پیچیدگی تصادفی، کران‌های ظاهر شده در تعریف ۲۱.۳ را می‌توان در حد وارون نمایی کاهش داد. برای نشان دادن این موضوع کافی است با تکرار الگوریتم به تعداد کافی، از خروجی‌ها رای اکثریت بگیریم و نهایتاً از کران چرنف استفاده کنیم. به طریق مشابه، می‌توان دید که اگر تفاضل کران‌ها در حد وارون چندجمله‌ای باشد نیز، تعریف جدید به همان کلاس BQP معرفی شده در تعریف ۲۱.۳ منجر خواهد شد.

درباره‌ی ارتباط کلاس BQP با بقیه‌ی کلاس‌های پیچیدگی می‌توان به موارد زیر اشاره کرد:

۱. در بخش ۳.۳ نشان دادیم که چگونه می‌توان محاسبات کلاسیک را با مدارهای کوانتومی شبیه‌سازی کرد. با توجه به قضیه‌ی ۹.۳، می‌توان دید که هر مدار کلاسیک را می‌توان با سربار چندجمله‌ای به مداری کوانتومی تبدیل کرد. این حقیقت، در کنار این که در محاسبات کوانتومی می‌توان یک بیت تصادفی را با اندازه‌گیری حالتی مانند $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ در پایه‌ی محاسباتی تولید کرد، نتیجه می‌دهد که $BPP \subseteq BQP$.

۲. پیتر شور با ارائه‌ی الگوریتم مشهور خود برای حل مسأله تجزیه در [۷۹]، نشان داد که این مسأله در کلاس BQP قرار دارد. این در حالی است که باور عمومی بر این است که این مسأله را نمی‌توان با الگوریتم‌های تصادفی چندجمله‌ای حل کرد. بنابراین باور عمده بر این است که $BPP \neq BQP$.

۳. با وجود آن چه در بند قبل بیان شد، می‌توان نشان داد اوراکل‌هایی مانند A و B وجود دارند چنان‌که $BPP^A = BQP^A$ و $BQP^B \neq BPP^B$. A را کافی است یک اوراکل $PSPACE$ -کامل در نظر بگیریم؛ و B می‌تواند همان اوراکل مسأله‌ی سایمون باشد.

۴. روشن است که محاسبات کوانتومی را نیز می‌توان با محاسبات کلاسیک شبیه‌سازی کرد. تنها مشکل این‌جاست که پیچیدگی این شبیه‌سازی می‌تواند بسیار زیاد باشد. در مورد کلاس BQP ، می‌توان نشان داد که کلاس $PSPACE$ کران بالایی کلاسیک برای آن است. در فصل ۴ نشان خواهیم داد که QMA که کران بالایی بدیهی برای BQP است نیز مشمول در $PSPACE$ است. بنابراین در این‌جا اثباتی مستقیم برای این حقیقت ارائه نمی‌دهیم. خواننده‌ی علاقه‌مند می‌تواند چنین اثباتی را در [۷۳] بیابد.

۵. همان‌گونه که ادلمن و همکاران در [۵] نشان داده‌اند، کران بالایی بهتر برای BQP ، کلاس تصادفی PP است. ایده‌ی اثبات آن‌ها این است که مدارها را محدود به استفاده از مجموعه‌ی خاصی از گیت‌های به‌طور تقریبی جهانی می‌کنند؛ و همین آن‌ها را قادر می‌سازد تا در زمان چندجمله‌ای با خطای کمتر از $\frac{1}{p}$ خروجی مدار را محاسبه کنند. با توجه به این‌که در فصل ۴ نشان خواهیم داد که $QMA \subseteq PP$ ، در این‌جا از بیان اثبات ادلمن صرف‌نظر می‌کنیم.

۶. مشاهده‌ی چرایی این حقیقت که $P^P = P$ بسیار ساده است. در واقع نکته‌ی ساده‌ی نهفته در این اثبات این است که ترکیب دو چندجمله‌ای، یک چندجمله‌ای خواهد بود. با این حال، در محاسبات کوانتومی این سوال ظریف‌تر است و نیاز به دقت بیشتری دارد. اساساً این‌که آیا می‌توان از یک الگوریتم کوانتومی به‌عنوان زیرروالی در الگوریتم دیگر استفاده کرد، موضوعی نابدیهی است. دلیل این امر آن است که ممکن است کیوبیتی که با اندازه‌گیری آن خروجی زیرروال مشخص می‌شود، با دیگر کیوبیت‌های سیستم درهم‌تنیده باشد؛ و همین در نهایت منجر به خطا در خروجی نهایی روال شود. با این همه، می‌توان نشان داد که امکان کاهش خطا در کلاس BQP منتج به این می‌شود که بتوانیم مقدار چنین درهم‌تنیدگی‌هایی را تا حدی که در خروجی نهایی الگوریتم تاثیر نگذارد، کم کنیم. به این ترتیب، می‌توان نتیجه گرفت که $BQP^{BQP} = BQP$.

۴ اثبات‌های غیرتعاملی کوانتومی

فقط قضیه‌ها را برایم بفرست؛ خودم اثبات‌هایشان را خواهم یافت.

کرایسیپوس، در نامه‌ای به کلئانتس

۱.۴ کلاس پیچیدگی QMA

همان‌گونه که خواهیم دید، کلاس پیچیدگی QMA تعمیمی طبیعی از کلاس NP به قلمرو محاسبات کوانتومی است. با این حال، باید توجه داشت که به دلیل آن‌که الگوریتم‌های کوانتومی ذاتاً احتمالاتی هستند، تعریف کلاس QMA بیش از آن‌که به تعریف NP شبیه باشد، یادآور تعمیم کلاسیک احتمالاتی آن، یعنی MA است.

از پیچیدگی محاسبات کلاسیک می‌دانیم که کلاس NP را می‌توان با سیستم‌های اثبات نیز مشخص کرد. در واقع، اگر $L \in NP$ ، در این صورت برای هر $x \in L$ ، اثباتی کوتاه مانند π_x موجود است که به صورت موثری قابل تصدیق شدن است، و برای هر $x \notin L$ ، چنین اثباتی وجود ندارد. در این جا یادآور می‌شویم که مقصودمان از کوتاه بودن اثبات آن است که طول اثبات π_x از مرتبه‌ی چندجمله‌ای بر حسب طول ورودی x است؛ و مقصود از تصدیق کردن به طور موثر، وجود الگوریتمی مانند V_L است که x و π_x را به عنوان ورودی می‌گیرد، و در زمان چندجمله‌ای بر حسب طول x ، اگر π_x اثباتی درست برای $x \in L$ باشد، خروجی «بله» می‌دهد.

تعمیم‌های کوانتومی متفاوتی را می‌توان برای سیستم اثبات فوق در نظر گرفت. در ادامه یکی از این تعمیم‌ها را، که در آن الگوریتم تصدیق‌کننده با یک الگوریتم کوانتومی و اثبات نیز با یک اثبات کوانتومی جایگزین می‌شود، بررسی خواهیم کرد؛ تعمیمی که برای اولین بار در [۶۶] معرفی شده است. یادآوری می‌کنیم که همان‌گونه که پیشتر نیز تصریح کردیم، در پیچیدگی محاسبات کوانتومی، مسائل و کلاس‌های قراردادی مورد توجه ما هستند، و تعریف پیش رو نیز مشخص‌کننده‌ی یک کلاس قراردادی است.

تعریف ۱.۴ برای هر چندجمله‌ای $p(x)$ ، کلاس $QMA_p(\frac{2}{3}, \frac{1}{3})$ عبارت است از تمام مسأله‌های قراردادی مانند $\Pi = (\Pi_{Yes}, \Pi_{No})$ به طوری که مدار کوانتومی یکنواخت-چندجمله‌ای (C_0, C_1, C_2, \dots) و چندجمله‌ای $q(x)$ موجودند به نحوی که برای هر C_n ، $n \in \mathbb{N}$ یک مدار کوانتومی است که روی یک ورودی n کیوبیتی (رجیستر in)، یک اثبات کوانتومی $p(n)$ کیوبیتی (رجیستر pr) و $q(n)$ کیوبیت کمکی (رجیستر an) با حالت اولیه‌ی صفر، عمل می‌کند، به طوری که:

۱. برای هر ورودی $x \in \{0, 1\}^n$ و هر اثبات $C_n, |\psi\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ حالت $|0\rangle_{pr}^{\otimes q(n)} |0\rangle_{an}^{\otimes q(n)}$ را ورودی می‌گیرد و پس از اعمال شدن بر آن، یک کیوبیت خاص (مثلاً اولین کیوبیت رجیستر an) در پایه‌ی محاسباتی اندازه‌گیری می‌شود. فرض کنید حاصل اندازه‌گیری $\{0, 1\}$ باشد b .

۲. **تمامیت:** اگر $x \in \Pi_{Yes}$ ، در این صورت اثبات $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ وجود دارد به طوری که

$$\Pr[b = 1] \geq \frac{2}{3}.$$

۳. **درستی:** اگر $x \in \Pi_{No}$ ، در این صورت برای هر اثبات $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ داریم:

$$\Pr[b = 1] \leq \frac{1}{3}.$$

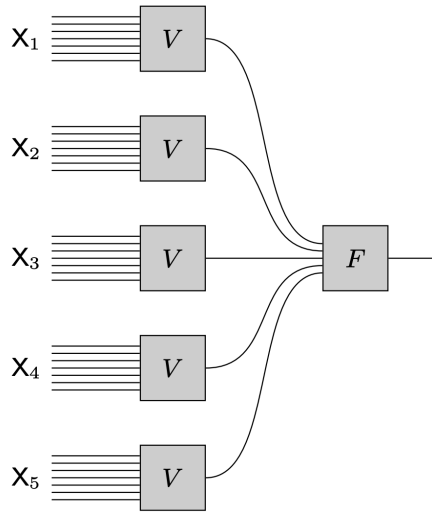
توجه کنید که اگر به جای ثوابت تمامیت و درستی اعداد (یا توابع) a و b را قرار دهیم، کلاس $QMA_p(a, b)$ به دست می‌آید. همچنین تعریف می‌کنیم: $QMA(a, b) = \bigcup_{p(x)} QMA_p(a, b)$. علاوه بر این، $(\frac{1}{3}, \frac{2}{3})$ را معمولاً به اختصار با QMA نشان می‌دهیم.

همان‌گونه که از تعریف بالا بر می‌آید، در تعریف کلاس QMA ، روی (توزیع) خروجی مدار در حالتی که ورودی x رشته‌ای عضو $\Pi_{Yes} \cup \Pi_{No}$ نیست، شرطی نداریم و در چنین حالاتی، خروجی می‌تواند دلخواه باشد.

یادداشت ۲.۴ QMA سرواژه‌ای برای کوانتوم مرلین-آرتور^{۴۸} است و گویای آن است که کلاس فوق، همتای کوانتومی کلاس پیچیدگی مرلین-آرتور (MA) می‌باشد. این نام‌گذاری اولین بار در [۸۸] به کار رفت و به تدریج جایگزین $BQNP$ ، نامی که [۶۶] نخستین بار برای این کلاس به کار برده بود، شد.

⁴⁸Quantum Merlin-Arthur

شکل ۵: کاهش خطای موازی، تصویر برگرفته شده از مرجع [۸۶] است.



کاهش احتمال خطا در تعریف ۱.۴: مشابه دیگر کلاس‌های پیچیدگی احتمالاتی با احتمال خطای کراندار، در تعریف کلاس QMA نیز می‌توان این سوال را مطرح کرد که آیا کران بالای $\frac{1}{p}$ روی احتمال خطا را می‌توان کاهش داد یا نه. می‌دانیم کاهش خطای کلاس MA امکان‌پذیر است؛ کافی است آرتور اثبات دریافت‌شده از مرلین را $k \in O(\log(\frac{1}{\epsilon}))$ بار کپی کند و برای هر کپی، الگوریتم تصدیق‌کننده را یک‌بار اجرا کرده و نهایتاً از خروجی‌های دفعات مختلف اجرای الگوریتم رای اکثریت بگیرد. به این ترتیب، با استفاده از کران چرنف می‌توان دید کران بالای احتمال خطا به $\epsilon = 2^{-r(x)}$ که $r(x)$ یک چندجمله‌ای است، کاهش می‌یابد.

با این حال، در کلاس QMA باید به این مطلب توجه کرد که بنابر قضیه‌ی عدم امکان شبیه‌سازی، نمی‌توان اثبات ارسال‌شده از طرف مرلین را کپی کرد و آرتور باید از خود مرلین بخواهد که k نسخه از اثبات را برایش ارسال کند. به این روش، روش کاهش خطای موازی^{۴۹} یا کاهش خطای ضعیف^{۵۰} می‌گویند. در این روش، مرلین یک اثبات $|\psi\rangle \in (\mathbb{C}^2)^{\otimes kp(n)}$ برای آرتور ارسال می‌کند و آرتور می‌بایست مشابه همان کاری که در کاهش خطای MA انجام می‌داد را تکرار کند. در این روش کاهش خطا دو مشکل قابل طرح است:

• آیا درهم‌تنیدگی امکان تقلب به مرلین نمی‌دهد؟

در حالتی که $x \in \Pi_{Yes}$ ، می‌دانیم اثبات $|\psi\rangle \in (\mathbb{C}^2)^{\otimes kp(n)}$ وجود دارد که تصدیق‌کننده با احتمال حداقل $\frac{1}{p}$ آن را می‌پذیرد. در این حالت، مرلین کافی است k نسخه از این اثبات را به صورت $|\psi'\rangle = |\psi\rangle \otimes \dots \otimes |\psi\rangle \in (\mathbb{C}^2)^{\otimes kp(n)}$ برای آرتور بفرستد و آرتور مطابق شکل ۵ الگوریتم تصدیق‌کننده را روی هر یک از k رجیستر اثبات اجرا کند و نهایتاً رای اکثریت بگیرد.

با این وجود، در حالتی که $x \in \Pi_{No}$ ، باید برای هر اثبات $|\psi'\rangle \in (\mathbb{C}^2)^{\otimes kp(n)}$ احتمال پذیرفته شدن اثبات توسط آرتور کراندار باشد. در این حالت، ممکن است مرلین اثباتی درهم‌تنیده برای آرتور ارسال کند. به این ترتیب اگر آرتور مطابق شکل ۵ عمل کند، حالت رجیسترهای مختلف اثبات لزوماً حالت خالص نخواهد ماند و ممکن است به دلیل درهم‌تنیدگی، رجیستری از اثبات حالت مخلوط پیدا کند.

با این حال به سادگی می‌توان دید که اگر برای هر اثبات $|\psi\rangle$ در حالت خالص، بدانیم آرتور آن را با احتمال حداکثر $\frac{1}{p}$ می‌پذیرد، در این صورت برای هر اثبات با حالت مخلوط ρ نیز احتمال پذیرفته شدن حداکثر $\frac{1}{p}$ خواهد بود. بنابراین، درهم‌تنیدگی نمی‌توان امکان تقلب را برای مرلین فراهم کند. نهایتاً، با استفاده از روشی که در بالا گفته شد، می‌توان قضیه‌ی زیر را ثابت کرد:

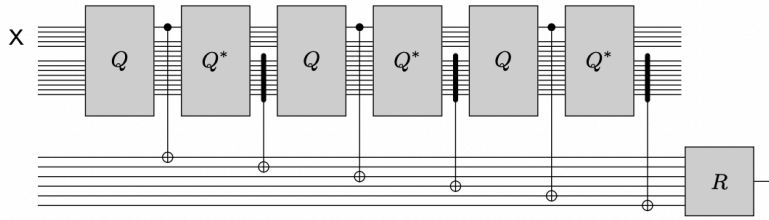
قضیه ۳.۴ برای هر چندجمله‌ای $p(n)$ و ثابت $0 < c < 1$ به طوری که $0 < c - \frac{1}{p(n)}$ داریم $[1, c]$:

$$QMA(c - \frac{1}{p(n)}, c) \subseteq QMA(\frac{1}{p}, \frac{1}{p}) = QMA(\frac{1}{p(n)}, 1 - \frac{1}{p(n)}).$$

⁴⁹Parallel Error Reduction

⁵⁰Weak Error Reduction

شکل ۶: کاهش خطای حافظ اثبات، تصویر برگرفته شده از مرجع [۸۶] است.



- اندازه‌ی اثبات در این روش افزایش یافته است. آیا این افزایش طول اثبات غیرقابل اجتناب است؟ در واقع، این افزایش طول اثبات ضروری نیست. [۷۱] روشی هوشمندانه موسوم به کاهش خطای حافظ اثبات یا کاهش خطای قوی ارائه کرده است که در ادامه کلیتی از آن را بدون اثبات، بیان می‌کنیم.

الگوریتم

فرض کنید مدار تصدیق برای یک ورودی، اثبات را در رجیستر X و کیویت‌های کمکی را در رجیستر Y می‌گیرد. این مدار را با Q نمایش می‌دهیم. هم‌چنین فرض کنید کیویتی که با اندازه‌گیری آن، خروجی مدار Q مشخص می‌شود را با A و مابقی کیویت‌های خروجی را با Z نمایش دهیم. هم‌چنین فرض کنید ثوابت درستی و تمامیت به ترتیب برابر c و s باشند و بخواهیم آن‌ها را به $1 - 2^{-p(n)}$ و $2^{-p(n)}$ برسانیم. در این صورت مراحل زیر را باید $T = O\left(\frac{p(n)}{c-s}\right)$ بار انجام دهیم (شکل ۶) [۸۶]:

- Q را بر (X, Y) اعمال کرده و (A, Z) را به دست می‌آوریم.
- A را در پایه‌ی محاسباتی اندازه‌گیری می‌کنیم و نتیجه‌ی اندازه‌گیری را a_j می‌نامیم.
- Q^\dagger را بر (A, Z) اعمال می‌کنیم تا (X, Y) به دست آید.
- اندازه‌گیری افکنشی $\{|0^m\rangle\langle 0^m|, I - |0^m\rangle\langle 0^m|\}$ را روی Y انجام می‌دهیم و نتیجه‌ی اندازه‌گیری را b_j می‌نامیم.
- حال تعریف کنید: $c_1 = a_1$ ، و برای هر i ، $c_{2i} = a_i \oplus b_i$ و $c_{2i-1} = a_i \oplus b_{i-1}$. الگوریتم فوق اثبات را می‌پذیرد اگر و تنها اگر $\sum_{i=1}^{2T} c_i \geq \frac{c+s}{2}$.

به این ترتیب، قضیه‌ی زیر را خواهیم داشت:

قضیه ۴.۴ فرض کنید $a, b : \mathbb{N} \rightarrow [0, 1]$ دو تابع محاسبه‌پذیر در زمان چندجمله‌ای باشند و $q(x)$ یک چندجمله‌ای باشد به نحوی که برای هر $n \in \mathbb{N}$ (به جز احتمالاً تعداد متناهی از اعداد طبیعی)،

$$a(n) - b(n) \geq \frac{1}{q(n)}. \quad (۳۳)$$

در این صورت برای هر دو چندجمله‌ای $p(x), r(x)$ با این شرط که $r(n) \geq 2$ برای هر عدد طبیعی n (بجز احتمالاً تعداد متناهی از اعداد طبیعی)، داریم:

$$QMA_p(a, b) = QMA_p(1 - 2^{-r}, 2^{-r}). \quad (۳۴)$$

مسئله‌ی دیگری که پس از تعریف کلاس QMA باید به آن پاسخ دهیم، بررسی رابطه‌ی این کلاس با دیگر کلاس‌های پیچیدگی و یافتن کران‌های پایین و بالایی برای آن است. روشن است که MA و BQP ، هر دو، کران‌های پایینی برای QMA هستند. در ادامه، کران بالایی را نیز برای QMA خواهیم یافت.

۱. به سادگی می‌توان نشان داد که $QMA \subseteq \mathcal{NEXP}$. فرض کنید که Π مسئله‌ای در QMA باشد. در این صورت، ماشینی را در نظر بگیرید که ابتدا یک اثبات $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ را به صورت غیرقطعی حدس می‌زند

(تعداد پارامترهای چنین اثباتی بر حسب n نمایی است). سپس احتمال این که مدار تصدیق کننده ی آرتور خروجی ۱ بدهد را محاسبه می کند و با توجه به مقدار این احتمال، اثبات را می پذیرد یا رد می کند. محاسبه ی این احتمال در زمان نمایی بر حسب n ممکن است. بنابراین ماشین توصیف شده در بالا، ماشینی غیرقطعی با زمان نمایی است؛ که نتیجه می دهد مسأله ی مورد نظر عضو کلاس \mathcal{NEXP} است.

۲. به عنوان کران بالایی نابدهی تر از \mathcal{NEXP} ، می توان نشان داد که $\mathcal{QMA} \subseteq \mathcal{EXP}$. بدین منظور، نخست توجه کنید که احتمال این که مدار تصدیق آرتور برای ورودی با طول n (که آن را با Q_n نمایش می دهیم) به ازای اثبات $|\psi\rangle$ خروجی ۱ بدهد برابر است با^{۵۱}:

$$\begin{aligned} \Pr[\text{output} = 1] &= \|\langle 1 | \otimes \mathbb{I}_{N-1} \rangle Q_n |x\rangle_{in} |\psi\rangle_{pr} | \circ^{q(n)} \rangle_{an}\|_2^2 \\ &= \text{tr} \left(\langle x |_{in} \langle \psi |_{pr} \langle \circ^{q(n)} |_{an} Q_n^\dagger (|1\rangle \langle 1| \otimes \mathbb{I}_{N-1}) Q_n |x\rangle_{in} |\psi\rangle_{pr} | \circ^{q(n)} \rangle_{an} \right) \\ &= \text{tr} \left(P_x |\psi\rangle \langle \psi| \right) \\ &= \langle \psi | P_x | \psi \rangle \end{aligned}$$

که در آن، $N = n + p(n) + q(n)$ و

$$P_x = \left(\langle x |_{in} \otimes \mathbb{I}_{pr} \otimes \langle \circ^{q(n)} |_{an} Q_n^\dagger (|1\rangle \langle 1| \otimes \mathbb{I}_{N-1}) Q_n |x\rangle_{in} \otimes \mathbb{I}_{pr} \otimes | \circ^{q(n)} \rangle_{an} \right).$$

از طرفی می دانیم که

$$\max_{|\psi\rangle : \langle \psi | \psi \rangle = 1} \langle \psi | P_x | \psi \rangle = \lambda_{max}(P_x).$$

بنابراین، برای حل یک مسأله ی قراردادی در کلاس \mathcal{QMA} مانند Π ، که عبارت است از تعیین این که برای هر $x \in \Pi_{Yes} \cup \Pi_{No}$ کدامیک از $x \in \Pi_{Yes}$ یا $x \in \Pi_{No}$ درست است، کافی است بزرگترین مقدار ویژه ی عملگر خطی P_x را محاسبه کنیم. روشن است که ابعاد P_x بر حسب n نمایی است. با این وجود، پیدا کردن مقدار ویژه های یک ماتریس، در زمان چندجمله ای بر حسب ابعاد آن امکان پذیر است. در نتیجه، هر مسأله ی \mathcal{QMA} را می توان با ماشینی قطعی در زمان نمایی حل کرد.

۳. با استفاده از کاهش خطای قوی می توان نشان داد $\mathcal{QMA} \subseteq \mathcal{PP}$ [۷۱]. برای هر چندجمله ای دلخواه p و یک مسأله ی قراردادی دلخواه در \mathcal{QMA}_p مانند $\Pi = (\Pi_{Yes}, \Pi_{No})$ ، از قضیه ی ۴.۴ می دانیم:

$$\Pi \in \mathcal{QMA}_p(1 - \epsilon^{-(p(n)+r)}, \epsilon^{-(p(n)+r)})$$

حال الگوریتمی کوانتومی را در نظر بگیرید که برای یک ورودی دلخواه با طول n ، اثباتی را به تصادف از بین همه ی اثبات های با طول $p(n)$ انتخاب می کند؛ و آن در رجیستر اثبات مدار تصدیق کننده ی مسأله ی Π قرار می دهد و الگوریتم تصدیق کننده را اجرا می کند. احتمال این که این الگوریتم خروجی ۱ دهد برابر است با:

$$\text{tr} \left(P_x \frac{\mathbb{I}}{\epsilon^{p(n)}} \right) = \frac{1}{\epsilon^{p(n)}} \text{tr}(P_x).$$

• در حالتی که $x \in \Pi_{Yes}$ ، داریم:

$$\frac{1}{\epsilon^{p(n)}} \text{tr}(P_x) \geq \frac{1}{\epsilon^{p(n)}} \left(1 - \frac{1}{\epsilon^{p(n)+r}} \right) \geq \frac{1}{\epsilon^{p(n)+1}}$$

• در حالتی که $x \in \Pi_{No}$ ، داریم:

$$\frac{1}{\epsilon^{p(n)}} \text{tr}(P_x) \leq \frac{1}{\epsilon^{p(n)+r}}$$

با توجه به فاصله ی بین ضرایب درستی و تمامیت در بالا، می توان دید که فاصله ی مورد نظر در تعریف کلاس \mathcal{PP} برآورده می شود. تنها مشکل این جاست که الگوریتمی که در بالا ارائه شده است، الگوریتمی کوانتومی، و نه کلاسیک است. به عبارت دیگر، آن چه که در بالا ارائه کرده ایم نشان می دهد که Π عضو کلاس \mathcal{PQP} است؛ کلاسی که همناهی کوانتومی \mathcal{PP} محسوب می شود. با این همه، یاماگامی در [۹۵] نشان داده است که $\mathcal{PQP} = \mathcal{PP}$ ؛ و به این ترتیب مشکلی در اثبات وجود نخواهد داشت.

^{۵۱} در این جا فرض کرده ایم که مقدار بیت خروجی با اندازه گیری اولین کیوبیت تعیین می شود.

۲.۴ نسخه‌هایی دیگر از QMA

در این بخش به نسخه‌هایی تغییر یافته از کلاس QMA می‌پردازیم و برخی ویژگی‌های اثبات شده و حدس‌های اثبات نشده در ارتباط با این کلاس‌ها را مرور خواهیم کرد.

• QMA با اثبات‌های کلاسیک (QCMA):

اگر در تعریف کلاس QMA فرض کنیم که اثباتی که توسط مرلین ارسال می‌شود یک رشته‌ی کلاسیک است، کلاس QCMA به دست می‌آید. روشن است که $QCMA \subseteq QMA$. با این حال، این مسأله که آیا این شمول اکید است یا نه، مسأله‌ای باز است. آرانسون و کوپربرگ در [۴] نشان داده‌اند که یک اوراکل کوانتومی \mathcal{O} وجود دارد که $QMA^{\mathcal{O}} \neq QCMA^{\mathcal{O}}$. این نتیجه به این معنی است که در پاسخ به این سوال که آیا $QMA = QCMA$ یا نه، نیازمند تکنیک‌هایی هستیم که قابل نسبی‌شدن با اوراکل‌های کوانتومی نیستند.

• **QMA با خطای یک‌طرفه (QMA_1):** اگر در تعریف کلاس QMA، این تغییر را ایجاد کنیم که در حالتی که ورودی عضو Π_{Yes} است، اثباتی وجود داشته باشد که احتمال پذیرفته شدن آن توسط آرتور برابر با ۱ باشد، کلاس پیچیدگی QMA_1 به دست می‌آید. روشن است که $QMA_1 \subseteq QMA$. با این حال، این که آیا این شمول اکید است یا نه، مسأله‌ای باز است. آرانسون در [۲] اوراکلی کوانتومی مانند \mathcal{O} ارائه می‌دهد که $QMA_1^{\mathcal{O}} \neq QMA^{\mathcal{O}}$.

یادداشت ۵.۴ با وجود این که پرسش $QMA_1 \stackrel{?}{=} QMA$ بدون پاسخ مانده است، سوالی مشابه، $QCMA_1 \stackrel{?}{=} QCMA$ توسط کوبایاشی و همکاران در [۶۲] پاسخ داده شده است و می‌دانیم $QCMA_1 \subseteq QCMA$ با خطای یک‌طرفه برابر است. به این ترتیب، بلافاصله می‌توان نتیجه گرفت که $QCMA_1 \subseteq QCMA$. \triangleright

• **QMA با k مرلین ($QMA(k)$):** اگر در تعریف کلاس QMA، این تغییر را ایجاد کنیم که اثبات به صورت حاصلضرب تنسوری k حالت $p(n)$ کوبیتی باشد، در این صورت کلاس پیچیدگی $QMA(k)$ به دست می‌آید. این کلاس نخستین بار توسط کوبایاشی و همکاران در [۶۸] معرفی شد و مورد بررسی قرار گرفت.

در واقع، می‌توان درباره‌ی این کلاس چنین اندیشید که مجموعه‌ی تمام مسائلی است که می‌توان آن‌ها را با سیستم‌های اثبات غیرتعاملی با چند اثبات‌کننده، که اثبات‌کننده‌ها نیز با یکدیگر تعاملی ندارند (جداید پذیر بودن اثبات را می‌توان چنین تعبیر کرد)، مشخص کرد. در چهارچوب پیچیدگی محاسبات کلاسیک، افزودن به تعداد اثبات‌کننده‌های یک سیستم اثبات غیرتعاملی، با این فرض که اثبات‌کننده‌ها نیز با یکدیگر تعامل نداشته باشند، چیزی بر قدرت محاسباتی نمی‌افزاید؛ حال آن که در چهارچوب پیچیدگی کوانتومی هنوز نمی‌دانیم که چنین حکمی هم‌چنان برقرار خواهد ماند.

به بیان دقیق‌تر، روشن است که $QMA \subseteq QMA(k)$ ؛ با این وجود، اکید بودن این شمول هنوز مسأله‌ای بی‌پاسخ است. لیو و همکاران در [۷۰] مسأله‌ای به نام N -نمایش‌پذیری حالت خالص 5^2 را پیشنهاد داده‌اند که در $QMA(k)$ قرار دارد اما به نظر نمی‌رسد که عضو QMA باشد. پرسش دیگر در مورد QMA با چند مرلین این است که آیا در حالتی که تعداد اثبات‌کننده‌ها حداقل دو تاست، با افزایش تعداد مرلین‌ها قدرت محاسباتی افزایش می‌یابد یا نه. آرام هرو و موتانارو در [۶۰] به این پرسش پاسخ داده و نشان داده‌اند که برای هر $k \geq 2$ ، $QMA(2) = QMA(k)$.

بهترین کران‌های بالا و پایین شناخته شده برای $QMA(k)$ به ترتیب کران‌های بدیهی QMA و $NEXP$ هستند. البته، کران بالای دیگری نیز برای $QMA(k)$ شناخته شده است که کلاس $Q\Sigma_2$ می‌باشد. کلاس اخیر، معادل کوانتومی کلاس Σ_2 ، طبقه‌ی سوم سلسله‌مراتب چندجمله‌ای است. با این وجود، کلاس مزبور چندان شناخته شده نیست و شواهدی وجود ندارد که $Q\Sigma_2 \neq NEXP$.

• **StoqMA:** اگر در تعریف QMA، تغییرات زیر را اعمال کنیم کلاس StoqMA به دست می‌آید:

۱. کیوبیت‌های کمکی می‌توانند با مقادیر اولیه‌ی $|0\rangle$ یا $|+\rangle$ مقداردهی شوند.
۲. مداری که آرتور اعمال می‌کند، تنها از گیت‌های وارون‌پذیر کلاسیک تشکیل شده است.
۳. اندازه‌گیری نهایی در پایه‌ی X انجام می‌شود.

در واقع، StoqMA را می‌توان به صورت سیستم اثباتی دید که در آن اثبات، یک حالت کوانتومی است اما مدار تصدیق، یک مدار کلاسیک است.

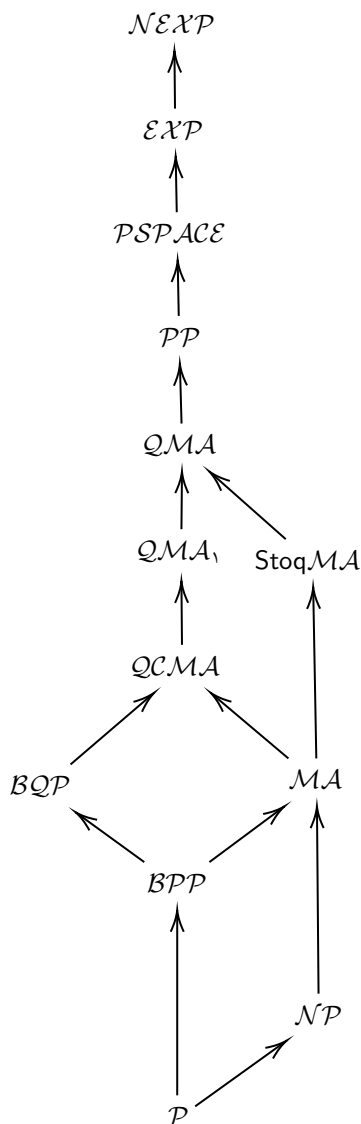
کلاس StoqMA نسخه‌ای عجیب از QMA است. یکی از وجوه تفاوت StoqMA با دیگر نسخه‌های QMA این است که باور بر این است که StoqMA شامل BQP نیست. در توضیح می‌توان گفت که از یک سو، همان‌گونه که ترهال و همکاران در [۳۰] نشان داده‌اند،

$$\text{StoqMA} \subseteq \text{AM} \subseteq \text{PH}.$$

⁵²pure state N -Representability

از سوی دیگر، باور بر این است که $BQP \not\subseteq PH$. بنابراین، شمول BQP در $StoqMA$ بعید دانسته می‌شود. وجه دیگری از تفاوت‌های $StoqMA$ با دیگر نسخه‌ها این است که برقرار بودن کاهش خطای ضعیف برای این کلاس، مسأله‌ای باز است. اخیراً آهارونوف و همکاران در [۸] نشان داده‌اند که امکان کاهش خطای $StoqMA$ از $O(1)$ به $1 - o(\frac{1}{poly(n)})$ نتیجه خواهد داد که $StoqMA = MA$. با این حال، هنوز مشخص نیست که آیا این نتیجه در تعیین تکلیف کاهش خطای ضعیف برای این کلاس تأثیری خواهد داشت یا نه.

نهایتاً، این زیربخش را با ارائه‌ی یک جمع‌بندی در قالب یک دیاگرام از روابط کلاس‌های پیچیدگی معرفی شده در این بخش به پایان می‌بریم.



۳.۴ مسأله‌هایی در QMA

بحث ما تا به این‌جا درباره‌ی تعریف کلاس QMA ، نسخه‌های مختلف آن، و ارتباط میان QMA و دیگر کلاس‌های پیچیدگی شناخته شده بوده است. متأسفانه بر خلاف کلاس NP که تا به امروز عضویت مسائل زیادی در آن را می‌دانیم؛ و حتی لیست بلندبالایی از مسائل کامل برای آن وجود دارد، تعداد مسائل شناخته‌شده‌ی QMA چندان زیاد نیست [۲۶]. افزودن به لیست مسائل شناخته‌شده‌ی QMA ، و بالاخص مسائل کامل آن، یکی از اهدافی است که در پیچیدگی محاسباتی کوانتومی دنبال می‌شود. در این بخش درباره‌ی نمونه‌هایی از مسائلی که عضو QMA هستند بحث می‌کنیم و افزون بر

این، در فصل ۵ نیز یکی از مهم‌ترین مسائل QMA را مفصلاً مورد بررسی قرار خواهیم داد.
مسئله‌ی عدم عضویت در گروه^{۵۳}:

عضویت این مسئله در QMA نخستین بار در [۸۸] مطرح و اثبات شده است. نکته‌ی شایان توجه در مورد این مسئله این است که این مسئله، نه یک مسئله‌ی قراردادی، بلکه یک زبان است؛ و از این جهت با دیگر مسائل نابدیهی شناخته شده در QMA متفاوت است.

فرض کنید گروهی متناهی مانند G داریم که اعضای آن را می‌توان با رشته‌های باینری با طول حداکثر n به طور یکتا کد کرد. در ادامه، از ساختار جعبه‌سیاه گروه^{۵۴} که در [۱۶] معرفی شده است استفاده می‌کنیم^{۵۵}. توجه کنید که به طور کلی، نتایجی که در ساختار جعبه‌سیاه گروه به دست می‌آوریم را می‌توانیم در صورت وجود روشی موثر برای پیاده‌سازی الگوریتمی اعمال گروه، به ساختار غیر اوراکلی نیز گسترش دهیم. در این ساختار، مقصود از یک اوراکل کوانتومی گروه^{۵۶}، یک نگاشت یکانی است که می‌تواند در یک گام، حاصلضرب دو عضو از گروه (یا حاصلضرب وارون یکی در دیگری) را محاسبه کند.

مسئله‌ی عدم عضویت در گروه

ورودی: مجموعه‌ی $H = \{g_1, g_2, \dots, g_m\} \subset G$ که یک گروه است؛ و یک عضو $h \in G$.
سوال: آیا $h \notin \langle g_1, g_2, \dots, g_n \rangle$ ؟

می‌توان نشان داد که یک اثبات کوانتومی برای عدم عضویت h در گروه H ، حالت کوانتومی زیر است:

$$|H\rangle = \frac{1}{\sqrt{|H|}} \left(\sum_{g \in H} |g\rangle \right)$$

توضیح آن است که اگر $h \in H$ ، در این صورت

$$|hH\rangle = \frac{1}{\sqrt{|H|}} \left(\sum_{g \in H} |hg\rangle \right) = |H\rangle.$$

از طرفی اگر $h \notin H$ ، خواهیم داشت $|hH\rangle \perp |H\rangle$ (زیرا در این حالت، $hH \cap H = \emptyset$). حال برای تمییز دادن هر یک از این دو حالت از مدار شکل ۷ استفاده می‌کنیم. در این مدار، گیت یکانی U دسترسی به یک اوراکل کوانتومی گروه برای G دارد و به صورت زیر عمل می‌کند:

$$U |g\rangle = |hg\rangle, \quad \forall g, h \in G$$

مطابق این مدار، داریم:

۱. حالت سیستم پس از اعمال اولین هادامارد روی کیوبیت اول به صورت

$$|\phi_1\rangle = |+\rangle |H\rangle$$

خواهد بود.

۲. پس از اعمال گیت کنترلی U ، حالت سیستم برابر است با:

$$|\phi_2\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |H\rangle + |1\rangle \otimes |hH\rangle).$$

۳. پس از اعمال آخرین هادامارد، حالت سیستم مساوی است با:

$$|\phi_3\rangle = \frac{1}{2} (|0\rangle \otimes (|H\rangle + |hH\rangle) + |1\rangle \otimes (|H\rangle - |hH\rangle)).$$

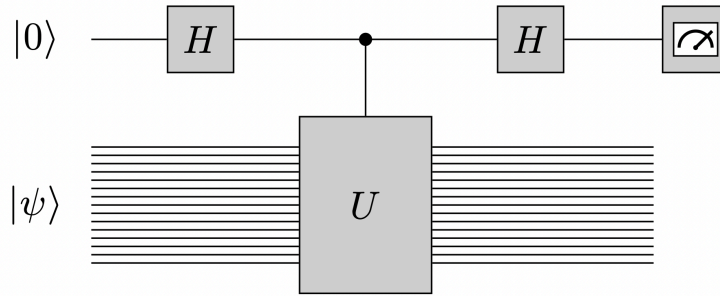
⁵³group non-membership problem

⁵⁴Black-box Group

⁵⁵توجه کنید که روش‌های متفاوتی برای نمایش اعضای گروه وجود دارد؛ و روشن است که پیچیدگی مسئله به نحوه‌ی توصیف اعضای گروه وابسته است. با این حال، در ساختار جعبه‌سیاه گروه، فرض می‌کنیم که اعضا یا برجسب‌هایی نمایش داده شده‌اند؛ و ضرب دو عضو یا وارون کردن یک عضو توسط یک جعبه‌سیاه انجام می‌شود و پیچیدگی آن به نحوه‌ی نمایش اعضا حساس نیست [۸۹].

⁵⁶Quantum Group Oracle

شکل ۷: مدار برای تمییز دادن $h \in H$ از $h \notin H$. تصویر برگرفته از منبع [۸۶] است.



۴. حال اگر $h \in H$ ، در این صورت پس از اندازه‌گیری، حالت سیستم حتماً برابر با $|0\rangle$ خواهد بود، و اگر $h \notin H$ ، در این صورت با توجه به تعامد $|H\rangle$ و $|hH\rangle$ ، احتمال آن که حاصل اندازه‌گیری $|0\rangle$ باشد برابر با $\frac{1}{2}$ است. بنابراین در حالتی که $h \notin H$ ، اثبات $|H\rangle$ موجود است که مرلین با ارسال آن، بتواند با احتمال حداقل $\frac{1}{2}$ آرتور را متقاعد کند. در حالتی که $h \in H$ ، باید به این توجه کرد که مرلین لزوماً $|H\rangle$ را به عنوان اثبات نخواهد فرستاد. با این حال، می‌توان با تغییراتی جزئی در الگوریتم بالا نخست چک کرد که اثبات، همان $|H\rangle$ است یا نه و سپس تست بالا را روی آن اجرا کرد. در این جا برای اجتناب از درگیری با جزئیات، از ذکر الگوریتم اصلی و اثبات آن خودداری می‌کنیم. خواننده می‌تواند اثبات مفصلی را در [۸۸، ۸۶] بیابد.

مسئله‌ی صدق‌پذیری مدار کوانتومی: مسئله‌ی صدق‌پذیری مدار کوانتومی همتای کوانتومی مسئله‌ی صدق‌پذیری مدار در محاسبات کلاسیک است؛ که می‌دانیم مسئله‌ای \mathcal{NP} -کامل است. به سادگی می‌توان دید که مسئله‌ی زیر نیز مسئله‌ای \mathcal{QMA} -کامل است. با این وجود، با توجه به این که تحویلی که از هر مسئله‌ی \mathcal{QMA} به این مسئله ارائه می‌شود تحویلی کانونی و معادل با تعریف \mathcal{QMA} است، به نظر نمی‌رسد که کامل بودن آن جذابیت ویژه‌ای داشته باشد.

مسئله‌ی صدق‌پذیری مدار کوانتومی

ورودی: یک مدار کوانتومی C که بر یک استیت n کیوبیتی به عنوان ورودی و یک رجیستر $m = q(n)$ کیوبیتی کمکی با حالت $|0^{q(n)}\rangle$ عمل می‌کند؛ و نهایتاً یک کیوبیت مشخص اندازه‌گیری می‌شود و حاصل اندازه‌گیری در بیت b قرار داده می‌شود که $b \in \{0, 1\}$.

• (Π_{Yes}) یک استیت $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ وجود دارد به طوری که اگر در رجیستر ورودی قرار داده شود، خواهیم داشت: $\Pr[b = 1] \geq \frac{2}{3}$.

• (Π_{No}) برای هر استیت $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ ، اگر $|\psi\rangle$ در رجیستر ورودی قرار داده شود، $\Pr[b = 1] \leq \frac{1}{3}$.

۵ پیچیدگی همیلتنی کوانتومی

چیزهای بزرگ نه به طور ناگهانی، که با دنباله‌ای از چیزهای کوچک ساخته می‌شوند.

ونسان ون گوگ

همان‌گونه که در بخش ۲.۲ بحث کردیم، مطالعه‌ی رفتار سیستم‌های فیزیکی متشکل از تعدادی ذره‌ی در حال حرکت، مسأله‌ای است که در قلب مکانیک (کوانتومی) قرار دارد. توصیف چنین سیستم‌هایی، وقتی که از تعداد زیادی ذره تشکیل شده‌اند که با یکدیگر برهم‌کنش می‌کنند، به دلیل رفتار پیچیده‌ای که سیستم از خود نشان می‌دهد، کار سختی است. انگیزه‌ی اصلی نظریه‌ی سیستم‌های چندپیکره^{۵۷} در فیزیک، سعی در فهمیدن ویژگی‌های چنین سیستم‌هایی است. از دیگر سو، اگر مطالعات فیزیکی را در سه مرحله‌ی مدل‌سازی، حل تقریبی مدل و پیش‌بینی کردن یک کمیت بر اساس آن، و نهایتاً بررسی کمیت پیش‌بینی شده به صورت تجربی و تنظیم و بهبود مدل خلاصه کنیم، به دلیل ذات الگوریتمی مرحله‌ی دوم، ملاحظات پیچیدگی محاسباتی در این مرحله اهمیت پیدا می‌کند [۷۴].

در این بخش، توجه ما معطوف به مطالعه‌ی پیچیدگی محاسباتی روش‌هایی است که در نظریه‌ی سیستم‌های چندپیکره برای توصیف سیستم‌های کوانتومی به کار گرفته می‌شود. یک مشاهده‌ی غیرمنتظره آن است که مشابهتی کانونی میان اشیاء مورد مطالعه در نظریه‌ی پیچیدگی محاسبه و نظریه‌ی سیستم‌های چندپیکره وجود دارد؛ و همین مشابهت‌ها انگیزه‌بخش ما برای تلاش در جهت استفاده از ابزارهای نظریه‌ی پیچیدگی محاسبه برای پاسخ دادن به این پرسش که «شبیه‌سازی یک سیستم فیزیکی تا چه اندازه سخت است؟» خواهد بود. مطالعه‌ی این مشابهت‌ها، که به شکوفایی‌هایی هم در علوم کامپیوتر و هم در فیزیک انجامیده است، حوزه‌ای است که از آن به عنوان پیچیدگی همیلتنی کوانتومی^{۵۸} یاد می‌شود؛ و از مهم‌ترین زمینه‌های پژوهش در اشتراک فیزیک و علوم کامپیوتر به حساب می‌آید.

۱.۵ همیلتنی‌های موضعی

در یک سیستم فیزیکی متشکل از n ذره، وقتی که n بزرگ می‌شود، برهم‌کنش ذرات با یکدیگر پیچیده‌تر شده و توصیف حالت سیستم دشوار می‌شود. فیزیکدانان برای مدل‌سازی چنین سیستم‌هایی، عموماً فرض‌هایی ساده‌کننده را در مدل لحاظ می‌کنند. مثلاً فرض می‌کنند که آرایش ذرات به صورت یک مشبک‌ی ۲ یا ۳-بعدی است؛ و ذرات در چنین آرایشی تنها با نزدیک‌ترین همسایه‌شان برهم‌کنش می‌کنند. مدل‌های ساده‌شده‌ی مختلفی در نظریه‌ی سیستم‌های چندپیکره برای توصیف سیستم‌های فیزیکی توسعه یافته است؛ که از جمله‌ی آن‌ها می‌توان به مدل آیسینگ^{۵۹}، مدل هایزنبرگ و مدل AKLT اشاره کرد.

با داشتن مدلی در دست، سوال‌های متعددی را می‌توان درباره‌ی سیستم طرح کرد. مثلاً می‌توان به محاسبه‌ی یک ویژگی موضعی از سیستم (مثلاً حالت یک زیرسیستم متشکل از تعداد کوچکی ذره در یک دمای خاص) پرداخت؛ یا تحول سیستم را در طول زمان مورد مطالعه قرار داد. همان‌گونه که در ادامه خواهیم دید، بخش قابل توجهی از تلاش‌های سیستم‌های چندپیکره مربوط به مطالعه‌ی انرژی سیستم است. این تمرکز بر انرژی سیستم از آن جهت است که در عمل، محاسبه‌ی انرژی سیستم می‌تواند منجر به محاسبه‌ی بسیاری از کمیت‌های موضعی آن شود.

در فیزیک کلاسیک، برای هر سیستم فیزیکی با یک فضای حالت مانند \mathcal{S} ، تابعی مانند $\mathcal{E} : \mathcal{S} \rightarrow \mathbb{R}$ وجود دارد که بیانگر انرژی سیستم است. در واقع این تابع، به هر حالت که سیستم ممکن است در آن قرار گیرد، یک انرژی نسبت می‌دهد. مثلاً در مدل آیسینگ کلاسیک، فرض بر این است که ذرات روی رئوس یک مشبک قرار دارند؛ و حالت سیستم به صورت n تایی‌هایی مانند $(x_1, x_2, \dots, x_n) \in \{-1, 1\}^n$ است؛ که ۱ یا -۱ بودن متغیر x_i ، معرف اسپین رو به بالا یا پایین آن است. در چنین مدل‌سازی‌ای، تابع انرژی به صورت

$$\mathcal{E}(x_1, \dots, x_n) = \sum_{\langle i, j \rangle} J_{i,j} x_i x_j$$

تعریف می‌شود؛ که $J_{i,j}$ ها قدرت برهم‌کنش را مدل می‌کنند و مقصود از $\langle i, j \rangle$ این است که جمع روی همه‌ی زوج‌های (i, j) ای که نزدیک‌ترین همسایه هستند، انجام می‌شود.

در فیزیک کوانتوم، انرژی سیستم را وقتی در حالت $|\psi\rangle$ قرار دارد، نمی‌توان به صورت قطعی تعیین کرد. در واقع، انرژی مشاهده‌پذیری است که ویژه‌مقادیر آن، بیانگر سطوح انرژی سیستم هستند؛ و با اندازه‌گیری انرژی سیستم، بر اساس توزیع

⁵⁷many body theory

⁵⁸quantum Hamiltonian complexity

⁵⁹Ising model

احتمالی که روی این سطوح انرژی وجود دارد، حاصل اندازه‌گیری یکی از این ویژه‌مقادیر خواهد بود. به چنین مشاهده‌پذیرهایی، همیلتنی سیستم گفته می‌شود. به عنوان مثال، در مدل آیسینگ کوانتومی، همیلتنی به صورت

$$H = -J \sum_{\langle i,j \rangle} \sigma_i^z \sigma_j^z - g \sum_i \sigma_i^x$$

تعریف می‌شود؛ که در آن عملگرهای پاولی X و Z هستند؛ و g بیانگر بزرگی میدان مغناطیسی است [۵۰]. از میان سطوح انرژی مختلف، سطح انرژی کمینه از اهمیت ویژه‌ای برخوردار است. چه آن‌که از توزیع بولتزمن می‌دانیم حالت سیستم در دمای بسیار پایین و نزدیک به صفر، هنگردی از حالت‌های با انرژی کمینه خواهد بود؛ و به این ترتیب، با دانستن کمینه‌ی انرژی سیستم و حالت‌هایی که سیستم در آن‌ها این انرژی کمینه را دارد، می‌توان اطلاعاتی درباره‌ی بسیاری از خواص ترمودینامیکی سیستم در دمای پایین به دست آورد. از سوی دیگر، همان‌گونه که در اصل ۱۷.۲ دیدیم، تحول زمانی یک سیستم فیزیکی با معادله‌ی شرودینگر توصیف می‌شود که به صورت زیر است:

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle$$

و در این معادله، همیلتنی سیستم است که نحوه‌ی تحول آن را تعیین می‌کند. همین سبب می‌شود که همیلتنی‌ها در مسأله‌ی شبیه‌سازی سیستم‌های کوانتومی، به عنوان توصیفی از سیستمی که قصد شبیه‌سازی آن را داریم، ظاهر شوند. در این مسأله، توصیفی از یک همیلتنی H ، حالت اولیه‌ی ρ ، مشاهده‌پذیری مانند M و لحظه‌ای از زمان مانند t به عنوان ورودی داده شده است و خواسته‌ی مسأله آن است که به عنوان خروجی، تقریبی از

$$\text{Tr} \left[M \frac{(e^{iHt})^\dagger \rho e^{iHt}}{\text{Tr}((e^{iHt})^\dagger \rho e^{iHt})} \right]$$

محاسبه شود. می‌توان دید که مسأله‌ی یافتن تقریبی از کمینه‌ی انرژی سیستم، حالت خاصی از مسأله‌ی فوق است [۷۴]. با مقدمه‌ی بالا، در ادامه‌ی این فصل تمرکز خود را بر روش‌های محاسباتی برای یافتن تقریبی از کمینه‌ی مقدار انرژی برخی سیستم‌های خاص خواهیم گذاشت؛ و پیچیدگی محاسباتی این روش‌ها را مطالعه خواهیم کرد.

تعریف ۱.۵ یک همیلتنی k موضعی^{۶۰} بر روی یک سیستم n کیوبیتی، عملگری هرمیتی مانند $H : (\mathbb{C}^2)^{\otimes n} \rightarrow (\mathbb{C}^2)^{\otimes n}$ است که می‌توان آن را به صورت $H = \sum_i H^{(i)}$ نوشت؛ به نحوی که هر $H^{(i)}$ عملگری هرمیتی است که فقط روی k کیوبیت سیستم به طور نابدهی عمل می‌کند. مقادیر ویژه‌ی H ، سطوح انرژی^{۶۱} سیستم توصیف شده با H نامیده می‌شوند و کمترین مقدار ویژه‌ی H که آن را با $\lambda_{\min}(H)$ نمایش می‌دهیم، انرژی حالت پایه‌ی سیستم^{۶۲} نام دارد. همچنین به بردار ویژه‌ی متناظر با $\lambda_{\min}(H)$ حالت پایه‌ی^{۶۳} سیستم گوئیم.

یادداشت ۲.۵ در حالتی کلی‌تر از تعریف سطوح انرژی که در بالا بیان شد، می‌توان گفت که هر همیلتنی که بر یک سیستم n کیوبیتی عمل می‌کند، به هر حالت سیستم مانند $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ یک انرژی نسبت می‌دهد که برابر با مقدار $\langle \psi | H | \psi \rangle$ است. (توجه کنید که این عدد، حقیقی است.) به سادگی می‌توان دید که انرژی حالت پایه‌ی سیستم، کمینه‌ی مقدار انرژی همه‌ی حالت‌های سیستم است. به عبارت دیگر:

$$\lambda_{\min}(H) = \min_{|\psi\rangle} \langle \psi | H | \psi \rangle. \quad (۲۵)$$

▷

مسأله‌ی همیلتنی k موضعی

تعریف ۳.۵ فرض کنید $p : \mathbb{N} \rightarrow \mathbb{R}^+$ یک چندجمله‌ای باشد. مسأله‌ی همیلتنی k موضعی با فاصله‌ی قراردادی^a $p(n)$ b (k -LH)^c، مسأله‌ای قراردادی است که به صورت زیر تعریف می‌شود [۶۶]:

⁶⁰ k -Local Hamiltonian
⁶¹ energy levels
⁶² ground state energy
⁶³ ground state

• ورودی: توصیفی از یک همیلتنی k موضعی ($k \in O(1)$) $H = \sum_i H^{(i)}$ که بر روی n کیوبیت عمل می‌کند و توابع به طور موثر محاسبه‌پذیر $\alpha(n), \beta(n)$ به طوری که $\beta(n) - \alpha(n) \geq \frac{1}{p(n)}$.

• خروجی:

- اگر $\lambda_{\min}(H) \leq \alpha(n)$ ، خروجی «بله» می‌دهیم.
- اگر $\lambda_{\min}(H) \geq \beta(n)$ ، خروجی «خیر» می‌دهیم.
- در حالتی غیر از دو حالت فوق، به طور دلخواه خروجی می‌دهیم.



^apromise gap

^b k -Local Hamiltonian problem

^cاین‌که این مسأله بر حسب p پارامتریزه شده است را به طور ضمنی فرض می‌کنیم و از نوشتن آن خودداری خواهیم کرد.
^dتوجه کنید که این فاصله را می‌توان به یک عدد ثابت افزایش داد؛ کافی است هر جمله در H را $p(n)$ بار تکرار کنیم [۵۰].

در واقع مسأله‌ی همیلتنی k موضعی، تعمیم کوانتومی مسأله‌ی k -CSP است. در ادامه نشان خواهیم داد که ۳-SAT را می‌توان به ۳-LH تحویل کرد؛ و به این ترتیب، نتیجه خواهیم گرفت که ۳-LH مسأله‌ای سخت برای کلاس \mathcal{NP} است.

قضیه ۴.۵

$$3\text{-SAT} \leq_m^p 3\text{-LH} \quad (۲۶)$$

برهان. می‌دانیم هر فرمول ۳-CNF فرمولی مانند

$$\varphi(x_1, \dots, x_n) = \bigwedge_i c_i(x_{i_1}, x_{i_2}, x_{i_3}) \quad (۲۷)$$

است به طوری که c_i ، یک ترکیب فصلی مانند $A_{i_1} \vee A_{i_2} \vee A_{i_3}$ است که هر A_{i_j} برابر با x_{i_j} یا $\neg x_{i_j}$ است. برای هر $c_i(x_{i_1}, x_{i_2}, x_{i_3})$ همیلتنی $(\mathbb{C}^2)^{\otimes n} \rightarrow (\mathbb{C}^2)^{\otimes n}$ را به این صورت تعریف کنید:

$$H_{i_1, i_2, i_3}^{(i)} = \sum_{\substack{x \in \{0,1\}^3 \\ \text{s.t. } c(x)=0}} |x\rangle \langle x| \quad (۲۸)$$

(سمت راست تساوی بالا به صورت مختصر نوشته شده است و باید این‌گونه تعبیر شود: $H_{i_1, i_2, i_3}^{(i)}$ تنها روی کیوبیت‌های i_1, i_2, i_3 به صورت نابديهی عمل می‌کند و عمل آن روی این سه کیوبیت نیز مطابق با نگاشت

$$\sum_{\substack{x \in \{0,1\}^3 \\ \text{s.t. } c(x)=0}} |x\rangle \langle x|$$

است.)

حال تعریف کنید:

$$H = \sum_i H_{i_1, i_2, i_3}^{(i)} \quad (۲۹)$$

روشن است که H یک همیلتنی ۳ موضعی است و توصیف آن را می‌توان از روی توصیف φ و در زمان چندجمله‌ای (بر حسب طول توصیف φ) به دست آورد.

اکنون توجه کنید که اگر $\varphi \in 3\text{-SAT}$ ، در این صورت ارزش‌گذاری $x \in \{0,1\}^n$ به متغیرهای φ وجود دارد به طوری که $\varphi(x) = 1$ به طور خاص، برای هر i ، $c_i(x_{i_1}, x_{i_2}, x_{i_3}) = 1$ بنابراین $\langle x | H | x \rangle = 0$ یا معادلاً $\lambda_{\min}(H) \leq 0$. از سوی دیگر، اگر $\varphi \notin 3\text{-SAT}$ ، در این صورت برای هر ارزش‌گذاری $x \in \{0,1\}^n$ به متغیرهای φ ، $\varphi(x) = 0$ یا معادلاً i وجود دارد به طوری که $c_i(x_{i_1}, x_{i_2}, x_{i_3}) = 0$ ، که معادل است با $\langle x | H_{i_1, i_2, i_3}^{(i)} | x \rangle = 1$ بنابراین، برای هر

داریم $x \in \{0, 1\}^n$:

$$\langle x | H | x \rangle = \sum_{x \in \{0, 1\}^n} \langle x | H_{i_l, i_r, i_r}^{(i)} | x \rangle \geq 1. \quad (40)$$

حال برای هر $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ که $|\psi\rangle = \sum_{x \in \{0, 1\}^n} \alpha_x |x\rangle$ داریم:

$$\langle \psi | H | \psi \rangle = \sum_{x \in \{0, 1\}^n} |\alpha_x|^2 \langle x | H | x \rangle \quad (41)$$

$$\geq \sum_{x \in \{0, 1\}^n} |\alpha_x|^2 = 1 \quad (42)$$

بنابراین، در این حالت نیز $\lambda_{\min}(H) \geq 1$.

۲.۵ قضیه‌ی کوک-لوین کوانتومی

قضیه‌ی کوک-لوین را می‌توان یکی از عمیق‌ترین نتایج به دست آمده در نظریه‌ی پیچیدگی محاسبات کلاسیک دانست. این قضیه، که مستقلاً توسط لئونید لوین [۸۳] و استفن کوک [۳۶] اثبات شده است، از جهات متعددی حائز اهمیت است:

- نخست آن که این قضیه آغازگر مسیری طولانی در جهت یافتن مسائل \mathcal{NP} -کامل به امید پاسخ‌دادن به مسأله‌ی \mathcal{P} vs. \mathcal{NP} بوده است.
- اگر روح محاسبه را «یافتن توصیف‌هایی متناهی برای مجموعه‌های نامتناهی» بدانیم، قضیه‌ی کوک-لوین ارتباطی میان دو روش متفاوت برای توصیف متناهی مجموعه‌ها - یکی الگوریتم‌ها و دیگری عبارات منطقی - برقرار می‌کند.
- این قضیه ناظر به یکی از اساسی‌ترین ویژگی‌های مفهوم محاسبه، یعنی موضعی بودن آن است. حقیقتی که در پس اثبات قضیه‌ی کوک-لوین نهفته است آن است که هر محاسبه‌ای، عبارت است از دنباله‌ای از تغییرات موضعی بر پیکربندی ماشین محاسبه که نهایتاً به یک پیکربندی مطلوب ختم شود.

در روندی مشابه با محاسبات کلاسیک، در این بخش نشان خواهیم داد که کلاس QMA نیز مسأله‌ای کامل دارد؛ مسأله‌ای که برخلاف مسأله‌ی صدق‌پذیری مدار کوانتومی که در فصل قبل معرفی شد، مسأله‌ای کانونی نیست و در شاخه‌های دیگری از دانش، یعنی نظریه‌ی سیستم‌های چندپیکره، بامعنی و قابل مطالعه است. به علاوه، خواهیم دید سخت بودن این مسأله برای کلاس QMA ، اطلاعاتی را در مورد یکی از اولین انگیزه‌های مطالعه‌ی محاسبات کوانتومی، یعنی امید برای شبیه‌سازی کارای سیستم‌های فیزیکی کوانتومی به وسیله‌ی کامپیوترهای کوانتومی، فراهم خواهد کرد.

در بخش قبل دیدیم که مسأله‌ی k -LH تعمیمی از مسأله‌ی k -CSP است؛ و بدین ترتیب کاندیدای طبیعی ما برای مسأله‌ای کامل در QMA مسأله‌ی k -LH خواهد بود. برای اثبات کامل بودن، باید نشان دهیم k -LH مسأله‌ای در QMA است؛ و بعلاوه این مسأله برای کلاس QMA مسأله‌ای سخت است. اثبات مورد اول نسبتاً ساده است و نخست به آن می‌پردازیم.

قضیه ۵.۵ برای هر $k \in \mathcal{O}(\log n)$ و هر پارامتر چندجمله‌ای p ، k -LH $\in QMA$ [۶۶].

برهان. برای آن که نشان دهیم k -LH $\in QMA$ ، الگوریتم تصدیق‌کردنی برای آرتور ارائه می‌دهیم که چنانچه برای ورودی (H, α, β) ، داشته باشیم $(H, \alpha, \beta) \in k$ -LH، اثباتی وجود داشته باشد که مرلین بتواند برای آرتور ارسال کرده و آرتور در زمان چندجمله‌ای آن را با احتمال بالایی تصدیق کند؛ و در حالتی که $(H, \alpha, \beta) \notin k$ -LH، چنین اثباتی وجود نداشته باشد. نشان خواهیم داد که الگوریتم زیر این ویژگی را دارد.

ابتدا فرض کنید $H = \sum_{i=1}^m H^{(i)}$ برای سادگی، فرض کنید هر یک از جملات موضعی $H^{(i)}$ ، عملگرهایی مثبت معین با مقادیر ویژه‌ی بین ۰ و ۱ هستند. در این صورت، فرض کنید تجزیه‌ی طیفی هر $H^{(i)}$ به صورت

$$H^{(i)} = \sum_s \lambda_s |s\rangle \langle s| \quad (43)$$

باشد.

الگوریتم

مرلین: به عنوان اثبات، حالت پایه ی H (بردار $|\psi\rangle$) را برای آرتور ارسال می کند.
آرتور:

- حالت ارسال شده از طرف مرلین را در کنار یک کیوبیت اضافی که در حالت $|\circ\rangle$ آماده سازی شده است قرار می دهد. این کیوبیت اضافه را «کیوبیت جواب» می نامیم.
 - به طور تصادفی و با احتمال یکسان، عدد i را بین 1 تا m انتخاب می کند.
 - نگاشت W_i را روی $|\circ\rangle \otimes |\psi\rangle$ اعمال می کند و کیوبیت جواب را در پایه ی محاسباتی اندازه گیری می کند. چنانچه حالت سیستم پس از اندازه گیری $|\circ\rangle$ باشد، اثبات را رد می کند و در غیر این صورت، می پذیرد.
- برای هر i ، عمل W_i روی پایه ی $\{|s\rangle \otimes |\circ\rangle\}_s$ به صورت زیر تعریف شده است:

$$W_i(|s\rangle \otimes |\circ\rangle) = \sqrt{\lambda_s} |s\rangle \otimes |\circ\rangle + \sqrt{1 - \lambda_s} |s\rangle \otimes |1\rangle \quad (44)$$

نخست توجه کنید که با توجه به این که $k \in \mathcal{O}(\log n)$ ، آرتور می تواند نگاشت W_i را در زمان چند جمله ای اعمال کند. حال نشان می دهیم برای هر حالت $|\psi\rangle$ که توسط مرلین ارسال شده باشد، احتمال پذیرفته شدن اثبات توسط آرتور

$$1 - \frac{1}{m} \langle \psi | H | \psi \rangle$$

است.

فرض کنید برای هر i داشته باشیم:

$$|\psi\rangle = \sum_s \alpha_s |s\rangle \quad (45)$$

در این صورت برای هر i داریم:

$$W_i(|\psi\rangle \otimes |\circ\rangle) = W_i\left(\sum_s \alpha_s |s\rangle \otimes |\circ\rangle\right) \quad (46)$$

$$= \sum_s \alpha_s W_i(|s\rangle \otimes |\circ\rangle) \quad (47)$$

$$= \sum_s \alpha_s (\sqrt{\lambda_s} |s\rangle \otimes |\circ\rangle + \sqrt{1 - \lambda_s} |s\rangle \otimes |1\rangle) \quad (48)$$

بنابراین احتمال این که آرتور پس از اعمال W_i و اندازه گیری کیوبیت جواب در پایه ی محاسباتی اثبات را بپذیرد برابر است با:

$$\sum_s |\alpha_s|^2 (1 - \lambda_s).$$

از طرفی داریم:

$$\sum_s |\alpha_s|^2 (1 - \lambda_s) = \sum_s |\alpha_s|^2 - \sum_s \lambda_s |\alpha_s|^2 \quad (49)$$

$$= 1 - \sum_s \lambda_s |\alpha_s|^2 \quad (50)$$

$$= 1 - \langle \psi | H^{(i)} | \psi \rangle \quad (51)$$

حال توجه کنید که احتمال پذیرفته شدن اثبات $|\psi\rangle$ توسط آرتور برابر است با:

$$\sum_{i=1}^m \frac{1}{m} (1 - \langle \psi | H^{(i)} | \psi \rangle) = 1 - \frac{1}{m} \langle \psi | H | \psi \rangle \quad (52)$$

بنابراین اگر $(H, \alpha, \beta) \in k\text{-LH}$ ، مرلین می‌تواند حالت پایه‌ی H را برای آرتور ارسال کند و آرتور با احتمال

$$1 - \frac{1}{m} \langle \psi | H | \psi \rangle \geq 1 - \frac{\alpha}{m}$$

آن را می‌پذیرد. از طرفی اگر $(H, \alpha, \beta) \notin k\text{-LH}$ ، هر حالتی که از طرف مرلین ارسال شود، با احتمال

$$1 - \frac{1}{m} \langle \psi | H | \psi \rangle \leq 1 - \frac{\beta}{m}$$

پذیرفته خواهد شد. نهایتاً با توجه به این که اختلاف ثوابت درستی و تمامیت، بزرگتر از $\frac{1}{p(n)}$ است، حکم از قضیه‌ی ۲.۴ نتیجه خواهد شد.

■

پیش از آن که به اثبات سخت بودن $k\text{-LH}$ برای کلاس QMA پردازیم، خالی از فایده نیست که روند اثبات سخت بودن SAT برای \mathcal{NP} را در قضیه‌ی کوک-لوین کلاسیک مرور کنیم. فرض کنید $L \subseteq \{0, 1\}^*$ زبانی عضو کلاس \mathcal{NP} باشد. هدف ما این است که تحویلی با زمان چندجمله‌ای از این زبان به SAT بسازیم. به عبارت دیگر، برای هر ورودی $z \in \{0, 1\}^*$ ، در زمان چندجمله‌ای بر حسب طول z ، فرمولی بولی مانند ϕ_z بیابیم به طوری که

$$z \in L \iff \phi_z \in \text{SAT}.$$

بدین منظور، توجه کنید که چون $L \in \mathcal{NP}$ ، پس ماشین تورینگ قطعی $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{accept}})$ با زمان چندجمله‌ای وجود دارد که تصدیق‌کننده‌ی زبان L است. می‌دانیم

$$z \in L \iff \exists y \in \{0, 1\}^{\text{poly}(|z|)} M(z, y) = 1.$$

ایده آن است که عبارت بولی ϕ_z را طوری بیابیم که عملکرد M روی z را شبیه‌سازی کند. در چنین شبیه‌سازی‌ای باید مولفه‌های زیر لحاظ شود:

- **مقداردهی اولیه‌ی نوار:** پیش از شروع به کار ماشین M ، ورودی مناسب روی نوار نوشته شده باشد.
- **انتقال پیکربندی‌ها:** هر پیکربندی مطابق با قانون انتقال δ از پیکربندی قبل به دست آمده باشد.
- **خروجی:** وقتی محاسبه پایان می‌یابد، $z \in L$ اگر و تنها اگر حالت نهایی q_{accept} باشد.

در اثبات قضیه‌ی کوک-لوین در محاسبات کلاسیک، برای چک کردن هر یک از موارد فوق، فرمولی بولی با طول حداکثر چندجمله‌ای بر حسب طول z ساخته می‌شود و نهایتاً، عطف این فرمول‌ها فرمول ϕ_z را در اختیار ما قرار می‌دهد. خواننده‌ی علاقه‌مند می‌تواند جزئیات اثبات را در [۱۷] دنبال کند. در محاسبات کوانتومی نیز، در روندی مشابه با حالت کلاسیک، سه مورد فوق را با همیلتنی‌های مناسبی کد خواهیم کرد.

قضیه ۶.۵ $k\text{-LH}$ برای هر $k \geq 5$ تحت تحویل چند به یک با زمان چندجمله‌ای، مسأله‌ای سخت برای کلاس QMA است.

برهان. فرض کنید $\Pi = (\Pi_{\text{Yes}}, \Pi_{\text{No}})$ مسأله‌ی قراردادی دلخواهی در کلاس QMA باشد. طبق تعریف، می‌دانیم مدار کوانتومی تصدیق‌کننده‌ی V برای این مسأله وجود دارد. فرض کنید $V = V_T V_{T-1} \dots V_1$ ؛ که V_i ها گیت‌های ۱-موضعی یا ۲-موضعی هستند و $T \in \mathcal{O}(\text{poly}(n))$ است. تکنیکی که برای اثبات قضیه‌ی کوک-لوین کوانتومی استفاده می‌شود، این است که برای هر ورودی مانند $|x\rangle$ ، تاریخچه‌ی محاسبه‌ی $|x\rangle$ توسط مدار V را در یک استیت کوانتومی کد می‌کنیم؛ و سپس با همیلتنی‌های موضعی برای چک کردن این که مقداردهی اولیه‌ی رجیسترها درست است، انتقال پیکربندی‌ها به درستی انجام می‌شود و خروجی مدار همان خروجی مطلوب است، بهره می‌گیریم. در این اثبات کیتائف برای کد کردن مفهوم زمان، بر اساس ایده‌ای از فاینمن، از یک رجیستر اضافه استفاده کرده و تاریخچه‌ی محاسبه را به صورت زیر کد کرده است:

$$|\psi_{\text{hist}}\rangle = \sum_t |\psi_t\rangle_{in,pr,an} |t\rangle_C,$$

که در آن

$$|\psi_t\rangle = (V_T V_{T-1} \dots V_1 |x\rangle_{in} |\psi\rangle_{pr} |0 \dots 0\rangle_{an}) |0 \dots 0\rangle_C,$$

و از پانونیس C برای نمایش رجیستر کلاک استفاده کرده‌ایم.

در ادامه تلاش می‌کنیم یک همیلتنی مناسب H را طوری طراحی کنیم که حالت کوانتومی فوق، حالت پایه‌ی آن باشد.

- برای آن که مقداردهی اولیه‌ی رجیسترها را به آن چه مطلوب ماست ($|x\rangle$) در رجیستر ورودی و ($|\circ \dots \circ\rangle$) در رجیستر کمکی (مقید کنیم، همیلتنی H_{in} را به صورت زیر تعریف می‌کنیم:

$$H_{in} = (\mathbb{I} - |x\rangle\langle x|)_{in} \otimes \mathbb{I}_{pr} \otimes \mathbb{I}_{an} \otimes |\circ \dots \circ\rangle\langle \circ \dots \circ|_C \\ + \mathbb{I}_{in} \otimes \mathbb{I}_{pr} \otimes (\mathbb{I} - |\circ \dots \circ\rangle\langle \circ \dots \circ|)_{an} \otimes |\circ \dots \circ\rangle\langle \circ \dots \circ|_C$$

روشن است که H_{in} مثبت نیمه‌معین است و به علاوه برای حالت $|\phi(y)\rangle$ که برای هر $y \in \{\circ, \mathbb{1}\}^{q(n)}$ ، به صورت زیر تعریف شده است:

$$|\phi(y)\rangle = |x\rangle_{in} |\psi\rangle_{pr} |y\rangle_{an} |\circ \dots \circ\rangle_C$$

داریم $\langle \phi(y) | H_{in} | \phi(y) \rangle = \circ$ اگر و تنها اگر $y = \circ^{q(n)}$.

- برای آن که در زمان $t = T$ ، پس از اندازه‌گیری بیت خروجی (که در این جا فرض کنید کیویت اول رجیستر کمکی است) خروجی مدار برابر $\mathbb{1}$ باشد، همیلتنی H_{out} را به صورت زیر تعریف می‌کنیم:

$$H_{out} = \mathbb{I}_{in} \otimes \mathbb{I}_{pr} \otimes (|\circ\rangle\langle \circ|)_{an} \otimes |T\rangle\langle T|_C.$$

در این جا مقصود از $(|\circ\rangle\langle \circ|)_{an}$ نگاشتی است که کیویت اول رجیستر کمکی را روی زیرفضای تولید شده توسط $|\circ\rangle$ می‌افکند و اثر آن روی باقی کیویت‌های رجیستر کمکی، همانی است.

- برای چک کردن انتقال درست پیکربندی‌ها، همیلتنی H_{prop} را به صورت زیر تعریف می‌کنیم:

$$H_{prop} = \sum_{t=\circ}^{T-\mathbb{1}} -V_{t+\mathbb{1}} \otimes |t+\mathbb{1}\rangle\langle t| - V_{t+\mathbb{1}}^\dagger \otimes |t\rangle\langle t+\mathbb{1}| \\ + \mathbb{I}_{in,pr,an} \otimes |t\rangle\langle t| + \mathbb{I}_{in,pr,an} \otimes |t+\mathbb{1}\rangle\langle t+\mathbb{1}|$$

می‌توان دید که برای هر حالت

$$|\phi\rangle = \frac{\mathbb{1}}{\sqrt{T+\mathbb{1}}} \sum_{t=\circ}^T (V_t V_{t-\mathbb{1}} \dots V_{\mathbb{1}} |\eta\rangle_{in,pr,an}) \otimes |t\rangle_C,$$

$H_{prop} |\phi\rangle = \circ$ ؛ زیرا:

$$H_{prop} |\phi\rangle = \sum_{t=\circ}^{T-\mathbb{1}} -(V_{t+\mathbb{1}} V_t \dots V_{\mathbb{1}} |\eta\rangle) \otimes |t+\mathbb{1}\rangle \\ + \sum_{t=\circ}^{T-\mathbb{1}} -(V_{t+\mathbb{1}}^\dagger V_{t+\mathbb{1}} V_t \dots V_{\mathbb{1}} |\eta\rangle) \otimes |t\rangle \\ + \sum_{t=\circ}^{T-\mathbb{1}} (V_{t+\mathbb{1}} V_t \dots V_{\mathbb{1}} |\eta\rangle) \otimes |t+\mathbb{1}\rangle \\ + \sum_{t=\circ}^{T-\mathbb{1}} (V_{t+\mathbb{1}}^\dagger V_{t+\mathbb{1}} V_t \dots V_{\mathbb{1}} |\eta\rangle) \otimes |t\rangle = \circ$$

حال تعریف کنید:

$$H = H_{in} + H_{out} + H_{prop}.$$

در ادامه α و β را به نحو مناسبی انتخاب خواهیم کرد تا (H, α, β) عضو k -LH باشد.

نخست فرض کنید $x \in \Pi_{Yes}$ است. در این صورت اثبات $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ موجود است که با احتمال حداقل $1 - \epsilon$

توسط مدار تصدیق‌کننده‌ی V پذیرفته می‌شود. می‌خواهیم در این حالت همیلتنی ساخته‌شده به صورت بالا، حالت پایه‌ای کمتر از α داشته باشد. توجه کنید که

$$\begin{aligned} \langle \psi_{hist} | H | \psi_{hist} \rangle &= \langle \psi_{hist} | H_{in} | \psi_{hist} \rangle + \langle \psi_{hist} | H_{out} | \psi_{hist} \rangle + \langle \psi_{hist} | H_{prop} | \psi_{hist} \rangle \\ &= 0 + 0 + \frac{1}{T+1} \Pr[\psi \text{ را نپذیرد } | \psi, V] \leq \frac{\epsilon}{T+1} \end{aligned}$$

بنابراین کافی است قرار دهیم $\alpha = \frac{\epsilon}{T+1}$.

حال فرض کنید $x \in \Pi_{No}$ است. در این صورت برای هر اثبات $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ ، احتمال پذیرفته شدن $|\psi\rangle$ توسط مدار V حداکثر ϵ است. کیتائف با استفاده از لمی که به لم هندسی^{۶۴} مشهور است نشان داد که در این حالت، نامساوی زیر برقرار خواهد بود:

$$\lambda_{min}(H) \geq \frac{\pi^2(1-\sqrt{\epsilon})}{2(T+1)^2}.$$

در این‌جا از بیان اثبات لم خودداری می‌کنیم. خواننده‌ی علاقه‌مند می‌تواند اثباتی برای این لم را در [۶۶] بیابد. با استفاده از آن چه در بالا به دست آمد، کافی است قرار دهیم $\beta = \frac{\pi^2(1-\sqrt{\epsilon})}{2(T+1)^2}$. به این ترتیب، تحویل مورد نظر یافت می‌شود.

تنها مشکلی که در این‌جا وجود دارد آن است که همیلتنی‌های معرفی‌شده، همیلتنی‌هایی ۵-موضعی نیستند. با کمی دقت می‌توان دریافت که همیلتنی‌های ارائه‌شده روی تمام کیوبیت‌های رجیستر کلاک به طور نابدیهی عمل می‌کنند؛ و می‌دانیم رجیستر کلاک متشکل از $O(\log n)$ کیوبیت است. به علاوه، در همیلتنی H_{in} می‌توان دید که عملگرهای $|x\rangle\langle x| - \mathbb{I}$ و $|\circ \dots \circ\rangle\langle \circ \dots \circ| - \mathbb{I}$ ۵-موضعی نیستند. رفع مشکل در حالت دوم ساده است. مثلاً می‌توان $|\circ \dots \circ\rangle\langle \circ \dots \circ| - \mathbb{I}$ را با $\sum_{i=1}^{q(n)} |1\rangle\langle 1|_{ani}$ جایگزین کرد؛ که مقصود از $|1\rangle\langle 1|_{ani}$ نگاهی است که تنها کیوبیت i ام رجیستر کمکی را روی زیرفضای تولید شده توسط $|1\rangle$ می‌افکند و بر روی باقی کیوبیت‌ها به صورت بدیهی عمل می‌کند. مشاهده می‌شود که حالت پایه‌ی همیلتنی مزبور با چنین تعویضی، تغییر نمی‌کند.

برای رفع مشکل رجیستر کلاک، باید از روش دیگری استفاده کرد. فرض کنید به جای آن که کلاک را به صورت دودویی کد کنیم، این کار را به طور یک‌یکی^{۶۵} انجام دهیم. به عبارت دیگر، فرض کنید نمایش لحظه‌ی t در این رجیستر، به صورت $|1^t \circ T^{-t}\rangle$ باشد. در این صورت چک کردن محتوای رجیستر کلاک با چک کردن تنها سه کیوبیت از آن امکان‌پذیر است (کیوبیت‌های $1-t$ ، t ، $t+1$ ام).

به این ترتیب با توجه به این‌که گیت‌های V_i حداکثر ۲-موضعی هستند و حالت رجیستر کلاک نیز با عملگری حداکثر ۳-موضعی چک می‌شود، همیلتنی‌های ارائه‌شده ۵-موضعی خواهند بود. تنها نکته‌ای که باید به آن توجه کرد این است که در بالا، تلویحاً فرض شده است که کدینگ رجیستر کلاک حتماً به صورت $1^t \circ T^{-t}$ است. برای این‌که این التزام را ایجاد کنیم، همیلتنی دیگری را نیز به صورت زیر تعریف می‌کنیم:

$$H_C = \mathbb{I}_{in,pr,out} \otimes \left(\sum_{i=1}^{T-1} |\circ\rangle\langle \circ|_{C_i} \otimes |1\rangle\langle 1|_{C_i} \right).$$

به این ترتیب همیلتنی جدید

$$H = H_{in} + H_{out} + H_{prop} + H_C$$

همیلتنی ۵-موضعی مطلوب ما خواهد بود. می‌توان نشان داد که با اعمال تغییرات فوق، $|\psi_{hist}\rangle$ همچنان حالت پایه‌ی همیلتنی جدید باقی می‌ماند؛ و ثوابت درستی و تمامیتی که انتخاب کرده بودیم نیز هم‌چنان کار می‌کنند.

■

یادداشت ۷.۵ نخستین اثبات قضیه‌ی کوک-لوین کوانتومی، که تحویلی از هر مسأله‌ی QMA به LH -۵ ارائه می‌کند، منسوب به کیتائف است و در [۶۶] بیان شده است. رگف و کمپ در [۶۵] این نتیجه را بهبود بخشیدند و نشان دادند LH -۳ مسأله‌ای کامل برای QMA است. نهایتاً کمپ، رگف و کیتائف در [۶۴] نشان دادند که LH -۲ نیز مسأله‌ای QMA -کامل است.

▷

نتیجه ۸.۵ نتیجه‌ی سر راست قضیه‌ی کوک-لوین کوانتومی این است که با فرض $QMA \neq BQP$ ، مسأله‌ی همیلتنی موضعی را نمی‌توان حتی با کامپیوترهای کوانتومی به صورت کارایی حل کرد. همان‌گونه که پیشتر بیان شد،

⁶⁴geometric lemma

⁶⁵unary

مسئله‌ی همپلتنی‌های موضعی حالت خاصی از مسئله‌ای کلی‌تر، یعنی مسئله‌ی شبیه‌سازی سیستم‌های کوانتومی است. در واقع، قضیه‌ی کوک-لوین کوانتومی موید این مطلب است که مطالعه‌ی سیستم‌های کوانتومی می‌تواند از نظر محاسباتی، حتی در حضور کامپیوترهای کوانتومی، سخت باشد.

نتیجه ۹.۵ نتیجه‌ای دیگر از سختی k -LH برای کلاس QMA این است که با فرض $QMA \neq NP$ ، همپلتنی‌هایی وجود دارند که حالت پایه‌ی آن‌ها توصیف کارای کلاسیک ندارد. می‌توان نشان داد که این مطلب بدان معنی است که حالت پایه‌ی چنین همپلتنی‌هایی قویاً درهم‌تنیده است^{۶۶}. این نتیجه، موید بسیاری از خواص فیزیکی مانند ابرشارگی^{۶۷} و ابررسانایی^{۶۸} است که ماده در دمای نزدیک به صفر از خود نشان می‌دهد، و برخاسته از وجود نوعی درهم‌تنیدگی قوی در حالت آن است.

۳.۵ اثبات‌های قابل بررسی احتمالاتی کوانتومی

۱.۳.۵ قضیه‌ی PCP کلاسیک

فرض کنید قرار است درستی اثبات یک قضیه را بررسی کنید. متأسفانه اثبات‌ها می‌توانند بسیار طولانی باشند. مثلاً اثبات قضیه‌ی لافورگ که در سال ۲۰۰۰ در پی کامل کردن برنامه‌ی لنگلندز^{۶۹} توسط لورن لافورگ ارائه شد، چیزی در حدود ۶۰۰ صفحه است! بسیار جالب بود اگر می‌توانستید از کل اثبات تنها یک خط را بخوانید و مطمئن شوید که اثبات درست است یا نه؛ و به این ترتیب می‌توانستید در زمان نیز صرفه‌جویی کنید. اگرچه برای داوران ژورنال‌ها حتی تصور کردن چنین خیالی نیز دلپذیر است، با این حال به نظر عجیب می‌رسد و بعید است که بتوان آن را عملی کرد. در واقع اگر شما بخشی از اثبات را به عنوان نمونه‌ی کوچکی در نظر بگیرید، همواره این احتمال وجود دارد که ایراد اثبات در آن قسمتی باشد که شما آن را در نظر نگرفته‌اید (حتی اگر قسمت «کوچکی» را چک نکرده باشید)؛ چه برسد به این که برای تحقیق درستی اثبات، فقط یک خط آن را در نظر بگیرید.

با این همه، بگذارید توجه خود را به جای هر اثباتی، به معنای عام ریاضیاتی آن، معطوف به اثبات‌هایی کنیم که برای یک ورودی مسئله‌ای در کلاس NP داده می‌شود. یک نگرش به قضیه‌ی PCP، این را بیان می‌کند که راهی وجود دارد که بتوان چنین اثباتی را به گونه‌ای بازنویسی کرد که تصدیق‌کننده، که قرار است در زمان چندجمله‌ای اثبات را تصدیق کند، بدون نیاز به خواندن کل اثبات، و تنها با خواندن تکه‌ی کوچکی از آن، که به صورت تصادفی انتخاب می‌شود، با احتمال بالا بتواند اطمینان یابد که اثبات درست است یا غلط. این امکان، تعریف جدیدی برای کلاس NP بر حسب نوعی از سیستم‌های اثبات، که به آن‌ها اثبات‌های قابل بررسی احتمالاتی^{۷۰} می‌گویند، در اختیار ما می‌گذارد.

به قضیه PCP می‌توان از منظری دیگر نیز نگریست. همان‌طور که می‌دانیم، اگر $P \neq NP$ باشد، مسائلی وجود خواهند داشت که هیچ راه حل دقیق چندجمله‌ای برایشان وجود ندارد. با این حال، بعضی از مسائل بهینه‌سازی NP —سخت را می‌توان با الگوریتم‌های تقریبی چندجمله‌ای، در حد یک ضریب تقریب کوچک حل کرد؛ به این معنی که الگوریتمی چندجمله‌ای وجود دارد که جوابی که تولید می‌کند، مثلاً از دو برابر جواب بهینه بدتر نیست. برای بسیاری از چنین مسائلی، این ضریب تقریب، حدی دارد. قضیه‌ی PCP روشی برای اثبات وجود چنین محدودیت‌هایی در تقریب‌زدن را فراهم می‌کند و می‌تواند نشان دهد که برای بسیاری از مسائل، الگوریتم‌های تقریبی فعلی، بهینه هستند و ضریب تقریب را نمی‌توان از آنچه که تا کنون بدست آورده‌ایم بهتر کرد؛ و این‌ها نتایجی هستند که ظاهراً بدون قضیه‌ی PCP نمی‌توانستیم به آن‌ها دست پیدا کنیم.

در ادامه‌ی این زیربخش، پس از بیان برخی مقدمات، دو صورت‌بندی معادل برای قضیه‌ی PCP را بیان خواهیم کرد؛ و معادل بودن این دو صورت‌بندی را نشان خواهیم داد.

نمادگذاری ۱۰.۵ فرض کنید \mathbb{P} یک مسئله‌ی بهینه‌سازی باشد. در این صورت برای یک ورودی مسئله مانند I ، مقدار بهینه‌ی مسئله را با $OPT(I)$ نمایش می‌دهیم. اگر A یک الگوریتم برای حل مسئله باشد، مقصود از $A(I)$ پاسخی است که با ورودی I ، توسط الگوریتم A تولید می‌شود.

□

تعریف ۱۱.۵ الگوریتم A را برای مسئله‌ی کمینه‌سازی \mathbb{P} یک الگوریتم $\alpha(n)$ -تقریب گوئیم ($\alpha(n) \geq 1$)، هرگاه برای ورودی I از \mathbb{P} ، $A(I) \leq \alpha(n) OPT(I)$ باشد. به همین ترتیب برای یک مسئله‌ی بیشینه‌سازی \mathbb{P} ، یک الگوریتم $\alpha(n)$ -تقریب است ($\alpha(n) \leq 1$)، هرگاه $A(I) \geq \alpha(n) OPT(I)$. بعلاوه، $\alpha(n)$ را ضریب تقریب می‌نامیم.

^{۶۶} به یاد آورید که در بخش ۳.۲.۲، معیاری ساده برای اندازه‌گیری درهم‌تنیدگی یک حالت کوانتومی بیان کردیم. نسخه‌ی بهبودیافته‌ی این معیار، مفهوم آنتروپی فون نویمان است که معمولاً از آن برای اندازه‌گیری میزان درهم‌تنیدگی استفاده می‌شود.

^{۶۷} superfluidity

^{۶۸} superconductivity

^{۶۹} Langlands program

^{۷۰} Probabilistically checkable proofs



مثال ۱۲.۵ مسأله‌ی MAX-۳SAT را به عنوان مسأله‌ی یافتن بیشترین تعداد پراپزهای ممکن در یک فرمول ۳-CNF که به طور هم‌زمان قابل ارضا شدن هستند، در نظر بگیرید. الگوریتم زیر، الگوریتمی $\frac{1}{3}$ -تقریب برای این مسأله است: الگوریتم را به صورت حریصانه تعریف می‌کنیم. به این صورت که در هر مرحله یک متغیر را انتخاب می‌کنیم، مقداری از $\{true, false\}$ به آن نسبت می‌دهیم به طوری که بیشترین تعداد پراپتز را برآورده کند. بعد از آن، عباراتی که برآورده شده‌اند را از مسأله حذف کرده و به سراغ متغیر بعدی می‌رویم. همین کار را انجام می‌دهیم تا زمانی که تمام متغیرها مقداردهی شوند. با توجه به نحوه‌ی مقداردهی به هر متغیر، واضح است که در هر قدم الگوریتم، اگر برآورده شدن یا نشدن t عبارت مشخص شود، حداقل $\frac{t}{3}$ آنها برآورده می‌شوند و بنابراین در نهایت حداقل $\frac{1}{3}$ کل عبارات اولیه برآورده شده‌اند. بنابراین الگوریتم پیشنهادشده یک الگوریتم $\frac{1}{3}$ -تقریب برای مسأله‌ی MAX-۳SAT است. \diamond

تعریف ۱۳.۵ برای مسأله‌ی کمینه‌سازی \mathcal{P} ، مسأله‌ی $Gap-\mathcal{P}_{h(n),g(n)}$ یک مسأله‌ی قراردادی است که در آن برای ورودی I با طول n :

- $OPT(I) \leq h(n)$ اگر و تنها اگر $I \in Gap-\mathcal{P}_{h(n),g(n)}_{Yes}$
- $OPT(I) \geq g(n)h(n)$ اگر و تنها اگر $I \in Gap-\mathcal{P}_{h(n),g(n)}_{No}$



به طور مشابه، تعریف بالا را می‌توان برای مسأله‌های بیشینه‌سازی نیز انجام داد. اهمیت تعریف بالا آن‌جاست که می‌توان از آن برای نشان دادن سختی حل تقریبی یک مسأله‌ی بهینه‌سازی بهره گرفت. در واقع، برای آن‌که نشان دهیم حل کردن \mathcal{P} با ضریب تقریب $\alpha(n)$ در زمان چندجمله‌ای مسأله‌ای سخت است، کافی است نشان دهیم $Gap-\mathcal{P}_{\alpha(n)}$ مسأله‌ی \mathcal{NP} -سخت است. گزاره‌ی زیر، چرایی این امر را بیان می‌کند.

گزاره ۱۴.۵ فرض کنید برای یک مسأله‌ی کمینه‌سازی \mathcal{P} ، مسأله‌ی $Gap-\mathcal{P}_{h(n),\alpha(n)}$ \mathcal{NP} -سخت است. در این صورت الگوریتمی $\alpha(n)$ -تقریب با زمان چندجمله‌ای برای \mathcal{P} وجود ندارد؛ مگر آن‌که $\mathcal{P} = \mathcal{NP}$ باشد.

برهان. با فرض وجود الگوریتمی $\alpha(n)$ -تقریب با زمان چندجمله‌ای برای \mathcal{P} (مثلاً A)، می‌توانیم هر مسأله‌ی \mathcal{NP} -کامل مانند L را در زمان چندجمله‌ای حل کنیم. به این ترتیب که برای هر $x \in \{0, 1\}^*$ ، ابتدا با تحویل چندجمله‌ای موجود از L به $Gap-\mathcal{P}_{h(n),\alpha(n)}$ ، یک ورودی مانند I_x را برای مسأله‌ی $Gap-\mathcal{P}_{h(n),\alpha(n)}$ بدست می‌آوریم. حال، الگوریتم $\alpha(n)$ -تقریب موجود برای حل \mathcal{P} را روی I_x اجرا می‌کنیم. توجه کنید که:

- $I_x \in Gap-\mathcal{P}_{h(n),\alpha(n)}_{Yes} \implies OPT(I_x) \leq h(n) \implies A(I_x) \leq \alpha(n)h(n)$
- $I_x \in Gap-\mathcal{P}_{h(n),\alpha(n)}_{No} \implies OPT(I_x) \geq \alpha(n)h(n) \implies A(I_x) \geq \alpha(n)h(n)$

بنابراین با توجه به مقدار $A(I_x)$ ، می‌توان $Gap-\mathcal{P}_{h(n),\alpha(n)}$ و در نتیجه L را تصمیم گرفت.



حال قادر هستیم اولین صورت قضیه‌ی PCP را بیان کنیم.

قضیه ۱۵.۵ (قضیه‌ی PCP: سختی تقریب) ثابت $\rho < 1$ وجود دارد به نحوی که $Gap-MAX-3SAT_{1,\rho}$ \mathcal{NP} -سخت است [۱۳].

در این جا شایان ذکر است که نتیجه‌ی فوق را می‌توان بر بسیاری دیگر از مسائل بهینه‌سازی \mathcal{NP} -کامل پیاده کرد. بدین منظور کافی است تعریفمان از تحویل را به صورت زیر تغییر دهیم:

تعریف ۱۶.۵ فرض کنید \mathcal{P} و \mathcal{P}' دو مسأله‌ی بیشینه‌سازی باشند. یک تحویل حافظ فاصله γ از \mathcal{P} به \mathcal{P}' با پارامترهای $(g(n), g'(n'), h(n), h'(n'))$ که $g(n), g'(n') \leq 1$ ، عبارت است از الگوریتمی که هر ورودی I مانند I را، که طول I برابر n است، به یک ورودی برای \mathcal{P}' مانند I' نظیر می‌کند، که طول I' برابر با n' است؛ به نحوی که:

- اگر $OPT(I) \geq h(n)$ ، آنگاه $OPT(I') \geq h'(n')$
- اگر $OPT(I) \leq g(n)h(n)$ ، آنگاه $OPT(I') \leq g'(n')h'(n')$



به سادگی می‌توان دید که اگر تحویلی حافظ فاصله و چندجمله‌ای از \mathcal{P} به \mathcal{P}' با پارامترهای $(g(n), g'(n'), h(n), h'(n'))$ موجود باشد، در این صورت اگر $Gap-\mathcal{P}_{h(n),g(n)}$ مسأله‌ی \mathcal{NP} -کامل باشد،

⁷¹gap-preserving reduction

را اثبات کرد. $Gap-PCP_{h'(n'),g'(n')}$ نیز چنین است. به این ترتیب، می‌توان با استفاده از قضیه ۱۵.۵، سختی تقریب مسائل بیشتری را اثبات کرد. حال به صورت بندی دوم قضیه PCP می‌پردازیم.

تعریف ۱۷.۵ یک تصدیق کننده $(r(n), q(n))$ -محدود، تصدیق کننده‌ای چندجمله‌ای است که به استفاده از حداکثر $r(n)$ بیت تصادفی محدود است؛ و قادر است تنها با استفاده از برآمد این بیت‌های رندوم، حداکثر $q(n)$ کوئری به بیت‌های مختلف اثبات برزند و آن‌ها را بخواند.

تعریف ۱۸.۵ کلاس پیچیدگی $PCP(r(n), q(n))$ عبارت است از همگی زبان‌هایی مانند L ، به طوری که تصدیق کننده $(r(n), q(n))$ -محدودی مانند V برایشان وجود دارد چنانکه:

- اگر $x \in L$ ، در این صورت اثبات π موجود است که $\Pr[V(x, \pi) = 1] = 1$
- اگر $x \notin L$ ، در این صورت برای هر اثبات π ، $\Pr[V(x, \pi) = 1] \leq \frac{1}{2}$

قضیه ۱۹.۵ (قضیه PCP: اثبات‌های قابل بررسی احتمالاتی) $PCP(\mathcal{O}(\log n), \mathcal{O}(1)) = \mathcal{NP}$ [۱۳].

قضیه فوق، به طور شگفت‌آوری با شهود ما در تناقض است. مثلاً فرمول ۳-CNF ای را در نظر بگیرید که ارضاشدنی نیست؛ اما تمام پرانتزهای آن به جز یکی به طور همزمان ارضاشدنی هستند. برای چنین فرمولی، به نظر می‌رسد اثباتی وجود دارد که با نگاه کردن تصادفی به تنها $\mathcal{O}(1)$ بیت از آن، نتوان با احتمال بالا عضویت فرمول را در ۳-SAT رد کرد. با این حال، شگفتی قضیه PCP در آن است که وجود نوعی از اثبات‌های «قدرتمند» را برای مسأله‌های \mathcal{NP} پیشنهاد می‌دهد؛ به این معنی که اگر ایرادی در بخش کوچکی از اثبات وجود داشته باشد، این ایراد در سرتاسر این اثبات‌های قدرتمند پراکنده شده است و با احتمال بالایی می‌توان آن را تشخیص داد.

نخستین اثبات قضیه PCP، که اثباتی جبری و مبتنی بر نظریه کدگذاری است، در [۱۳] مطرح شده است؛ گرچه بسیاری از بخش‌های اثبات، نتایجی هستند که در [۱۲] اثبات شده بودند. اثباتی جدیدتر و ترکیباتی، با تکیه بر ویژگی‌های گراف‌های گسترده، توسط دینور در [۴۲] ارائه شده است. هر دوی اثبات‌ها طولانی و پیچیده هستند و بیان آن‌ها در این مقاله نمی‌گنجد. با این حال، به عنوان خاتمه‌ای این بخش، نشان خواهیم داد که دو صورت بیان‌شده از قضیه PCP با هم معادلند.

قضیه ۲۰.۵ $\mathcal{NP} = PCP(\mathcal{O}(\log n), \mathcal{O}(1))$: اگر و تنها اگر ثابت ρ وجود داشته باشد به نحوی که $Gap-MAX-3SAT_{1,\rho}$ -سخت \mathcal{NP} باشد [۱۳].

برهان. ابتدا سمت «اگر» را ثابت می‌کنیم. این که $PCP(\mathcal{O}(\log n), \mathcal{O}(1)) \subseteq \mathcal{NP}$ را به سادگی می‌توان اثبات کرد. فرض کنید $L \in PCP(\mathcal{O}(\log n), \mathcal{O}(1))$ باشد. در این صورت تصدیق کننده $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود V برای L وجود دارد. توجه کنید که طول اثبات حداکثر $2^{\mathcal{O}(\log n)}$ بیت است. حال تصدیق کننده‌ای مانند V' را در نظر بگیرید که برآمد بیت‌های تصادفی را حدس می‌زند؛ و برای هر حدس، احتمال آن که V اثبات را با توجه به کوئری‌هایی که بر اساس برآمد بیت‌های تصادفی تعیین می‌شوند، بپذیرد حساب می‌کند؛ و اگر این احتمال برابر ۱ باشد، اثبات را می‌پذیرد. روشن است که V یک ماشین غیرقطعی چندجمله‌ای است که L را می‌پذیرد. بنابراین $L \in \mathcal{NP}$.

حال می‌خواهیم نشان دهیم $\mathcal{NP} \subseteq PCP(\mathcal{O}(\log n), \mathcal{O}(1))$. بدین منظور نشان می‌دهیم هر زبان $L \in \mathcal{NP}$ یک تصدیق کننده $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود دارد. با توجه به تحویلی که از $L \in Gap-MAX-3SAT_{1,\rho}$ وجود دارد، هر $x \in \{0, 1\}^*$ به فرمولی ۳-CNF مانند ϕ_x نگاشته می‌شود که متغیرهای y_1, y_2, \dots, y_k و پرانتزهای با اجرای الگوریتم تحویل، از ورودی x فرمول ϕ_x را به دست می‌آورد. سپس با استفاده از $\log m \in \mathcal{O}(\log n)$ بیت تصادفی، به تصادف یکی از پرانتزها را انتخاب می‌کند. در این جا، اثبات گمارشی از مقادیر $\{true, false\}$ به متغیرهای y_1, y_2, \dots, y_k است. با توجه به پرانتز انتخاب‌شده، تصدیق کننده مقادیر مربوط به متغیرهای ظاهر شده در پرانتز مزبور را از اثبات می‌خواند؛ و اثبات را می‌پذیرد اگر و فقط اگر با آن مقادیر، پرانتز مزبور ارضا شود. توجه کنید در حالتی که ϕ_x ارضاپذیر است و اثباتی وجود دارد که توسط تصدیق کننده پذیرفته شود. در حالتی که $x \notin L$ ، احتمال آن که اثباتی توسط تصدیق کننده پذیرفته شود، حداکثر برابر ρ است (زیرا تعداد پرانتزهایی که همزمان ارضاشدنی هستند، ρ برابر تعداد کل پرانتزهاست). از طرفی، با تکرار می‌توان خطا را کاهش داد و به $\frac{1}{2}$ رساند. بنابراین تصدیق کننده‌ای $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود برای L وجود دارد.

حال به اثبات سمت «تنها اگر» می‌پردازیم. فرض کنید $L \in \mathcal{NP}$ است و تصدیق کننده $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود دارد. حال یک مسأله‌ی CSP را به این صورت طرح می‌کنیم: متغیرهای $y_1, y_2, \dots, y_{|\pi|}$ نمایانگر بیت‌های اثبات π هستند؛ و برای هر برآمد از بیت‌های تصادفی مانند C_0, C_1, \dots, C_o قیدی است که تنها وابسته به بیت‌هایی است که با توجه به آن برآمد از اثبات خوانده می‌شوند؛ و C_0 برآورده می‌شود، اگر و تنها اگر تصدیق کننده با خواندن بیت‌هایی از اثبات که با توجه به C_0 تعیین شده‌اند، اثبات را بپذیرد.

توجه کنید که هر قید CSP فوق، تنها به $O(1)$ متغیر وابسته است؛ و $2^{O(\log n)}$ قید دارد. در حالتی که $x \in L$ ، می‌دانیم اثباتی وجود دارد که تصدیق‌کننده با احتمال ۱ آن را می‌پذیرد؛ پس ورودی مسأله‌ی CSP بالا که از روی x تولید می‌شود نیز حتماً ارضاشدنی است. در حالتی که $x \notin L$ ، برای هر اثبات π ، احتمال پذیرفته‌شدن اثبات توسط تصدیق‌کننده حداکثر $\frac{1}{4}$ است؛ بنابراین حداکثر $\frac{1}{4}$ قیود ورودی مسأله به طور همزمان ارضا شدنی هستند. بنابراین یک تحویل از L به $Gap\text{-CSP}$ بالا ارائه شد.

حال توجه کنید که CSP بالا را می‌توان به یک فرمول ۳-CNF تبدیل کرد. در واقع، هر قید k موضعی را می‌توان به یک فرمول ۳-CNF با k^2 پراکنش تبدیل کرد، به طوری که ارضاپذیری ورودی CSP با ارضاپذیری فرمول ۳-CNF یکسان باشد. به این ترتیب، ثوابت تمامیت و درستی به ترتیب برابر با ۱ و $1 - \frac{1}{k^2}$ خواهد بود؛ که می‌دانیم با تکرار می‌توان ثابت درستی را به عددی ثابت کاهش داد. از طرفی چون $k \in O(1)$ ، تحویل به دست آمده تحویلی چندجمله‌ای است. ■

۲.۳.۵ حدس PCP کوانتومی

همان‌گونه که تا به این‌جا دیده‌ایم، همتای بسیاری از مفاهیم و نتایج پیچیدگی محاسباتی کلاسیک را می‌توان در محاسبات کوانتومی جست‌وجو کرد. در بخش قبل، به یکی از درخشان‌ترین نتایج پیچیدگی محاسبات کلاسیک پرداختیم و دو صورت معادل را برای آن بیان کردیم. دور از انتظار نیست که با پیشرفت پیچیدگی محاسبات کوانتومی، در پی معادل کوانتومی این قضیه باشیم. هر چند یافتن چنین معادلی می‌تواند خوشایند باشد، با این حال به نظر می‌رسد هنوز راه زیادی تا اثبات این قضیه باقی است. افزون بر این، حتی درستی یا نادرستی این حدس نیز در حاله‌ای از ابهام است و شواهدی کافی به نفع هیچ‌یک وجود ندارد [۷].

در این زیربخش، به معرفی دو صورت از حدس PCP کوانتومی خواهیم پرداخت. این حدس نخستین بار به صورت دقیق در [۶] صورت‌بندی شده است؛ گرچه شواهدی برای این‌که پیش از این مقاله نیز افراد دیگری به وجود چنین همتای کوانتومی‌ای برای قضیه‌ی PCP امیدوار بوده‌اند، در [۱۰] و [۱] قابل مشاهده است.

تعریف ۲۱.۵ یک تصدیق‌کننده‌ی $QPCP(k)$ ، تصدیق‌کننده‌ای کوانتومی است که با در اختیار داشتن اثباتی مانند $(|\psi\rangle) \in (\mathbb{C}^2)^{\otimes p(n)}$ ، ابتدا به صورت تصادفی k بیت از اثبات مانند (i_1, i_2, \dots, i_k) را انتخاب می‌کند؛ و سپس مدار V_{i_1, i_2, \dots, i_k} را روی ورودی، k بیت مشخص شده از اثبات و نیز رجیستر کمکی اعمال می‌کند؛ و نهایتاً یک کیوبیت را (که از قبل مشخص کرده) اندازه می‌گیرد و با توجه به حاصل اندازه‌گیری، اثبات را پذیرد یا رد می‌کند.

►

تعریف ۲۲.۵ کلاس پیچیدگی $QPCP(k, c, s)$ عبارت است از تمام مسأله‌های قراردادی مانند $\Pi = (\Pi_{Yes}, \Pi_{No})$ به طوری که تصدیق‌کننده‌ی $QPCP(k)$ وجود دارد چنان‌که:

- اگر $x \in \Pi_{Yes}$ ، در این صورت اثبات $|\psi\rangle$ وجود دارد که توسط تصدیق‌کننده با احتمال حداقل c پذیرفته می‌شود.
- اگر $x \in \Pi_{No}$ ، در این صورت برای هر اثبات $|\psi\rangle$ ، تصدیق‌کننده با احتمال حداکثر s اثبات را می‌پذیرد.

►

حدس ۲۳.۵ (حدس QPCP: نسخه‌ی اثبات‌های قابل بررسی احتمالاتی) $QMA = QPCP(O(1), c, s)$ که در آن، $c - s = \Omega(1)$ [۶].

پیش از بیان نسخه‌ی سختی تقریب این حدس، از تعریف ۲.۵ به یاد آورید که تا به این‌جا، فرض کرده بودیم فاصله‌ی قراردادی در مسأله‌ی همیلتنی‌های موضعی، یک چندجمله‌ای است؛ و به جهت اختصار از ذکر آن اجتناب می‌کردیم. با این حال، مسأله‌ی $k\text{-LH}$ را می‌توان برای فاصله‌های قراردادی دیگر نیز تعریف کرد. افزون بر این، از این‌جا به بعد فرض کنید که در مسأله‌ی همیلتنی موضعی، همه‌ی جمله‌های موضعی ورودی، نگاشت‌هایی مثبت نیمه‌معین هستند که نرم اثرشان حداکثر برابر ۱ است.

حدس ۲۴.۵ (حدس QPCP: نسخه‌ی سختی تقریب) ثابت $\gamma > 0$ وجود دارد به طوری که $k\text{-LH}$ با فاصله‌ی قراردادی γ ، تحت تحویل چند به یک چندجمله‌ای کوانتومی، مسأله‌ای QMA -سخت است [۶]. مقصود از یک تحویل چند به یک چندجمله‌ای کوانتومی در گزاره‌ی بالا یک الگوریتم کوانتومی و چندجمله‌ای است که با احتمال ثابت و ناصفر، تابع تحویل را پیاده‌سازی می‌کند.

یادداشت ۲۵.۵ مشابه با قضیه‌ی PCP کلاسیک، می‌توان نشان داد دو صورت بیان شده از حدس QPCP در بالا نیز با یکدیگر معادلند. در واقع اثبات یک سمت آن، سمتی که نسخه‌ی سختی تقریب نسخه‌ی اثبات‌های قابل بررسی احتمالاتی را نتیجه می‌دهد، ساده است؛ و می‌توان دید که چنانچه فاصله‌ی قراردادی مسأله‌ی $k\text{-LH}$ مقداری ثابت باشد، تصدیق‌کننده‌ای که در قضیه‌ی ۵.۵ ارائه کردیم تصدیق‌کننده‌ای $QPCP(k)$ است که ثوابت درستی و تمامیتی با فاصله‌ی ثابت خواهد

داشت. سمت دیگر دشوارتر است؛ و به نظر می‌رسد بدون فرض کامل بودن تحت تحویل کوانتومی، قادر به اثبات آن نیستیم. خواننده‌ی علاقه‌مند می‌تواند اثباتی برای سمت دیگر را در [۵۳] بیابد.

یادداشت ۲۶.۵ در نتیجه‌ی ۹.۵ دیدیم که درستی قضیه‌ی کوک-لوین کوانتومی نتیجه می‌دهد که سیستم‌هایی فیزیکی وجود دارند که اگر آن‌ها را تا دمای صفر سرد کنیم، در حالتی قویاً درهم‌تنیده قرار می‌گیرند. به طریقی مشابه، درستی حدس PCP کوانتومی، همراه با فرض $QMA \neq QCMA$ نتیجه خواهد داد که سیستم‌هایی فیزیکی وجود دارند که حالت آن‌ها حتی در دمای متناهی ناصفر نیز قویاً درهم‌تنیده است. چنین نتیجه‌ای خلاف شهود فیزیکی متخصصان نظریه‌ی سیستم‌های چندپیکره است؛ چه آن‌ها بر این باورند که نمی‌توان در دماهای بالا شاهد اثرات کوانتومی با مقیاس بزرگ بود؛ و مثلاً تلاش برای یافتن موادی که در دمای اتاق ابررسانا باشند، ناموفق است. به این ترتیب، چنانچه حدس PCP کوانتومی ثابت شود، بر شهود فیزیکی استاندارد ما نیز تاثیر خواهد گذاشت [۷].

۶ مؤخره: پیشرفت‌های جدیدتر و زمینه‌های پژوهش

در این بخش اجمالاً اشاره‌ای به برخی زمینه‌های پژوهش که مرتبط با اثبات‌های غیر تعاملی کوانتومی هستند، و نیز پیشرفت‌های نسبتاً جدیدتری که در این زمینه‌ها رخ داده است، خواهیم داشت.

۱. در جست‌وجوی ارتباطاتی عمیق‌تر بین فیزیک و نظریه‌ی محاسبه: همان‌گونه که در طول این پایان‌نامه دیدیم، برخی زمینه‌های پژوهش حول اثبات‌های کوانتومی ارتباطات عمیقی میان مفهوم محاسبه و نظریه‌های فیزیکی برقرار می‌کنند. مطالعه‌ی چنین ارتباط‌هایی از دو جهت حائز اهمیت است:

- همان‌گونه که در یادداشت آغازین فصل ۵ اشاره شد، پیچیدگی همیلتنی کوانتومی حوزه‌ای است که از یک سو مورد توجه فیزیکدان‌های سیستم‌های چندپیکره و از دیگر سو مورد توجه پژوهشگران علوم کامپیوتر است. با وجود آن‌که معمولاً متخصصین علوم کامپیوتر، چندان علاقه‌ای به وجه فیزیکی مسائل ندارند و ترجیح می‌دهند تا حد امکان از درگیر شدن با آن اجتناب کنند، به نظر می‌رسد که توجه به این وجه، ضروری و پیش‌برنده‌ی مسائل این حوزه باشد. در توضیح می‌توان گفت که یک رویکرد به روند توسعه‌ی نظریه‌ی پیچیدگی محاسبات کوانتومی، همان‌گونه که تا به این‌جای این پایان‌نامه بارها بر آن تاکید کرده‌ایم، تلاش برای یافتن آنالوژی‌های میان محاسبات کلاسیک و محاسبات کوانتومی است. نظریه‌ی محاسبه و پیچیدگی محاسبه‌ی کلاسیک در طول حدود یک قرن که از تولد آن می‌گذرد، دستاوردهای متعدد و درخشانی داشته است؛ و حال با ظهور مدل محاسباتی جدیدی به نام محاسبات کوانتومی، این‌که آیا نتایج مشابهی در این زمینه نیز یافت خواهد شد، کنج‌کاوی‌برانگیز است. با این حال، این سوال ممکن است در ذهن ایجاد شود که آیا چنین نتایج «مشابهی»، واقعاً سودمند و عمیق نیز هستند؟ این‌جاست که اهمیت فیزیکی مسأله می‌تواند به عنوان راهنمایی برای گزینش مسائل «خوب» به یاری ما بیاید [۸۵].

همان‌گونه که در یادداشت‌های ۹.۵ و ۲۶.۵ دیدیم، مسائلی که در حال حاضر در پیچیدگی همیلتنی از منظر محاسباتی مورد مطالعه قرار دارند، معنایی فیزیکی نیز دارند؛ و نتایج آن‌ها نه تنها برای فیزیکدانان نظری، بلکه برای متخصصان و مهندسان زمینه‌های دیگر نیز اهمیت دارد (برای نمونه رجوع کنید به [۵۱]). پژوهش‌های متعددی در سال‌های اخیر صورت گرفته است که با توجه به این معناداری فیزیکی، محدودیت‌هایی روی همیلتنی‌هایی که ممکن است در حدس QPCP ظاهر شوند، قرار داده شود. مثلاً برخی همیلتنی‌هایی که این حدس نمی‌تواند برای آن‌ها درست باشد در [۲۹] مورد مطالعه قرار گرفته‌اند.

- وجهی دیگر از این ارتباطات، تاثیر آن بر پیشبرد فیزیک نظری است. آن‌گونه که ویگگرسون در [۹۲] می‌گوید، «شاید خواسته‌ی فیزیکدانان برای درک ساختار بنیادین فضا و زمان فیزیکی، وابسته به داشتن فهمی عمیق از منابع محاسباتی فضا و زمان باشد». نمونه‌ای از چنین تاثیراتی را می‌توان در کار هارلو و هایدن در [۵۹] دید؛ که به بررسی همواری افق‌های سیاه‌چاله‌ها از منظر محاسباتی و ارتباط این موضوع با اثبات‌های دانش صفر کوانتومی می‌پردازد. انتظار می‌رود که موارد بیشتری از چنین ارتباطاتی، در حوزه‌های مختلف فیزیک یافت شود؛ و باور بر این است که آشنایی فیزیکدانان با مفاهیم و روش‌های محاسباتی، به شکوفایی‌های بیشتری در دستاوردهای فیزیکی می‌انجامد [۹۲].

۲. در تلاش برای شناختن بهتر نسخه‌های مختلف QMA : همان‌گونه که در زیربخش ۲.۳.۵ دیدیم، یکی از صورت‌های حدس PCP کوانتومی مرتبط با یافتن صورت‌بندی جدیدی از کلاس QMA با استفاده از نوعی تصدیق‌کننده‌های بسیار کارا است. به نظر می‌رسد چنانچه کلاس QMA و نسخه‌های مختلف آن را بهتر بشناسیم، راه ما برای یافتن اثباتی در تایید یا رد این حدس هموارتر خواهد شد [۷]. از طرفی، همان‌گونه که در بخش ۲.۴ بحث کردیم، مسائل حل‌نشده‌ی بسیاری درباره‌ی ارتباط میان این کلاس‌ها وجود دارد؛ و همین سبب شده است که بخشی از توجه پژوهشگران پیچیدگی محاسبات کوانتومی معطوف به مطالعه‌ی روابط میان این کلاس‌ها و مسائل کامل آن‌ها شود. نمونه‌هایی از برخی از این پژوهش‌های متاخر را می‌توان در [۲۴، ۳۱، ۵۴] مشاهده کرد.

۳. نتایج یافته‌های پیچیدگی کوانتومی در پیچیدگی کلاسیک: پیشرفت‌های پیچیدگی محاسبات کوانتومی در سال‌های اخیر به حصول نتایج ارزشمندی در محاسبات کلاسیک انجامیده است. یکی از نمونه‌های چنین پیامدهایی، یافتن صورت‌بندی جدیدی از کلاس NP از طریق ارائه‌ی پروتکلی برای تصدیق یک اثبات SAT به طول m با استفاده از $O(\sqrt{m})$ شاهد کوانتومی غیر درهم‌تنیده به طول $O(\log m)$ است؛ که توسط بیگی و همکاران در [۳] معرفی شده است. نمونه‌های دیگر و متاخرتر، نتیجه‌ای است که توسط آهارونوف و همکاران در [۸] به دست آمده است. در آن‌جا ثابت می‌شود که اثبات حدس PCP کوانتومی برای خانواده‌ی خاصی از همیلتنی‌ها، معادل با پاسخ دادن به MA vs. NP است. مسأله‌ی اخیر، که نمونه‌ای از مسائل غیرتصادفی‌سازی^{۲۲} محسوب می‌شود؛ برنامه‌ای است که در حال حاضر در پیچیدگی محاسبات کلاسیک در جریان است؛ و باور عمومی بر این است که این برنامه به نتیجه خواهد رسید؛ و می‌توان نشان داد که تصادفی‌سازی بر قدرت محاسباتی نمی‌افزاید.

^{۲۲}derandomization

References

- [1] Aaronson, S.: The Quantum PCP manifesto (Oct 2006), <https://scottaaronson.blog/?p=139>
- [2] Aaronson, S.: On Perfect Completeness for QMA. *Quantum Info. Comput.* 9(1), 81–89 (jan 2009)
- [3] Aaronson, S., Beigi, S., Drucker, A., Fefferman, B., Shor, P.: The power of unentanglement. In: *Proceedings of the 2008 IEEE 23rd Annual Conference on Computational Complexity*. p. 223–236. CCC '08, IEEE Computer Society, USA (2008), <https://doi.org/10.1109/CCC.2008.5>
- [4] Aaronson, S., Kuperberg, G.: Quantum versus classical proofs and advice. *Theory of Computing* 3(7), 129–157 (2007), <https://theoryofcomputing.org/articles/v003a007>
- [5] Adleman, L.M., DeMarrais, J., Huang, M.D.A.: Quantum computability. *SIAM Journal on Computing* 26(5), 1524–1540 (1997), <https://doi.org/10.1137/S0097539795293639>
- [6] Aharonov, D., Arad, I., Landau, Z., Vazirani, U.: The detectability lemma and quantum gap amplification. In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. p. 417–426. STOC '09, Association for Computing Machinery, New York, NY, USA (2009), <https://doi.org/10.1145/1536414.1536472>
- [7] Aharonov, D., Arad, I., Vidick, T.: Guest column: the quantum PCP conjecture. *SIGACT News* 44(2), 47–79 (jun 2013), <https://doi.org/10.1145/2491533.2491549>
- [8] Aharonov, D., Grilo, A.B., Liu, Y.: StoqMA vs. MA: the power of error reduction. *CoRR abs/2010.02835* (2020), <https://arxiv.org/abs/2010.02835>
- [9] Aharonov, D., Kitaev, A., Nisan, N.: Quantum circuits with mixed states. *arXiv* (1998)
- [10] Aharonov, D., Naveh, T.: Quantum NP - A Survey (2002), <https://arxiv.org/abs/quant-ph/0210077>
- [11] Akama, S.: *Elements of Quantum Computing: History, Theories and Engineering Applications*. Springer Publishing Company, Incorporated (2014)
- [12] Arora, S., Safra, S.: Probabilistic checking of proofs; a new characterization of NP. In: *Proceedings., 33rd Annual Symposium on Foundations of Computer Science*. pp. 2–13 (1992)
- [13] Arora, S., Lund, C., Motwani, R., Sudan, M., Szegedy, M.: Proof verification and hardness of approximation problems. *Proceedings., 33rd Annual Symposium on Foundations of Computer Science* pp. 14–23 (1992)
- [14] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G., Buell, D.A., et al.: Quantum supremacy using a programmable superconducting processor. *Nature* 574(7779), 505–510 (2019)
- [15] Babai, L., Fortnow, L., Lund, C.: Nondeterministic exponential time has two-prover interactive protocols. In: *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*. pp. 16–25 vol.1 (1990)
- [16] Babai, L., Szemerédi, E.: On the complexity of matrix group problems i. In: *IEEE Annual Symposium on Foundations of Computer Science* (1984)

- [17] Balcazar, J.L., Diaz, J., Gabarro, J.: Structural Complexity I. Springer Publishing Company, Incorporated, 2nd edn. (2012)
- [18] Barenco, A.: A universal two-bit gate for quantum computation. Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences 449(1937), 679–683 (Jun 1995)
- [19] Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P., Sleator, T., Smolin, J.A., Weinfurter, H.: Elementary gates for quantum computation. Physical Review A 52(5), 3457–3467 (Nov 1995)
- [20] Benioff, P.: The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of Statistical Physics 22, 563–591 (1980)
- [21] Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters 70(13), 1895–1899 (Mar 1993)
- [22] Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters 69(20), 2881–2884 (Nov 1992)
- [23] Bernstein, E., Vazirani, U.: Quantum complexity theory. SIAM Journal on Computing 26(5), 1411–1473 (1997), <https://doi.org/10.1137/S0097539796300921>
- [24] Bittel, L., Gharibian, S., Kliesch, M.: Optimizing the depth of variational quantum algorithms is strongly QCMA-hard to approximate (2022)
- [25] Bohr, N.: On the Constitution of Atoms and Molecules, pp. 13–33. Springer International Publishing, Cham (2016), https://doi.org/10.1007/978-3-319-14316-3_2
- [26] Bookatz, A.D.: QMA-Complete Problems. Quantum Info. Comput. 14(5 amp; 6), 361–383 (apr 2014)
- [27] Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature 390(6660), 575–579 (Dec 1997)
- [28] Boyer, M., Brassard, G., Høyer, P., Tapp, A.: Tight bounds on quantum searching. Fortschritte der Physik 46(4-5), 493–505 (jun 1998), <https://doi.org/10.1002/2F%28sici%291521-3978%28199806%2946%3A4%2F5%3C493%3A%3Aaid-prop493%3E3.0.co%3B2-p>
- [29] Brandao, F.G., Harrow, A.W.: Product-state approximations to quantum ground states. In: Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing. p. 871–880. STOC '13, Association for Computing Machinery, New York, NY, USA (2013), <https://doi.org/10.1145/2488608.2488719>
- [30] Bravyi, S., Bessen, A.J., Terhal, B.M.: Merlin-Arthur Games and Stoquastic Complexity (2006), <https://arxiv.org/abs/quant-ph/0611021>
- [31] Chailloux, A., Sattath, O.: The complexity of the separable Hamiltonian problem. 2012 IEEE 27th Conference on Computational Complexity pp. 32–41 (2011)
- [32] Chi-Chih Yao, A.: Quantum circuit complexity. In: Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science. pp. 352–361 (1993)
- [33] Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Quantum algorithms revisited. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences 454(1969), 339–354 (Jan 1998)
- [34] Cleve, R.: An introduction to quantum complexity theory, p. 103–127. World Scientific (Jan 2001)

- [35] Cobham, A.: The intrinsic computational difficulty of functions. In: Bar-Hillel, Y. (ed.) *Logic, Methodology and Philosophy of Science: Proceedings of the 1964 International Congress (Studies in Logic and the Foundations of Mathematics)*, pp. 24–30. North-Holland Publishing (1965)
- [36] Cook, S.A.: The complexity of theorem-proving procedures. In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing*. p. 151–158. STOC '71, Association for Computing Machinery, New York, NY, USA (1971), <https://doi.org/10.1145/800157.805047>
- [37] Dawson, C.M., Nielsen, M.A.: The Solovay-Kitaev algorithm (2005), <https://arxiv.org/abs/quant-ph/0505030>
- [38] Densmore, D., Donahue, W.H., Newton, I.: *Newton's Principia: The central argument*. Green Lion Press (1996)
- [39] Deutsch, D.: Quantum computational networks. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 425(1868), 73–90 (Sep 1989)
- [40] Deutsch, D., Barenco, A., Ekert, A.: Universality in quantum computation. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 449(1937), 669–677 (Jun 1995)
- [41] Deutsch, D., Jozsa, R.: Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439, 553 – 558 (1992)
- [42] Dieks, D.: Communication by EPR devices. *Physics Letters A* 92(6), 271–272 (Nov 1982)
- [43] Dinur, I., Reingold, O.: Assignment testers: towards a combinatorial proof of the PCP theorem. *SIAM Journal on Computing* 36(4), 975–1024 (2006), <https://doi.org/10.1137/S0097539705446962>
- [44] Dirac, P.A.M.: *The Principles of Quantum Mechanics*. Clarendon Press, reprint, revised edn. (1981)
- [45] Einstein, A.: Concerning an heuristic point of view toward the emission and transformation of light. *Annalen Phys.* 17, 132–148 (1905)
- [46] Even, S., Selman, A.L., Yacobi, Y.: The complexity of promise problems with applications to public-key cryptography. *Information and Control* 61(2), 159–173 (1984), <https://www.sciencedirect.com/science/article/pii/S001999588480056X>
- [47] Feynman, R.P.: Simulating physics with computers. *International Journal of Theoretical Physics* 21(6), 467–488 (1982)
- [48] Fortnow, L.: One complexity theorist's view of quantum computing. arXiv (2000)
- [49] Gharibian, S.: Strong NP-hardness of the quantum separability problem. *Quantum Info. Comput.* 10(3), 343–360 (mar 2010)
- [50] Gharibian, S., Huang, Y., Landau, Z., Shin, S.W.: Quantum Hamiltonian complexity. *Foundations and Trends® in Theoretical Computer Science* 10(3), 159–282 (2015), <https://doi.org/10.1561%2F04000000066>
- [51] Gharibian, S., Le Gall, F.: Dequantizing the quantum singular value transformation: hardness and applications to quantum chemistry and the quantum PCP conjecture. In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. p. 19–32. STOC 2022, Association for Computing Machinery, New York, NY, USA (2022), <https://doi.org/10.1145/3519935.3519991>
- [52] Gieres, F.: Mathematical surprises and Dirac's formalism in quantum mechanics. *Reports on Progress in Physics* 63(12), 1893–1931 (nov 2000), <https://doi.org/10.1088%2F0034-4885%2F63%2F12%2F201>

- [53] Grilo, A.: Quantum proofs, the local Hamiltonian problem and applications. Ph.D. thesis (2018)
- [54] Grilo, A.B., Kerenidis, I., Sikora, J.: QMA with subset state witnesses. In: Mathematical Foundations of Computer Science 2015: 40th International Symposium, MFCS 2015, Milan, Italy, August 24-28, 2015, Proceedings, Part II. pp. 163–174. Springer (2015)
- [55] Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. p. 212–219. STOC '96, Association for Computing Machinery, New York, NY, USA (1996), <https://doi.org/10.1145/237814.237866>
- [56] Guo, H.: What Are Tensors Exactly? World Scientific (2021), <https://www.worldscientific.com/doi/abs/10.1142/12388>
- [57] Gurvits, L.: Classical deterministic complexity of Edmonds' problem and quantum entanglement. In: Proceedings of the thirty-fifth ACM symposium on Theory of computing - STOC '03. p. 10. ACM Press, New York, New York, USA (Jun 2003)
- [58] Hao, K.: China seeks a quantum leap in computing (Oct 2022), <https://www.wsj.com/articles/china-competing-us-quantum-computing-11664997892>
- [59] Harlow, D., Hayden, P.: Quantum computation vs. firewalls. Journal of High Energy Physics 2013, 85 (Jun 2013)
- [60] Harrow, A.W., Montanaro, A.: Testing Product States, Quantum Merlin-Arthur Games and Tensor Optimization. J. ACM 60(1) (feb 2013), <https://doi.org/10.1145/2432622.2432625>
- [61] Hirvensalo, M.: Quantum Computing. Springer Publishing Company, Incorporated, 2nd edn. (2010)
- [62] Jordan, S.P., Kobayashi, H., Nagaj, D., Nishimura, H.: Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. Quantum Info. Comput. 12(5–6), 461–471 (may 2012)
- [63] Jozsa, R., Linden, N.: On the role of entanglement in quantum-computational speed-up. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences 459(2036), 2011–2032 (Aug 2003)
- [64] Kempe, J., Kitaev, A., Regev, O.: The complexity of the local Hamiltonian problem. In: Proceedings of the 24th International Conference on Foundations of Software Technology and Theoretical Computer Science. p. 372–383. FSTTCS'04, Springer-Verlag, Berlin, Heidelberg (2004), https://doi.org/10.1007/978-3-540-30538-5_31
- [65] Kempe, J., Regev, O.: 3-Local Hamiltonian is QMA-Complete. Quantum Info. Comput. 3(3), 258–264 (may 2003)
- [66] Kitaev, A.Y., Shen, A.H., Vyalıy, M.N.: Classical and Quantum Computation. American Mathematical Society, USA (2002)
- [67] Knill, E.: Quantum randomness and nondeterminism. arXiv preprint quant-ph/9610012 (1996)
- [68] Kobayashi, H., Matsumoto, K., Yamakami, T.: Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In: ISAAC. vol. 2906, pp. 189–198. Springer (2003)
- [69] Kraus, K., Böhm, A., Dollard, J.D., Wootters, W.H.: States, effects, and operations fundamental notions of quantum theory. Springer Berlin Heidelberg (1983)

- [70] Liu, Y.K., Christandl, M., Verstraete, F.: Quantum Computational Complexity of the N -Representability Problem: QMA Complete. *Phys. Rev. Lett.* 98, 110503 (Mar 2007), <https://link.aps.org/doi/10.1103/PhysRevLett.98.110503>
- [71] Marriott, C., Watrous, J.: Quantum Arthur-Merlin games. In: *Proceedings. 19th IEEE Annual Conference on Computational Complexity*, 2004. pp. 275–285 (2004)
- [72] Metz, C.: White House earmarks new money for A.I. and quantum computing (Feb 2020), <https://www.nytimes.com/2020/02/10/technology/white-house-earmarks-new-money-for-ai-and-quantum-computing.html>
- [73] Nielsen, M.A., Chuang, I.L.: *Quantum computation and quantum information: 10th anniversary edition*. Cambridge University Press (2010)
- [74] Osborne, T.J.: Hamiltonian complexity. *Reports on Progress in Physics* 75(2), 022001 (Jan 2012), <https://dx.doi.org/10.1088/0034-4885/75/2/022001>
- [75] Planck, M.: Ueber das gesetz der energieverteilung im normalspectrum. *Annalen der Physik* 309(3), 553–563 (1901), <https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19013090310>
- [76] Schrödinger, E., Born, M.: Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society* 31(04), 555 (Oct 1935)
- [77] Shamir, A.: $IP = PSPACE$. *J. ACM* 39(4), 869–877 (oct 1992), <https://doi.org/10.1145/146585.146609>
- [78] Shannon, K., Towe, E., Tonguz, O.K.: On the use of quantum entanglement in secure communications: A survey. *arXiv* (2020)
- [79] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* 26(5), 1484–1509 (1997), <https://doi.org/10.1137/S0097539795293172>
- [80] Simon, D.R.: On the power of quantum computation. *Proceedings 35th Annual Symposium on Foundations of Computer Science* pp. 116–123 (1994)
- [81] Sipser, M.: The History and Status of the P versus NP Question. In: *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*. p. 603–618. STOC '92, Association for Computing Machinery, New York, NY, USA (1992), <https://doi.org/10.1145/129712.129771>
- [82] Tang, C.L.: *Fundamentals of quantum mechanics: for solid state electronics and optics*. Cambridge University Press (Jun 2005)
- [83] Trakhtenbrot, B.: A survey of Russian approaches to perebor (brute-force searches) algorithms. *IEEE Annals of the History of Computing* 6(04), 384–400 (October 1984)
- [84] Valigra, L.: Canada lays the groundwork to become a powerhouse in quantum technology (Jun 2022), <https://sciencebusiness.net/news/canada-lays-groundwork-become-powerhouse-quantum-technology>
- [85] Vidick, T.: A Quantum PCP theorem? (Feb 2013), <https://mycqstate.wordpress.com/2013/02/24/a-quantum-pcp-theorem/>
- [86] Vidick, T., Watrous, J.: Quantum proofs. *Foundations and Trends® in Theoretical Computer Science* 11(1-2), 1–215 (2016), <https://doi.org/10.1561/2F04000000068>
- [87] Von Neumann, J.: *Mathematische grundlagen der quantenmechanik. Die grundlehren der mathematischen wissenschaften in einzeldarstellungen...* bd. XXXVIII, J. Springer (1932), <https://books.google.com/books?id=uqvQAAAAMAAJ>

- [88] Watrous, J.: Succinct quantum proofs for properties of finite groups. pp. 537–546 (2000)
- [89] Watrous, J.: Quantum computational complexity (2008), <https://arxiv.org/abs/0804.3401>
- [90] Watrous, J.: Guest column: An introduction to quantum information and quantum circuits. ACM SIGACT News 42(2), 52–67 (Jun 2011)
- [91] Watrous, J.: The Theory of Quantum Information. Cambridge University Press (2018)
- [92] Wigderson, A.: Mathematics and Computation: A Theory Revolutionizing Technology and Science. Princeton University Press (2019), <http://www.jstor.org/stable/j.ctvckq7xb>
- [93] de Wolf, R.: Quantum computing: Lecture notes. CoRR abs/1907.09415 (2019), <http://arxiv.org/abs/1907.09415>
- [94] Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature 299(5886), 802–803 (Oct 1982)
- [95] Yamakami, T.: Analysis of quantum functions. International Journal of Foundations of Computer Science 14(05), 815–852 (2003), <https://doi.org/10.1142/S0129054103002047>