

نسخه‌ی کوانتومی NP

علی الماسی*

چکیده. این مقاله 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 آن که 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 سوالاتی 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 نوشته پس از معرفی مدلی برای محاسبات کوانتومی، سیستم‌های اثبات غیرتعاملی کوانتومی را معرفی خواهیم کرد و به بررسی کلاس QMA از هر دو وجه فوق خواهیم پرداخت.

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 کند را می‌توان مربوط به پاول بنیوف دانست [۵۶]. با این وجود، معمولاً از ریچارد فاینمن به عنوان آغازکننده‌ی راه محاسبات کوانتومی یاد می‌شود. در حقیقت فاینمن در [۵۷]، با توجه به این‌که 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 [۳۸] نشان داد که هر دو مدل قدرت محاسباتی یکسانی 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 الگوریتم‌هایی کوانتومی 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 [۵۸]، 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 تر

^۱ quantum Turing machine

^۲ quantum circuit model

توسعه یافته‌ی چرخ-تورینگ منتج شود، نمایان کرد. سایمون با ارائه‌ی الگوریتمی در [۵۹] نشان داد که محاسبات کوانتومی کارا مشمول در محاسبات زیرنامایی^۱ تصادفی نیست، و گروه در [۶۰] ثابت کرد که مسأله‌ی جست‌وجو را با الگوریتم‌های کوانتومی می‌توان به صورت کارتری حل کرد. گرچه برنشتاین و وزیرانی در [۵۸] 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 الگوریتم‌های کارایی است که شور در [۶۱] 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 RSA، DH و ECC امکان‌پذیر می‌شد.

محاسبات کوانتومی از زمان ارائه‌ی الگوریتم‌های شور تا به امروز، 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 [۶۲]. از سوی دیگر، امروزه به طور نظری بسیاری از حوزه‌های علوم کامپیوتر همتایی 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 [۶۳]. یک نتیجه‌ی توسعه‌ی محاسبات کوانتومی آن است که با پیدا شدن الگوریتم‌های کوانتومی جدید، تنظیم رده‌بندی جدیدی از 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 مقاله تمرکز ما بر مطالعه‌ی سیستم‌های اثبات غیرتعاملی کوانتومی است. سیستم‌های اثبات در پیچیدگی کلاسیک به طور مشروحی مورد مطالعه قرار گرفته‌اند [۶۴، ۶۵، ۶۶]، 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 کیتائف در [۱] آغاز می‌شود. مشابه کلاس NP در پیچیدگی کلاسیک، می‌توان کلاسی از مجموعه‌ی ویژگی‌هایی مانند P تعریف کرد که تصدیق $x \in P$ با اثبات کوانتومی کوتاهی مانند y و با استفاده از الگوریتمی کوانتومی و کارا امکان‌پذیر است. مطالعه‌ی این کلاس، که همتای کوانتومی کلاس NP است، موضوع اصلی این مقاله است.

در جریان بررسی این کلاس، خواهیم دید مسأله‌ی همیلتنی‌های 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 همیلتنی 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 بین نوع خاصی از سیستم‌های اثبات کارا — که به آن‌ها اثبات‌های قابل بررسی احتمالاتی می‌گویند — و سختی یافتن الگوریتم‌های تقریبی کارا برای دسته‌ای از مسائل NP — سخت ارتباط 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 دارد. 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.

۲. مقدمه‌ای بر مکانیک کوانتومی برای علوم کامپیوتردانان

مکانیک کوانتومی، که در ادامه با آن بیشتر آشنا خواهیم شد، چهارچوبی ریاضی است که قواعد ساختن نظریه‌های فیزیکی توصیف‌کننده‌ی پدیده‌های کوانتومی را تعیین می‌کند [۴۵]. پیش از پرداختن به مکانیک کوانتومی، خالی از لطف نیست که مروری بر مکانیک کلاسیک داشته باشیم و سپس مکانیک کوانتومی را در آنالوژی با همتای کلاسیک آن معرفی کنیم.

حکایت مشهور سببی که بر سر نیوتن افتاد و الهام‌بخش او برای تدوین نظریه‌ی گرانشش شد را در نظر بگیرید. سببی که از درخت جدا شده و در حال افتادن بر زمین است، نمونه‌ای از یک سیستم فیزیکی است. برخی ویژگی‌های فیزیکی این سبب طی حرکتش به سمت زمین تغییر می‌کند؛ مثلاً سرعت، ارتفاع آن از سطح زمین، انرژی جنبشی و پتانسیل آن. از سوی دیگر،

^۱subexponential

برخی ویژگی‌های فیزیکی سیب نیز در طول این حرکت، ثابت باقی می‌ماند؛ برای مثال جرم سیب از جمله‌ی این ویژگی‌هاست. به خواص فیزیکی نوع اول، خواص پویا، و به خواص نوع دوم، خواص ایستا می‌گوییم [۴۹].

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، روشی 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 سیبی که از درخت افتاده است، می‌خواهیم رابطه‌ی بین ارتفاع اولیه‌ی سیب و سرعت آن را در هنگام برخورد به زمین 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؟».

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 (سیب 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

$$F = m \frac{d^2 x}{dt^2} \quad (۱.۲)$$

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 است. 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 ۱.۲ را نیز به صورت برداری بازنویسی کنیم.

توجه کنید که اصول موضوعه‌ی مکانیک کوانتومی نیز، در روند مشابهی با آنچه درباره‌ی 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.

۱.۲. 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 آن زمان دانست. معرفی مفهوم بسته‌های انرژی توسط مکس پلانک [۵۰] که بعدها اینشتین آن را توسعه داد و اثر فوتوالکتریک را به کمک این مفهوم توضیح داد [۵۱]، معرفی مدل اتمی بور برای توصیف طیف اتم هیدروژن [۵۲]، توسعه‌ی مکانیک ماتریسی توسط هایزنبرگ و توابع موج توسط شرودینگر برای توصیف ریاضی پدیده‌های کوانتومی و ارائه‌ی اصول موضوعه‌ی مکانیک کوانتومی توسط فون نویمان [۵۳] از جمله مهم‌ترین گام‌هایی است که در سه دهه‌ی اول قرن بیستم برداشته و منجر به ساخته شدن این نظریه‌ی ارزشمند، و البته غامض، شده‌اند. نظریه‌ای که تاثیرات 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، دراصلی که مشابه آن در مکانیک کلاسیک وجود ندارد، خواهیم دید که اندازه‌گیری یک سیستم کوانتومی — یکی از مفاهیم مناقشه‌برانگیز فیزیک کوانتوم — چگونه صورت‌بندی می‌شود.

در ادامه‌ی این نوشته، همه‌ی فضاهای برداری روی میدان مختلط تعریف شده‌اند، مگر خلاف آن ذکر شود. ما برای نمایش بردارها از نمادگذاری خاصی موسوم به نمادگذاری دیراک استفاده می‌کنیم. در نمادگذاری دیراک، هر بردار مانند $v \in V \cong \mathbb{C}^n$ را که برداری ستونی و $n \times 1$ است، با $|v\rangle$ و ترانهاده و مزدوج این بردار را با $\langle v|$ نمایش می‌دهیم. به این ترتیب ضرب داخلی دو بردار v و w برابر با حاصل ضرب ماتریسی $\langle v|$ و $|w\rangle$ خواهد بود که به اختصار به صورت $\langle v|w\rangle$ نمایش داده می‌شود. هم‌چنین در ادامه از مفهوم ضرب تنسوری به کرات استفاده خواهیم کرد. چنان‌چه با این ضرب آشنایی ندارید، می‌توانید این‌طور به آن فکر کنید:

ضرب تنسوری 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:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}. \quad (2.2)$$

ضرب تنسوری دو فضای برداری را نیز می‌توان با گسترش خطی ضرب فوق روی فضاها تعریف کرد. با این مقدمه، اکنون آماده‌ی ارائه‌ی اصول مکانیک کوانتومی هستیم.

اصل ۱.۲ (فضای حالت). به هر سیستم فیزیکی منزوی یک فضای هیلبرت^۱ نسبت داده می‌شود که به آن فضای حالت سیستم^۲ می‌گویند. بردار حالت^۳ سیستم (یا به طور خلاصه، حالت سیستم)، بردار یکه‌ای در فضای حالت آن است [۴۵].

تعریف ۲.۲. یک کیوبیت^۴، یک سیستم کوانتومی است که فضای حالت آن، فضای هیلبرت دو بعدی \mathbb{C}^2 است.

کیوبیت‌ها —همتای کوانتومی بیت‌های کلاسیک— اساسی‌ترین و ضروری‌ترین سیستم‌هایی هستند که در محاسبات و اطلاعات کوانتومی به کار گرفته می‌شوند. حالت یک کیوبیت می‌تواند به صورت

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (3.2)$$

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 ۳.۲) در یک برهم‌نهی^۵ از $|0\rangle$ و $|1\rangle$ قرار گیرد. این یکی از تفاوت‌های اساسی میان محاسبات کلاسیک و محاسبات کوانتومی است.

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 ۳.۲. 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 $\{|0\rangle, |1\rangle\}$ پایه‌ی محاسباتی یا \mathbb{C}^2 پایه‌ی Z نامیده می‌شود.

اصل ۴.۲ (تحول سیستم). این اصل را می‌توان به دو صورت متفاوت بیان کرد، و البته می‌توان نشان داد که این دو صورت با یکدیگر معادلند [۴۵]:

^۱ یک فضای هیلبرت، فضایی برداری مجهز به یک ضرب داخلی است که نسبت به نرم القاشده توسط آن ضرب داخلی کامل است، به این معنی که هر دنباله‌ی کوشی در آن همگراست. در این مقاله خود را به فضاهای هیلبرت متناهی‌البعد محدود می‌کنیم که می‌توان نشان داد با \mathbb{C}^n یکریخت هستند.

^۲ State Space

^۳ State Vector

^۴ Qubit

^۵ Superposition

- 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^۱ 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.

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. تعدادی از این گیت‌ها و نمایش گرافیکی و ماتریسی آن‌ها در مثال بعد معرفی شده‌اند.


مثال ۵.۲. گیت‌های زیر از پرکاربردترین گیت‌ها در مدارهای کوانتومی هستند.

- (۱) گیت Pauli-I با نمایش ماتریسی $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ و نمایش گرافیکی \boxed{I} .
- (۲) گیت Pauli-X با نمایش ماتریسی $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ و نمایش گرافیکی \boxed{X} .
- (۳) گیت Pauli-Z با نمایش ماتریسی $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ و نمایش گرافیکی \boxed{Z} .
- (۴) گیت Hadamard با نمایش ماتریسی $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$ و نمایش گرافیکی \boxed{H} .
- (۵) گیت T با نمایش ماتریسی $\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$ و نمایش گرافیکی \boxed{T} .

اصل ۶.۲ (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 [۴۵].

با توجه به اصول ۴.۲ و ۶.۲، تحول زمانی یک سیستم مرکب کوانتومی که متشکل از دو زیرسیستم با فضاهای حالت V و W است، با نگاشت‌های یکانی روی فضای $V \otimes W$ مشخص می‌شود. توجه کنید که زیرمجموعه‌ای از چنین نگاشت‌هایی، به صورت $L \otimes L'$ هستند، که L و L' به ترتیب نگاشت‌هایی یکانی روی فضاهای V و W هستند. با این وجود، باید توجه شود که این زیرمجموعه، زیرمجموعه‌ای سره از همه‌ی نگاشت‌های 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 نابدیهی عمل می‌کنند. یکی از مهم‌ترین این گیت‌ها، گیت CNOT است که روی دو کیوبیت عمل می‌کند. نمایش ماتریسی این

گیت به صورت $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ و نمایش گرافیکی آن به صورت  است.

^۱ Hamiltonian

اصل ۷.۲ (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 $\sum_{i=1}^m M_i^\dagger M_i = \mathbb{I}_n$ 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^۱ [۴۵].

توجه کنید که اندازه‌گیری راهی برای استخراج اطلاعات کلاسیک از یک سیستم کوانتومی است. با این حال، اصل فوق نشان می‌دهد که استخراج اطلاعات کلاسیک از یک سیستم کوانتومی اولاً ذاتی تصادفی و غیرقطعی دارد، و ثانیاً ضرورتاً منجر به تغییر حالت سیستم می‌شود، و این امری است که افتراقی اساسی میان فیزیک کلاسیک و فیزیک کوانتوم ایجاد می‌کند. در ادامه‌ی این نوشته، عموماً از حالت خاصی از اندازه‌گیری‌های معرفی‌شده در اصل ۷.۲ بهره خواهیم گرفت که در ادامه معرفی می‌شوند.

تعریف ۸.۲. یک اندازه‌گیری افکنشی یک اندازه‌گیری کوانتومی است که متشکل است از عملگرهای افکنشی دو به دو متعامد. یک عملگر افکنشی عملگری هریمیتی 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.

$$\sum_{i=1}^m P_i = \mathbb{I}_n \quad (۲)$$

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

همچنین ممکن است در ادامه‌ی این مقاله، 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.

نمادگذاری ۹.۲. در ادامه از نماد زیر برای نمایش گرافیکی اندازه‌گیری استفاده خواهیم کرد.



۲.۲. قضیه‌ی عدم امکان شبیه‌سازی و درهم‌تنیدگی. 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، امکان‌ناپذیری شبیه‌سازی^۲ یک حالت دلخواه کوانتومی است که نخستین بار در [۵۴] و [۵۵] بیان شد. این قضیه بیان می‌کند که اگر یک نگاهت 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 برهم 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 نمی‌توان از روی یک پیام کوانتومی دلخواه 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 سخت‌تر و نیازمند خلاقیت بیشتر است.

¹ Collapse

² No-cloning Theorem

مفهوم دوم، مفهوم ساده و در عین حال مهمی به نام درهم‌تنیدگی^۱ است.

تعریف ۱۰.۲. 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.) درهم‌تنیده می‌گوییم، هرگاه هیچ دو برداری مانند $|\phi_1\rangle \in \mathbb{C}^n$ و $|\phi_2\rangle \in \mathbb{C}^m$ وجود نداشته باشند چنان‌که

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

اگر یک حالت کوانتومی درهم‌تنیده نباشد، به آن جداشدنی یا ضری می‌گوییم.

مثال ۱۱.۲. حالت‌های زیر که به حالت‌های بل^۲ یا زوج‌های EPR^۳ مشهورند، نمونه‌ای از حالت‌های درهم‌تنیده‌اند.

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \left(\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}}\right)^t \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle = \left(\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad -\frac{1}{\sqrt{2}}\right)^t \end{aligned}$$

این بخش را با ذکر این نکته به پایان می‌رسانیم که درهم‌تنیدگی کوانتومی، همان‌گونه که شرویدنگر گفته است، «ویژگی بارز مکانیک کوانتومی است؛ آن چیزی که ماهیت آن را تماماً از خطوط فکری کلاسیک جدا می‌کند [۶۸]». تا به امروز 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 [۶۹].

۳. مدل محاسبات مداری کوانتومی

در این فصل به معرفی الگوریتم‌های کوانتومی و کلاس‌های مسائلی قابل حل با الگوریتم‌های کوانتومی کارا خواهیم پرداخت. پیش از آن‌که 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 [۳۲] 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 مجموعه‌ی $\{0, 1\}$ است.) که گذشته‌ی پیکربندی ماشین محاسبه در هر لحظه هستند. قانون انتقال حالت این سیستم دینامیکی، به این صورت است که در گذر هر لحظه، رشته‌ای که متناظر با حالت فعلی سیستم است را به طور موضعی 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^۴. با چنین فرمالیسمی، محاسبه‌ی یک ورودی توسط یک ماشین محاسبه، در واقع معادل با یک مسیر^۵ 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 اندازه‌گیری ما در

^۱Entanglement

^۲Bell States

^۳EPR Pairs

^۴این فرض چندان دور از ذهن نیست. به عنوان مثال، سیستم دینامیکی متناظر با یک مدار محاسبه روی n بیت، مثالی از چنین سیستمی است.

^۵trajectory

پایه‌ی محاسباتی است. در این صورت نتیجه‌ی اندازه‌گیری به صورت کاملاً تصادفی یکی از رشته‌های $x \in \{0, 1\}^n$ 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 موضعاً نابديهی یکانی بر بردار اولیه‌ای واقع در کروی واحد فضای \mathbb{C}^{2^n} که در پایان الگوریتم، با استفاده از اندازه‌گیری، به یک بردار توزیع احتمال تبدیل می‌شود.

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 چالش برانگیز 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 [۳۸].

۱.۳. الگوریتم‌های کوانتومی.

تعریف ۱.۳. یک گیت کوانتومی k موضعی روی یک رجیستر n -کیوبیتی، نگاشتی یکانی است که به طور نابديهی 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 $(i_1, i_2, \dots, i_k) \in [n]^k$ 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:

• اگر $k = 1$:

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

• 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 پانویس (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:

$$U = U_{\alpha_1}^1 U_{\alpha_2}^2 \dots U_{\alpha_s}^s,$$

که در آن $U_{\alpha_i}^i$ ها گیت‌های کوانتومی k_i موضعی روی n کیوبیت هستند که از روی نگاشت‌های $U^i \in B$ ساخته شده‌اند، و $\alpha_i \in [n]^{k_i}$ 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 [۳۹]. ما تا به این جا 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 رهنمون خواهند کرد که هر یک می‌توانند مبنای ساختن نظریه‌ای برای پیچیدگی محاسبات کوانتومی قرار گیرند.

ملاحظه ۳.۳. الگوریتم‌های کوانتومی را می‌توان به طرق مختلفی تعریف کرد. در ادامه، مطابق با مرجع [۴۰] 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^۱

با فرض این که تابعی جزئی مانند $f: \{0, 1\}^n \rightarrow \{0, 1\}^m$ 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 کوثری کوانتومی^۲

فرض کنید به عنوان ورودی مسأله جعبه‌سیاهی به ما داده شده است که تابعی مانند $f: \{0, 1\}^n \rightarrow \{0, 1\}^m$ را پیاده‌سازی می‌کند، و از ما خواسته شده است که اطلاعاتی درباره‌ی این تابع را با کوثری کردن از این جعبه‌سیاه (یا اوراکل) به دست آوریم. برای پرسیدن کوثری 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 براساس نتایج اندازه‌گیری، اطلاعات مورد نظر درباره‌ی تابع f به دست می‌آید. در این الگوریتم‌ها منبع محاسباتی مورد نظر جهت اندازه‌گیری پیچیدگی محاسباتی، تعداد کوثری‌ها (یا تعداد f -گیت‌های استفاده شده در مدار) است.

(۳) سناریوی سوم: پیچیدگی ارتباطی کوانتومی^۳

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 بفرستد) 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.

هدف این نوشته مطالعه‌ی کلاس‌های پیچیدگی‌ای است که در سناریوی پیچیدگی محاسباتی کوانتومی مورد مطالعه قرار می‌گیرند.

۲.۳. 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 فقط شامل گیت‌هایی از این مجموعه‌ها پیاده‌سازی کرد. مثلاً می‌توان نشان داد که برای محاسبات برگشت‌پذیر، مجموعه‌ی $\{\theta_3\}$ که در آن θ_3 گیت توفولی است، یکی از این مجموعه‌ها است، و نیز می‌توان نشان داد که هیچ مجموعه‌ای از گیت‌های ۱ و ۲ بیتی وجود ندارد که مجموعه‌ای جهانی برای محاسبات برگشت‌پذیر کلاسیک 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؛ 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 تعدادی

^۱ quantum computational complexity

^۲ quantum query complexity

^۳ quantum communication complexity

متناهی 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 ۴.۳. مجموعه‌ای از گیت‌های کوانتومی مانند \mathcal{G} به طور دقیق جهانی است هرگاه 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 نابدیهی عمل کنند 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، مجموعه‌هایی 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 [۴۱] 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 «تقریب زدن» چیست. برای آن‌که بتوانیم گیتی را تقریب بزنیم، 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 ۵.۳. p -نرم شاتن یک عملگر $T \in \mathcal{L}(\mathbb{C}^d)$ ، که در آن $p \in [1, \infty)$ ، به صورت زیر:

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

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^۱ و نرم طیفی^۲ گفته می‌شود.

حال به تعریف مفهوم جهانی بودن به طور تقریبی می‌پردازیم.

تعریف ۶.۳. 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 ۷.۳. هر یک از مجموعه‌های زیر از گیت‌های کوانتومی، به طور تقریبی جهانی هستند:

- گیت دویچ [۴۳]
- گیت بارنکو [۴۴]
- $\{H, T, \text{CNOT}\}$ [۴۵]
- تقریباً هر گیت کوانتومی که روی حداقل ۲ کیوبیت اثر می‌کند [۴۶]. (به این معنی که گیت‌هایی که جهانی نیستند، مجموعه‌ای اندازه صفر را مشخص می‌کنند.)

^۱trace norm

^۲spectral norm

در خاتمه‌ی این بخش، به پرسش مهم دیگری می‌پردازیم که پاسخ آن در ملاحظات پیچیدگی محاسباتی ما تاثیرگذار است. تا به اینجا دیدیم 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 [۴۵]. با این حال قضیه‌ی 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 ۸.۳ (قضیه‌ی سولووی-کیتائف). فرض کنید G مجموعه‌ای متناهی از گیت‌های کوانتومی ۱ کیوبیتی است که شامل وارون اعضایش نیز هست و گروهی که توسط اعضای G تولید می‌شود 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 G مانند $g_1, g_2, \dots, g_n \in G$ وجود دارد به طوری که $n \in O(\log^c(\frac{1}{\varepsilon}))$ و $\|U - g_1 g_2 \dots g_n\|_1 < \varepsilon$ [۴۷].

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 ۹.۳. فرض کنید $U = U_m U_{m-1} \dots U_1$ و $V = V_m V_{m-1} \dots V_1$ دو مدار کوانتومی باشند به طوری که برای هر $0 \leq i \leq m$ ، $\|U_i - V_i\|_1 < \varepsilon$. در این صورت $\|U - V\|_1 < m\varepsilon$.

لم ۹.۳، همراه با قضیه‌ی ۸.۳ نتیجه می‌دهد که اگر مداری کوانتومی مانند U داشته باشیم که از m گیت ۱ کیوبیتی کوانتومی ساخته شده است، می‌توان آن را به مداری مانند U' تبدیل کرد؛ چنان‌که مدار اخیر تنها از گیت‌های جهانی ساخته شده است؛ U' در ε -همسایگی U قرار دارد، و افزون بر این اندازه‌ی مدار اخیر $O(m \log^c(\frac{m}{\varepsilon}))$ است.

۳.۳. 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 [۴۸]. گرچه انتخاب چندجمله‌ای‌ها برای این منظور تا حدی دلخواه به نظر می‌رسد، این انتخاب در طول سالیان از نقطه‌ی نظرهای مختلفی تایید شده است؛ 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 تز چرچ-تورینگ می‌توان دید:

«هر چیز که به صورت کارایی محاسبه‌پذیر باشد، با یک ماشین تورینگ احتمالاتی در زمان چندجمله‌ای

قابل محاسبه است [۳۲].»

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 [۱۹]. با این وجود، اگر محاسبات کارا در مدل مداری را به عنوان وجود مداری با اندازه‌ی چندجمله‌ای برای یک مسأله تعبیر کنیم، 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 روش برای چنین کاری را بیان می‌کنیم.

اگرچه 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 ۱۰.۳. 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 مناسب‌تری 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 مسأله‌های قراردادی برتری یافته است. یک مسأله‌ی قراردادی^۱ عبارت است از زوج مرتبی مانند $\Pi = (\Pi_{Yes}, \Pi_{No})$ ، به طوری که $\Pi_{Yes} \cap \Pi_{No} = \emptyset$ و $\Pi_{Yes} \cup \Pi_{No} \subseteq \{0, 1\}^*$ ، در حالتی که ورودی مسأله عضو $\Pi_{Yes} \cup \Pi_{No}$ باشد، می‌گوییم ورودی قرارداد مسأله را برآورده می‌کند. روشن است که اگر $\Pi, \Pi_{Yes} \cup \Pi_{No} = \{0, 1\}^*$ یک مسأله‌ی تصمیم‌گیری خواهد بود.

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 $\Pi_{Yes} \cup \Pi_{No}$ نباشد، الگوریتم می‌تواند دلخواه باشد. حل کردن یک مسأله‌ی قراردادی را می‌توان در ساختار حل‌پذیری تصادفی نیز، کاملاً 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.

گرچه در پیچیدگی کلاسیک رایج است که اگر کلاسی مانند C بر اساس مسأله‌های قراردادی تعریف شده باشد، از آن به عنوان PromiseC 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 خلاف آن ذکر شود.

تعریف ۱۱.۳. 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، چنان که:

(۱) برای هر ورودی $x \in \{0, 1\}^n$ ، حالت $C_n, x \in \{0, 1\}^n$ را $|x\rangle_{in} |0\rangle_{an}^{\otimes q(n)}$ و پس از اعمال شدن آن، یک کیوبیت

خاص (مثلاً اولین کیوبیت رجیستر an) در پایه‌ی محاسباتی اندازه‌گیری می‌شود. فرض کنید حاصل اندازه‌گیری

$b \in \{0, 1\}$ باشد. در این صورت،

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

(۳) اگر $x \in \Pi_{No}$ ، آنگاه $\Pr[b = 1] \leq \frac{1}{3}$.

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 سولوی-کیتائف می‌توان نتیجه گرفت که انتخاب مجموعه‌های جهانی متفاوت، در حد یک سربار چندجمله‌ای در ساین مدار 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 $\{H, T, \text{CNOT}\}$ هستند.

^۱promise problem

ملاحظه ۱۲.۳. مانند بسیاری دیگر از کلاس‌های پیچیدگی تصادفی، کران‌های ظاهر شده در تعریف ۱۱.۳ را می‌توان در حد وارون نمایی کاهش داد. برای نشان‌دادن 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 معرفی‌شده در تعریف ۱۱.۳ منجر خواهد شد.

۴. اثبات‌های (غیرتعاملی) کوانتومی

۱.۴. کلاس پیچیدگی QMA . همان‌گونه که خواهیم دید، کلاس پیچیدگی QMA تعمیمی طبیعی از کلاس \mathcal{NP} به قلمروی 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 \mathcal{NP} شبیه باشد، یادآور نسخه‌ی کلاسیک احتمالاتی آن، یعنی MA است. از پیچیدگی محاسبات کلاسیک می‌دانیم که کلاس \mathcal{NP} را می‌توان با سیستم‌های اثبات نیز مشخص کرد. در واقع اگر $L \in \mathcal{NP}$ ، 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 این‌جا 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 [۱] معرفی شده است. یادآوری می‌کنیم که همان‌گونه که پیشتر 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 $QMA_p(\frac{1}{4}, \frac{1}{4})$ عبارت است از تمام مسئله‌های 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 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، چنان‌که:

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

(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 $\Pr[b = 1] \geq \frac{3}{4}$.

(۳) درستی: اگر $x \in \Pi_{No}$ ، در این صورت برای هر اثبات $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ ، $\Pr[b = 1] \leq \frac{1}{4}$.

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، $QMA(\frac{1}{4}, \frac{3}{4})$ را معمولاً به اختصار با QMA نشان می‌دهیم.

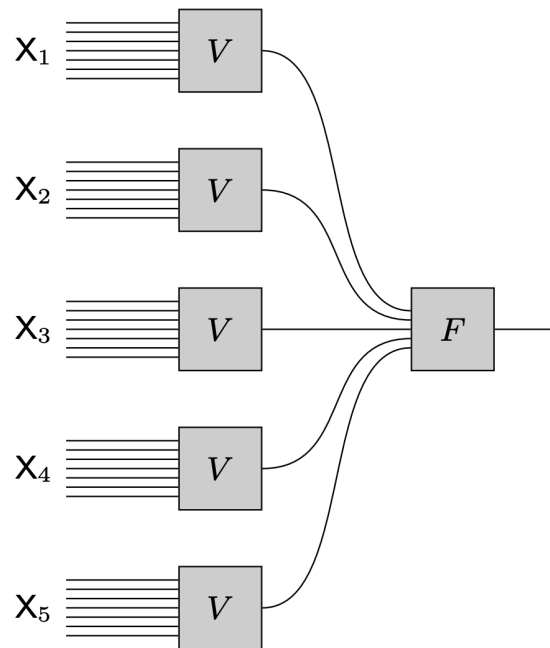
همان‌گونه که از تعریف بالا بر می‌آید، در تعریف کلاس QMA ، روی (توزیع) خروجی مدار در حالتی که ورودی x رشته‌ای عضو $\Pi_{Yes} \cup \Pi_{No}$ نیست، شرطی نداریم و در چنین حالتی، خروجی می‌تواند دلخواه باشد.

ملاحظه ۲.۴. QMA سرواژه‌ای برای کوانتوم مرلین-آرتور^۱ است و بیان می‌کند که کلاس فوق همتای کوانتومی کلاس پیچیدگی مرلین-آرتور (MA) است. این نام‌گذاری اولین بار در [۲] به کار رفت و به تدریج جایگزین $BQNP$ ، نامی که [۱] نخستین بار برای این کلاس به کار برده بود، شد.

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 $\frac{1}{4}$ روی احتمال خطا را می‌توان کاهش داد یا نه. می‌دانیم کاهش

^۱Quantum Merlin-Arthur

شکل ۱: کاهش خطای موازی، تصویر برگرفته شده از مرجع [۳] است.



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 کند 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^۱ یا کاهش خطای ضعیف^۲ می‌گویند. در این روش، مرلین یک اثبات $|\psi'\rangle \in (\mathbb{C}^2)^{\otimes kp(n)}$ را برای آرتور ارسال می‌کند و آرتور باید 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 $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ وجود دارد که تصدیق‌کننده با احتمال حداقل $\frac{2}{3}$ آن را می‌پذیرد. در این حالت، مرلین کافی است k نسخه از این اثبات را به صورت $|\psi'\rangle = |\psi\rangle \otimes \dots \otimes |\psi\rangle \in (\mathbb{C}^2)^{kp(n)}$ برای آرتور بفرستد و آرتور مطابق شکل ۱ 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 پذیرفته‌شدن اثبات توسط آرتور کراندار باشد. در این حالت، ممکن است مرلین اثباتی درهم‌تنیده برای آرتور ارسال کند. به این ترتیب اگر آرتور مطابق شکل ۱ عمل کند، حالت رجیسترهای مختلف اثبات لزوماً حالت خالص^۳ نخواهد ماند و ممکن است به دلیل درهم‌تنیدگی، رجیستری از اثبات در حالت مخلوط قرار گیرد.

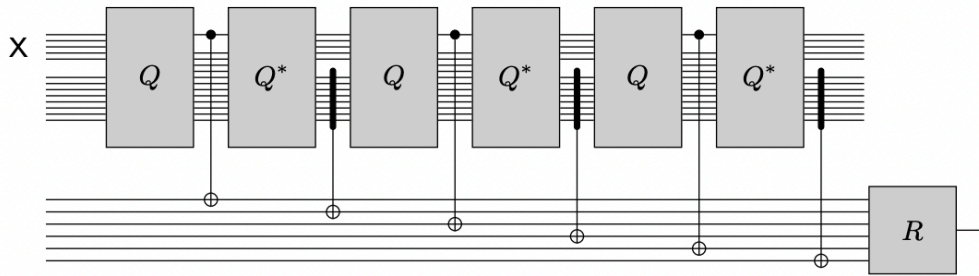
با این حال به سادگی می‌توان دید که اگر برای هر اثبات $|\psi\rangle$ در حالت خالص، بدانیم آرتور آن را با احتمال حداکثر

^۱ Parallel Error Reduction

^۲ Weak Error Reduction

^۳ فرض کنید مجموعه‌ای از حالت‌ها مانند $\{|\psi_1\rangle, \dots, |\psi_n\rangle\}$ داریم که روی آن‌ها توزیع احتمالی مانند p_1, \dots, p_n وجود دارد. اگر بدانیم دقیقاً یکی از p_i ها برابر با ۱ و مابقی برابر صفرند، به حالت این هنگام حالت خالص و در غیر این صورت، حالت مخلوط گفته می‌شود. حالت‌های مخلوط را می‌توان با کمک فرمول‌بندی ماتریس‌های چگالی مطالعه کرد. خواننده‌ی علاقه‌مند می‌تواند برای مطالعه‌ی بیشتر درباره‌ی حالت‌های مخلوط به [۴۵] مراجعه کند.

شکل ۲: کاهش خطای حافظ اثبات، تصویر برگرفته شده از مرجع [۲] است.



می‌پذیرد، در این صورت برای هر اثبات با حالت مخلوط ρ نیز احتمال پذیرفته‌شدن 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 [۴]:

$$\mathcal{QMA}(c - \frac{1}{p(n)}, c) \subseteq \mathcal{QMA}(\frac{1}{p}, \frac{2}{p}) = \mathcal{QMA}(\frac{1}{p(n)}, 1 - \frac{1}{p(n)}).$$

• اندازه‌ی اثبات در این روش افزایش یافته است. آیا این افزایش طول اثبات غیرقابل اجتناب است؟ در واقع، این افزایش طول اثبات ضروری نیست. [۵] روشی هوشمندانه موسوم به کاهش خطای حافظ اثبات یا کاهش خطای قوی (شکل ۲) ارائه کرده است که در نتیجه‌ی آن 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 تعدادی متناهی از اعداد طبیعی)،

$$a(n) - b(n) \geq \frac{1}{q(n)}. \quad (1.4)$$

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:

$$\mathcal{QMA}_p(a, b) = \mathcal{QMA}_p(1 - 2^{-r}, 2^{-r}). \quad (2.4)$$

مسئله‌ی دیگری که پس از تعریف کلاس \mathcal{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 \mathcal{MA} و \mathcal{BQP} ، هر دو، کران‌های پایینی برای \mathcal{QMA} هستند (زیرا محاسبات کلاسیک را می‌توان با محاسبات کوانتومی شبیه‌سازی کرد). در ادامه، کران‌های بالایی را نیز برای \mathcal{QMA} خواهیم یافت.

(۱) به سادگی می‌توان نشان داد که $\mathcal{QMA} \subseteq \mathcal{NEXP}$. فرض کنید که Π مسئله‌ای در \mathcal{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 تصدیق‌کننده‌ی آرتور خروجی ۱ بدهد را محاسبه می‌کند و با توجه به مقدار این احتمال، اثبات را می‌پذیرد یا رد می‌کند. محاسبه‌ی این احتمال در زمان نمایی بر حسب n ممکن است. بنابراین ماشین توصیف‌شده در بالا، ماشینی غیرقطعی با زمان نمایی است، که نتیجه می‌دهد مسئله‌ی مورد نظر عضو کلاس \mathcal{NEXP} است.

(۲) به عنوان کران بالایی نابديهی‌تر از \mathcal{NEXP} ، می‌توان 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 می‌دهیم) به ازای اثبات $|\psi\rangle$

خروجی ۱ بدهد برابر است با^۱:

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

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 می‌دانیم که

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

بنابراین، برای حل یک مسأله‌ی 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 ویژه‌ی عملگر خطی P_x را محاسبه کنیم. روشن است که ابعاد P_x بر حسب n نمایی است. با این وجود، پیدا کردن مقدار ویژه‌های یک ماتریس، در زمان چندجمله‌ای بر حسب ابعاد آن امکان‌پذیر است. در نتیجه، هر مسأله‌ی \mathcal{QMA} را می‌توان با ماشینی قطعی در زمان نمایی حل کرد.

(۳) با استفاده از کاهش خطای قوی می‌توان نشان داد $\mathcal{QMA} \subseteq \mathcal{PP}$ [۵]. برای هر چندجمله‌ای دلخواه p و هر مسأله‌ی قراردادی دلخواه در \mathcal{QMA}_p مانند $\Pi = (\Pi_{Yes}, \Pi_{No})$ ، از قضیه‌ی ۴.۴ می‌دانیم:

$$\Pi \in \mathcal{QMA}_p(1 - 2^{-(p(n)+2)}, 2^{-(p(n)+2)})$$

حال الگوریتمی کوانتومی را در نظر بگیرید که برای یک ورودی دلخواه با طول n ، اثباتی را به تصادف از بین همه‌ی اثبات‌های با طول $p(n)$ انتخاب می‌کند، و آن را در رجیستر اثبات مدار تصدیق‌کننده‌ی مسأله‌ی Π قرار می‌دهد و الگوریتم تصدیق‌کننده را اجرا می‌کند. احتمال این که این الگوریتم خروجی ۱ دهد برابر است با:

$$\text{tr}(P_x \frac{\mathbb{I}}{2^{p(n)}}) = \frac{1}{2^{p(n)}} \text{tr}(P_x).$$

- در حالتی که $x \in \Pi_{Yes}$ ، $\frac{1}{2^{p(n)}} \text{tr}(P_x) \geq \frac{1}{2^{p(n)+1}}(1 - \frac{1}{2^{p(n)+2}}) \geq \frac{1}{2^{p(n)+1}}$
- در حالتی که $x \in \Pi_{No}$ ، $\frac{1}{2^{p(n)}} \text{tr}(P_x) \leq \frac{1}{2^{p(n)+2}}$

با توجه به فاصله‌ی بین ضرایب درستی و تمامیت در بالا، می‌توان دید که فاصله‌ی مورد نظر در تعریف کلاس \mathcal{PP} برآورده می‌شود. 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 کرده‌ایم نشان می‌دهد که Π عضو کلاس \mathcal{PQP} است؛ کلاسی که همتای کوانتومی \mathcal{PP} محسوب می‌شود. با این همه، یاماکامی در [۶] نشان داده است که $\mathcal{PQP} = \mathcal{PP}$ ، و به این ترتیب اثبات تکمیل خواهد شد.

۲.۴. نسخه‌هایی دیگر از \mathcal{QMA} . در این بخش به معرفی نسخه‌هایی تغییر یافته از کلاس \mathcal{QMA} می‌پردازیم و برخی ویژگی‌های اثبات‌شده و حدس‌های اثبات‌نشده را در ارتباط با این کلاس‌ها مرور خواهیم کرد.

• \mathcal{QMA} با اثبات‌های کلاسیک (\mathcal{QCMA}):

اگر در تعریف کلاس \mathcal{QMA} فرض کنیم اثباتی که توسط مرلین ارسال می‌شود یک رشته‌ی کلاسیک است، کلاس \mathcal{QCMA} به دست می‌آید. روشن است که $\mathcal{QCMA} \subseteq \mathcal{QMA}$. با این حال، این مسأله که آیا این شمول اکید است یا نه، مسأله‌ای باز است. آرانسون و کوپربرگ در [۷] نشان داده‌اند که یک اوراکل کوانتومی \mathcal{O} وجود دارد که

^۱ در این جا فرض کرده‌ایم که مقدار بیت خروجی با اندازه‌گیری اولین کیوبیت تعیین می‌شود.

$QMA^O \neq QCMA^O$. 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 [۸] اوراکلی کوانتومی مانند O ارائه می‌دهد که $QMA^O \neq QMA_1^O$.

ملاحظه ۵.۴. با وجود این که پرسش $QMA \stackrel{?}{=} QMA_1$ بدون پاسخ مانده است، سوالی مشابه، $QCMA \stackrel{?}{=} QCMA_1$ ، توسط کوبایاشی و همکاران در [۹] پاسخ داده شده است و می‌دانیم $QCMA$ با $QCMA_1$ با خطای یک‌طرفه برابر است. به این ترتیب، بلافاصله می‌توان نتیجه گرفت که $QCMA \subseteq QMA_1$.

• QMA با k مرلین $(QMA(k))$: اگر در تعریف کلاس QMA ، این تغییر را ایجاد کنیم که اثبات به صورت حاصل ضرب تنسوری k حالت $p(n)$ کیوبیتی باشد، در این صورت کلاس پیچیدگی $QMA(k)$ به دست می‌آید. این کلاس نخستین بار توسط کوبایاشی و همکاران در [۱۰] معرفی شد.

می‌توان درباره‌ی این کلاس چنین اندیشید که مجموعه‌ی تمام مسائلی است که می‌توان آن‌ها را با سیستم‌های اثبات غیرتعاملی با چند اثبات‌کننده مشخص کرد، به طوری که اثبات‌کننده‌ها نیز با یکدیگر تعاملی ندارند (جداپذیر بودن اثبات را می‌توان چنین تعبیر 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 نتیجه‌ای 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 [۱۱] مسأله‌ای به نام N -نمایش‌پذیری حالت خالص^۱ 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. هرو و موتانارو در [۱۲] 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 همتای کوانتومی 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 [۱۳] نشان داده‌اند، $StoqMA \subseteq AM \subseteq PH$. 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 [۱۴] نشان داده‌اند که امکان کاهش خطای $StoqMA$ از

^۱ pure state N -Representability

$\mathcal{O}(1)$ به $1 - o(\frac{1}{\text{poly}(n)})$ نتیجه خواهد داد که $\text{StoqMA} = \text{MA}$. با این حال، هنوز مشخص نیست که آیا این نتیجه در تعیین تکلیف کاهش خطای ضعیف برای این کلاس تأثیری خواهد داشت یا نه.

۵. پیچیدگی همیلتنی کوانتومی

مطالعه‌ی رفتار سیستم‌های فیزیکی متشکل از تعدادی ذره 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^۱ 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 [۱۵]. 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 خواهد بود که «شبیه‌سازی یک سیستم فیزیکی تا چه اندازه سخت است؟». 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^۲ 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 شبکه‌ی 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^۳، مدل هاینبرگ 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 S ، تابعی مانند $\mathcal{E} : S \rightarrow \mathbb{R}$ 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 شبکه 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 این مدل‌سازی 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 احتمالی که روی این سطوح انرژی وجود دارد، حاصل اندازه‌گیری یکی از این ویژه‌مقادیر خواهد بود. به چنین مشاهده‌پذیرهایی همیلتنی

¹ many body theory

² quantum Hamiltonian complexity

³ Ising model

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 σ_i^x و σ_i^z عملگرهای پاولی X و Z هستند، و g بیانگر بزرگی میدان مغناطیسی است [۱۶].

در بین 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 ۴.۲ 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 [۱۵]. با مقدمه‌ی بالا، در ادامه‌ی این بخش 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^۱ 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 نابديهی عمل می‌کند. مقادیر ویژه‌ی H ، سطوح انرژی^۲ 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^۳ نام دارد. همچنین به بردار ویژه‌ی متناظر با $\lambda_{\min}(H)$ حالت پایه‌ی^۴ سیستم گوییم.

ملاحظه 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:

$$\lambda_{\min}(H) = \min_{|\psi\rangle} \langle \psi | H | \psi \rangle. \quad (۱.۵)$$

تعریف ۳.۵ (مسأله‌ی همیلتنی k موضعی). فرض کنید $p : \mathbb{N} \rightarrow \mathbb{R}^+$ یک چندجمله‌ای باشد. مسأله‌ی همیلتنی k موضعی با فاصله‌ی قراردادی $p(n)$ (k -LH)، مسأله‌ای قراردادی است که به صورت زیر تعریف می‌شود [۱]:

• ورودی: توصیفی از یک همیلتنی k موضعی ($k \in \mathcal{O}(1)$) $H = \sum_i H^{(i)}$ که بر روی n کیوبیت عمل می‌کند و

توابع به طور موثر محاسبه‌پذیر $\alpha(n), \beta(n)$ به طوری که $\beta(n) - \alpha(n) \geq \frac{1}{p(n)}$ ^۵.

^۱ k -Local Hamiltonian

^۲ energy levels

^۳ ground state energy

^۴ ground state

^۵ توجه کنید که این فاصله را می‌توان به یک عدد ثابت افزایش داد؛ کافی است هر جمله در H را $p(n)$ بار تکرار کنیم [۱۶].

• 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.
- در ادامه این که این مسأله بر حسب p پارامتریزه شده است را به طور ضمنی فرض می‌کنیم و از نوشتن آن خودداری خواهیم کرد.
- 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. به این ترتیب نتیجه خواهیم گرفت که ۳-LH مسأله‌ای سخت برای کلاس \mathcal{NP} است.
- قضیه ۴.۵

$$3\text{-SAT} \leq_m^p 3\text{-LH}. \quad (2.5)$$

اثبات. می‌دانیم هر فرمول ۳-CNF فرمولی مانند $\varphi(x_1, \dots, x_n) = \bigwedge_i c_i(x_{i_1}, x_{i_2}, x_{i_3})$ 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 $H_{i_1, i_2, i_3}^{(i)}$ را به این صورت تعریف کنید:

$$H_{i_1, i_2, i_3}^{(i)} = \sum_{\substack{x \in \{0, 1\}^3 \\ s.t. \ c(x)=0}} |x\rangle \langle x| \quad (3.5)$$

(سمت راست تساوی بالا به صورت مختصر نوشته شده است و باید این گونه تعبیر شود: $H_{i_1, i_2, i_3}^{(i)}$ تنها روی کیویتهای i_1, i_2, i_3 به صورت نابديهی عمل می‌کند و عمل آن روی این سه کیویت نیز مطابق با نگاشت $\sum_{\substack{x \in \{0, 1\}^3 \\ s.t. \ c(x)=0}} |x\rangle \langle x|$ است). حال تعریف کنید $H = \sum_i H_{i_1, i_2, i_3}^{(i)}$. 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 $x \in \{0, 1\}^n$ داریم:

$$\langle x | H | x \rangle = \sum_{x \in \{0, 1\}^n} \langle x | H_{i_1, i_2, i_3}^{(i)} | x \rangle \geq 1. \quad (4.5)$$

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:

$$\langle \psi | H | \psi \rangle = \sum_{x \in \{0, 1\}^n} |\alpha_x|^2 \langle x | H | x \rangle \geq \sum_{x \in \{0, 1\}^n} |\alpha_x|^2 = 1 \quad (5.5)$$

□

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

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 لئوید لوین [۱۷] و استفن کوک [۱۸] 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 پاسخ دادن 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 در شاخه‌های دیگری از علم نیز 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 نیز این مسأله برای کلاس QMA مسأله‌ای سخت است. اثبات مورد اول نسبتاً ساده است و نخست به آن می‌پردازیم.

قضیه ۵.۵. برای هر $k \in O(\log n)$ و هر پارامتر چندجمله‌ای p ، $k-LH \in QMA$ [۱].

اثبات. 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 $H^{(i)} = \sum_s \lambda_s |s\rangle \langle s|$ باشد.

الگوریتم

مرلین: به عنوان اثبات، حالت پایه‌ی H (بردار $|\psi\rangle$) را برای آرتور ارسال می‌کند.
آرتور:

- حالت ارسال شده از طرف مرلین را در کنار یک کیوبیت اضافی که در حالت $|0\rangle$ آماده‌سازی شده است قرار می‌دهد. این کیوبیت اضافه را «کیوبیت جواب» می‌نامیم.
- به طور تصادفی و با احتمال یکسان، عدد i را بین ۱ تا m انتخاب می‌کند.
- نگاشت W_i را روی $|0\rangle \otimes |\psi\rangle$ اعمال می‌کند و کیوبیت جواب را در پایه‌ی محاسباتی اندازه‌گیری می‌کند. چنانچه حالت سیستم پس از اندازه‌گیری $|0\rangle$ باشد، اثبات را رد می‌کند و در غیر این صورت، می‌پذیرد.

برای هر i ، عمل W_i روی مجموعه‌ی مستقل خطی $\{|0\rangle \otimes |s\rangle\}_s$ به صورت زیر تعریف شده است:

$$W_i(|s\rangle \otimes |0\rangle) = \sqrt{\lambda_s} |s\rangle \otimes |0\rangle + \sqrt{1 - \lambda_s} |s\rangle \otimes |1\rangle \quad (۶.۵)$$

نخست توجه کنید که با توجه به این که $k \in O(\log n)$ ، آرتور می‌تواند نگاشت W_i را در زمان چندجمله‌ای اعمال کند. حال نشان می‌دهیم 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 ، $|\psi\rangle = \sum_s \alpha_s |s\rangle$. در این صورت

$$W_i(|\psi\rangle \otimes |0\rangle) = W_i\left(\sum_s \alpha_s |s\rangle \otimes |0\rangle\right) \quad (۷.۵)$$

$$= \sum_s \alpha_s W_i(|s\rangle \otimes |0\rangle) \quad (۸.۵)$$

$$= \sum_s \alpha_s (\sqrt{\lambda_s} |s\rangle \otimes |0\rangle + \sqrt{1 - \lambda_s} |s\rangle \otimes |1\rangle). \quad (۹.۵)$$

بنابراین احتمال این که آرتور پس از اعمال W_i و اندازه‌گیری کیویت جواب در پایه‌ی محاسباتی اثبات را بپذیرد برابر است با:

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

از طرفی داریم:

$$\sum_s |\alpha_s|^2 (1 - \lambda_s) = \sum_s |\alpha_s|^2 - \sum_s \lambda_s |\alpha_s|^2 = 1 - \sum_s \lambda_s |\alpha_s|^2 = 1 - \langle \psi | H^{(i)} | \psi \rangle \quad (10.5)$$

حال توجه کنید که احتمال پذیرفته شدن اثبات $|\psi\rangle$ توسط آرتور برابر با $1 - \frac{1}{m} \langle \psi | H | \psi \rangle$ است. بنابراین اگر $(H, \alpha, \beta) \in k\text{-LH}$ ، مرلین می‌تواند حالت پایه‌ی H را برای آرتور ارسال کند و آرتور با احتمال $1 - \frac{\alpha}{m}$ آن را می‌پذیرد. از طرفی اگر $(H, \alpha, \beta) \notin k\text{-LH}$ ، هر حالتی که از طرف مرلین ارسال شود، با احتمال $1 - \frac{\beta}{m}$ پذیرفته خواهد شد. نهایتاً با توجه به این که اختلاف ثوابت درستی و تمامیت، بزرگتر از $\frac{1}{p(n)}$ است، حکم از قضیه‌ی ۳.۴ نتیجه خواهد شد. \square

پیش از آن که به اثبات سخت بودن $k\text{-LH}$ برای کلاس QMA بپردازیم، خالی از فایده نیست که روند اثبات سخت بودن SAT برای NP را در قضیه‌ی کوک-لوین کلاسیک مرور کنیم.

فرض کنید $L \subseteq \{0, 1\}^*$ زبانی عضو کلاس 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 بیاییم به طوری که

$$z \in L \iff \phi_z \in SAT.$$

بدین منظور، توجه کنید که چون $L \in NP$ ، پس ماشین تورینگ قطعی $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{accept})$ 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 بیاییم که عملکرد M روی z را شبیه‌سازی کند. در این شبیه‌سازی باید موارد 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 [۱۹] 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 چندبه یک با زمان چندجمله‌ای، مسأله‌ای سخت برای کلاس QMA است.

اثبات. فرض کنید $\Pi = (\Pi_{Yes}, \Pi_{No})$ 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 از 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 $|\psi_{hist}\rangle = \sum_t |\psi_t\rangle_{in,pr,an} |t\rangle_C$ ، کد کرده است 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 پانویس C برای نمایش رجیستر کلاک استفاده شده است.

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

- برای آن‌که مقدار دهی اولیه‌ی رجیسترها را به آن‌چه 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 $y \in \{\circ, 1\}^{q(n)}$ ، به صورت

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

- برای آن‌که در زمان $t = T$ ، پس از اندازه‌گیری بیت خروجی (که در این‌جا فرض می‌کنیم کیوبیت اول رجیستر کمکی است). خروجی مدار برابر ۱ 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 این‌جا مقصود از $(|\circ\rangle\langle \circ|)_{an}$ نگاهی است که کیوبیت اول رجیستر کمکی را روی زیرفضای تولید شده توسط $|\circ\rangle$ می‌افکند و اثر آن روی باقی کیوبیت‌های رجیستر کمکی، همانی است.

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

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

می‌توان دید که برای هر حالت $|\phi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=\circ}^T (V_t V_{t-1} \dots V_1 |\eta\rangle_{in,pr,an}) \otimes |t\rangle_C$

$$H_{prop} |\phi\rangle = \sum_{t=\circ}^{T-1} -(V_{t+1} V_t \dots V_1 |\eta\rangle) \otimes |t+1\rangle \\ + \sum_{t=\circ}^{T-1} -(V_{t+1}^\dagger V_{t+1} V_t \dots V_1 |\eta\rangle) \otimes |t\rangle \\ + \sum_{t=\circ}^{T-1} (V_{t+1} V_t \dots V_1 |\eta\rangle) \otimes |t+1\rangle \\ + \sum_{t=\circ}^{T-1} (V_{t+1}^\dagger V_{t+1} V_t \dots V_1 |\eta\rangle) \otimes |t\rangle = \circ$$

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 $k\text{-LH}$ 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

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

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^۱ مشهور است نشان داد که در این حالت، $\lambda_{\min}(H) \geq \frac{\pi^2(1-\sqrt{\epsilon})}{2(T+1)^2}$. در این جا از بیان اثبات لم هندسی خودداری می‌کنیم. خواننده‌ی علاقه‌مند می‌تواند اثباتی برای این لم را در [۱] 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 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 نابیهی 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 $|\circ \dots \circ\rangle\langle \circ \dots \circ| - \mathbb{I}$ جایگزین کرد، که مقصود از $|\circ \dots \circ\rangle\langle \circ \dots \circ|$ نگاشتی است که تنها کیوبیت i ام رجیستر کمکی را روی زیرفضای تولید شده توسط $|\circ \dots \circ\rangle$ 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^۲ انجام دهیم. به عبارت دیگر، فرض کنید نمایش لحظه‌ی t در این رجیستر، به صورت $|\circ \dots \circ\rangle\langle \circ \dots \circ|$ باشد. در این صورت چک کردن محتوای رجیستر کلاک با چک کردن تنها سه کیوبیت از آن امکان‌پذیر است (کیوبیت‌های $t-1$ ، t ، $t+1$ ام).

به این ترتیب با توجه به این که گیت‌های V_i حداکثر ۲-موضعی هستند و حالت رجیستر کلاک نیز با عملگری حداکثر ۳-موضعی چک می‌شود، همیلتنی‌های ارائه شده 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 $|\circ \dots \circ\rangle\langle \circ \dots \circ|$ است. برای این که این التزام را ایجاد کنیم، همیلتنی دیگری را نیز به صورت $(|\circ \dots \circ\rangle\langle \circ \dots \circ|_{C_i} \otimes |\circ \dots \circ\rangle\langle \circ \dots \circ|_{C_i})$ تعریف می‌کنیم. 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. □

ملاحظه 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 [۱] بیان شده است. رگف و کمپ در [۲۰] این نتیجه را بهبود بخشیدند و نشان دادند LH ۳-مسأله‌ای کامل برای QMA است. نهایتاً کمپ، رگف و کیتائف در [۲۱] نشان دادند که LH ۲-نیز مسأله‌ای QMA -کامل است.

نتیجه ۸.۵. نتیجه‌ی سراسر 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، مسأله‌ی همیلتنی‌های موضعی حالت خاصی از مسأله‌ای کلی‌تر، یعنی مسأله‌ی 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 LH برای کلاس QMA این است که با فرض $QMA \neq NP$ ، همیلتنی‌هایی وجود دارند که حالت پایه‌ی آن‌ها توصیف کارای کلاسیک ندارد. می‌توان نشان داد که این مطلب بدان معنی است که حالت پایه‌ی چنین همیلتنی‌هایی قویاً درهم‌تنیده است.^۳ این نتیجه، سازگار با این مطلب است که ماده در دمای نزدیک به صفر خواصی مانند ابرشارگی^۴ و ابررسانایی^۵ را از خود نشان می‌دهد که 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 جریان برنامه‌ی لنگلندز^۶ توسط لورن لافورگ ارائه شد،

^۱geometric lemma

^۲unary

^۳تاکنون اندازه‌های متعددی برای کمی‌سازی درهم‌تنیدگی و مقایسه‌ی آن توسعه یافته است.

^۴superfluidity

^۵superconductivity

^۶Langlands program

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 چنین خیالی نیز دلپذیر است، با این حال عجیب به نظر می‌رسد و بعید است که بتوان آن را عملی کرد. در واقع همواره این امکان وجود دارد که ایراد اثبات در آن قسمتی باشد که شما آن را نخوانده‌اید (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 حال بگذارید توجه خود را به جای هر اثباتی، معطوف به اثبات‌هایی کنیم که برای مصداقی از مسأله‌ای 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^۱ می‌گویند، در اختیار ما می‌گذارد.

به قضیه‌ی 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 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 به دست آورده‌ایم بهتر کرد. 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 را برای قضیه‌ی PCP بیان خواهیم کرد، و معادل بودن این دو صورت‌بندی را نشان خواهیم داد.

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

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

مثال ۱۲.۵. مسأله‌ی MAX-3SAT را به عنوان مسأله‌ی یافتن بیشترین تعداد پراکنش‌های ممکن در یک فرمول CNF-3 که به طور هم‌زمان قابل ارضاشدن هستند، در نظر بگیرید. الگوریتم زیر، الگوریتمی $\frac{1}{2}$ -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 پراکنش 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 برآورده‌شدن یا نشدن t عبارت مشخص شود، حداقل $\frac{1}{2}$ آنها برآورده می‌شوند و بنابراین در نهایت حداقل $\frac{1}{2}$ کل عبارات اولیه برآورده شده‌اند. بنابراین الگوریتم پیشنهادشده یک الگوریتم $\frac{1}{2}$ -تقریب برای مسأله‌ی MAX-3SAT است.

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

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

^۱ Probabilistically checkable proofs

به طور مشابه، تعریف بالا را می‌توان برای مسأله‌های بیشینه‌سازی نیز انجام داد. اهمیت تعریف بالا آن‌جاست که می‌توان از آن برای نشان‌دادن 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 $Gap\text{-}\mathcal{P}_{\alpha(n)}$ مسأله‌ای \mathcal{NP} -سخت است. گزاره‌ی زیر چرایی این امر را بیان می‌کند.

گزاره ۱۴.۵. فرض کنید برای یک مسأله‌ی کمینه‌سازی \mathcal{P} ، مسأله‌ی $Gap\text{-}\mathcal{P}_{h(n),\alpha(n)}$ ، \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.

اثبات. 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 $Gap\text{-}\mathcal{P}_{h(n),\alpha(n)}$ ، یک ورودی مانند I_x را برای مسأله‌ی $Gap\text{-}\mathcal{P}_{h(n),\alpha(n)}$ بدست می‌آوریم. حال، الگوریتم $\alpha(n)$ -تقریب موجود برای حل \mathcal{P} را روی I_x اجرا می‌کنیم. توجه کنید که:

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

بنابراین با توجه به مقدار $A(I_x)$ ، می‌توان $Gap\text{-}\mathcal{P}_{h(n),\alpha(n)}$ 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 $Gap\text{-}MAX\text{-}3SAT_{1,\rho}$ ، \mathcal{NP} -سخت است [۲۲].

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^۱ 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 \mathcal{P} 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، چنان‌که:

- 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 $Gap\text{-}\mathcal{P}_{h(n),g(n)}$ مسأله‌ای \mathcal{NP} -کامل باشد، $Gap\text{-}\mathcal{P}'_{h'(n'),g'(n')}$ نیز چنین است. به این ترتیب، می‌توان با استفاده از قضیه‌ی ۱۵.۵، سختی تقریب مسائل بیشتری را اثبات کرد. حال به صورت‌بندی دوم قضیه‌ی PCP می‌پردازیم.

تعریف ۱۷.۵. یک تصدیق‌کننده‌ی $(r(n), q(n))$ -محدود، تصدیق‌کننده‌ای 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 بزند و آن‌ها را بخواند.

تعریف ۱۸.۵. کلاس پیچیدگی $PCP(r(n), q(n))$ عبارت است از همه‌ی زبان‌هایی مانند L ، به طوری که تصدیق‌کننده‌ی $(r(n), q(n))$ -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 ، $\Pr[V(x, \pi) = 1] \leq \frac{1}{p}$.

^۱ gap-preserving reduction

قضیه ۱۹.۵ ((قضیه‌ی PCP: اثبات‌های قابل بررسی احتمالاتی)). $PCP(\mathcal{O}(\log n), \mathcal{O}(1)) = \mathcal{NP}$. [۲۲].

قضیه‌ی فوق، به طور شگفت‌آوری با شهود ما در تناقض است. مثلاً فرمول ۳-CNF ای را در نظر بگیرید که ارضاشدنی نیست، اما تمام پُرانتزهای آن به جز یکی به طور هم‌زمان ارضاشدنی هستند. برای چنین فرمولی، به نظر می‌رسد با نگاه کردن تصادفی به تنها $\mathcal{O}(1)$ بیت از یک اثبات، نتوان با احتمال بالا عضویت فرمول را در SAT-۳ رد کرد. با این حال شگفتی قضیه‌ی 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 قضیه‌ی PCP، که اثباتی جبری و مبتنی بر نظریه‌ی کدگذاری است، در [۲۲] مطرح شده است؛ گرچه بسیاری از بخش‌های اثبات نتایجی هستند که در [۲۳] اثبات شده بودند. اثباتی جدیدتر و ترکیباتی، با تکیه بر ویژگی‌های گراف‌های گسترده، توسط دینور در [۲۴] ارائه شده است. هر دوی اثبات‌ها طولانی و پیچیده هستند و بیان آن‌ها در این مجال نمی‌گنجد. با این حال، به عنوان خاتمه‌ی این بخش، نشان خواهیم داد که دو صورت بیان‌شده از قضیه‌ی 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 $\text{Gap-MAX-3SAT}_{1,\rho}$ ، \mathcal{NP} -سخت باشد [۲۲].

اثبات. 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 تصدیق‌کننده‌ی $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود V برای L وجود دارد. توجه کنید که طول اثبات حداکثر $2^{\mathcal{O}(\log n)}$ بیت است. حال تصدیق‌کننده‌ای 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 کوثری‌هایی که بر اساس برآمد بیت‌های تصادفی تعیین می‌شوند، بپذیرد حساب می‌کند. نهایتاً 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 تصدیق‌کننده‌ی $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود دارد. با توجه به تحویلی که از L به $\text{Gap-MAX-3SAT}_{1,\rho}$ 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 پُرانتزهای C_1, C_2, \dots, C_m را دارد $(m, n \in n^{\mathcal{O}(1)})$. یک تصدیق‌کننده‌ی $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود برای L ، ابتدا 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 پُرانتزها 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 پُرانتز انتخاب‌شده، تصدیق‌کننده مقادیر مربوط به متغیرهای ظاهر شده در پُرانتز مزبور را از اثبات می‌خواند، و اثبات را می‌پذیرد اگر و فقط اگر با آن مقادیر پُرانتز مزبور ارضا شود. توجه کنید در حالتی که $x \in L$ ، ϕ_x ارضا پذیر است و اثباتی وجود دارد که توسط تصدیق‌کننده پذیرفته شود. در حالتی که $x \notin L$ ، احتمال آن که اثباتی توسط تصدیق‌کننده پذیرفته شود، حداکثر برابر ρ است (زیرا تعداد پُرانتزهایی که هم‌زمان ارضاشدنی هستند، ρ برابر تعداد کل پُرانتزهاست). از طرفی، با تکرار می‌توان خطا را کاهش داد و به $\frac{1}{p}$ رساند. بنابراین تصدیق‌کننده‌ای $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود برای L وجود دارد.

حال به اثبات سمت «تنها اگر» می‌پردازیم. فرض کنید $L \in \mathcal{NP}$ است و تصدیق‌کننده‌ای $(\mathcal{O}(\log n), \mathcal{O}(1))$ -محدود دارد. 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 o ، C_o قیدی است که تنها وابسته به بیت‌هایی است که با توجه به آن برآمد از اثبات خوانده می‌شوند، و C_o برآورده می‌شود اگر و تنها اگر تصدیق‌کننده با خواندن بیت‌هایی از اثبات که با توجه به o تعیین شده‌اند، اثبات را بپذیرد.

توجه کنید که هر قید CSP فوق تنها به $\mathcal{O}(1)$ متغیر وابسته است، و $2^{\mathcal{O}(\log n)}$ 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 پذیرفته شدن اثبات توسط تصدیق‌کننده حداکثر $\frac{1}{p}$ است؛ بنابراین حداکثر $\frac{1}{p}$ قیود ورودی مسأله به طور هم‌زمان ارضاشدنی هستند. بنابراین یک تحویل از L به Gap-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^k} پرانتز 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 $1 - \frac{1}{k^{2^k}}$ خواهد بود، و می‌دانیم با تکرار می‌توان ثابت درستی را به عددی ثابت کاهش داد. از طرفی چون $k \in \mathcal{O}(1)$ ، تحویل به دست آمده تحویلی چندجمله‌ای است. □

۲.۳.۵. حدس PCP کوانتومی. همان‌گونه که تا به این جا 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 حدس باقی است. افزون بر این، حتی درستی یا نادرستی این حدس نیز در هاله‌ای از ابهام است و شواهدی کافی به نفع هیچ‌یک وجود ندارد [۲۵].

در این زیربخش، به معرفی دو صورت از حدس PCP کوانتومی خواهیم پرداخت. این حدس نخستین بار به صورت دقیق در [۲۷] صورت‌بندی شده است؛ گرچه شواهدی برای این که پیش از این مقاله نیز افرادی به وجود چنین همتای کوانتومی‌ای برای قضیه‌ی PCP امیدوار بوده‌اند، در [۴] و [۲۶] قابل ردگیری است.

تعریف ۲.۱.۵. 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 می‌پذیرد یا رد می‌کند.

تعریف ۲.۲.۵. کلاس پیچیدگی $QPCP(k, c, s)$ عبارت است از تمام مسأله‌های قراردادی مانند $\Pi = (\Pi_{Yes}, \Pi_{No})$ به طوری که تصدیق‌کننده‌ای $QPCP(k)$ 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 ۲.۳.۵ (حدس QPCP: نسخه‌ی اثبات‌های قابل بررسی احتمالاتی). $QMA = QPCP(\mathcal{O}(1), c, s)$ که در آن، $c - s = \Omega(1)$. [۲۷]

پیش از بیان نسخه‌ی سختی تقریب این حدس، از تعریف ۳.۵ به یاد آورید که تا به این جا، 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 -LH را می‌توان برای فاصله‌های قراردادی دیگر نیز تعریف کرد. افزون بر این، از این جا 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 ۲.۴.۵ (حدس QPCP: نسخه‌ی سختی تقریب). ثابت $\gamma > 0$ وجود دارد به طوری که k -LH با فاصله‌ی قراردادی γ ، تحت تحویل چندبه‌یک چندجمله‌ای کوانتومی مسأله‌ای QMA -سخت است [۲۷].

مقصود از یک تحویل چندبه‌یک چندجمله‌ای کوانتومی در گزاره‌ی بالا یک الگوریتم کوانتومی و چندجمله‌ای است که با احتمال ثابت و ناصفر، تابع تحویل را پیاده‌سازی می‌کند.

ملاحظه ۲.۵.۵. مشابه با قضیه‌ی PCP کلاسیک، می‌توان نشان داد دو صورت بیان‌شده 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 -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 [۲۸] بیابد.

ملاحظه 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 برای آن‌ها 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 [۲۵].

۶. مؤخره: پیشرفت‌های جدیدتر و زمینه‌های پژوهش

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

(۱) در جست‌وجوی ارتباطاتی عمیق‌ترین فیزیک و نظریه‌ی محاسبه: همان‌گونه که در این مقاله 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 بخش 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 این جای این مقاله بارها بر آن تاکید کرده‌ایم، تلاش برای یافتن آنالوژی‌هایی میان محاسبات کلاسیک و محاسبات کوانتومی است. نظریه‌ی محاسبه و پیچیدگی محاسبه‌ی کلاسیک طی 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، این که آیا نتایج مشابهی در این زمینه نیز یافت خواهد شد، کنجکاو‌برانگیز است. با این حال، این سوال ممکن است در ذهن ایجاد شود که آیا چنین نتایج «مشابهی»، واقعاً سودمند و عمیق نیز هستند؟ این جاست که اهمیت فیزیکی مسأله می‌تواند به عنوان راهنمایی برای گزینش مسائل «خوب» به یاری ما بیاید [۲۹].

همان‌گونه که در یادداشت‌های ۹.۵ و ۲۶.۵ دیدیم، مسأله‌ی 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 [۳۰]). 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 [۳۱] مورد مطالعه قرار گرفته‌اند.

- وجهی دیگر از این ارتباطات، تاثیر آن بر پیشبرد فیزیک نظری است. آن‌گونه که ویگدرسون در [۳۲] 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 [۳۳] دید، که به بررسی همواری افق‌های سیاه‌چاله‌ها از منظر محاسباتی و ارتباط این موضوع با اثبات‌های دانش صفر کوانتومی می‌پردازند. انتظار می‌رود که موارد بیشتری از چنین ارتباطاتی با 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 [۳۲].

(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 از

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 [۲۵]. 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 پژوهش‌های متاخر را می‌توان در [۳۴، ۳۵، ۳۶] 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. یک نمونه‌ی آن، یافتن صورت‌بندی جدیدی از کلاس NP از طریق ارائه‌ی پروتکلی برای تصدیق یک اثبات $3SAT$ 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 [۳۷] معرفی شده است. نمونه‌ای دیگر و متاخرتر، نتیجه‌ای است که توسط آهارونوف و همکاران در [۱۴] به دست آمده است. در این‌جا 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^۱ است، برنامه‌ای است که در حال حاضر در پیچیدگی محاسبات کلاسیک در جریان است. باور عمومی بر این است که این برنامه به نتیجه خواهد رسید و خواهیم توانست نشان دهیم که تصادفی‌سازی بر قدرت محاسباتی نمی‌افزاید.

مراجع

- [1] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalıy. 2002. Classical and Quantum Computation. American Mathematical Society, USA.
- [2] Watrous, J. (2000, November). Succinct quantum proofs for properties of finite groups. In Proceedings 41st Annual Symposium on Foundations of Computer Science (pp. 537-546). IEEE.
- [3] Vidick, T., & Watrous, J. (2016). Quantum proofs. Foundations and Trends® in Theoretical Computer Science, 11(1-2), 1-215.
- [4] Aharonov, D., & Naveh, T. (2002). Quantum NP-a survey. arXiv preprint quant-ph/0210077.
- [5] Marriott, C., & Watrous, J. (2005). Quantum arthur-merlin games. computational complexity, 14(2), 122-152.
- [6] Yamakami, T. (1999). Analysis of Quantum Functions: (Preliminary Version). In Foundations of Software Technology and Theoretical Computer Science: 19th Conference Chennai, India, December 13-15, 1999 Proceedings 19 (pp. 407-419). Springer Berlin Heidelberg.
- [7] Aaronson, S., & Kuperberg, G. (2007, June). Quantum versus classical proofs and advice. In Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07) (pp. 115-128). IEEE.
- [8] Aaronson, S. (2009). On perfect completeness for QMA. Quantum Information and Computation, 9(1), 0081-0089.
- [9] Jordan, S. P., Kobayashi, H., Nagaj, D., & Nishimura, H. (2012). Achieving perfect completeness in classical-witness quantum merlin-arthur proof systems. Quantum Information & Computation, 12(5-6), 461-471.
- [10] Kobayashi, H., Matsumoto, K., & Yamakami, T. (2003). Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur?. In Algorithms and Computation: 14th International Symposium, ISAAC 2003, Kyoto, Japan, December 15-17, 2003. Proceedings 14 (pp. 189-198). Springer Berlin Heidelberg.
- [11] Liu, Y. K., Christandl, M., & Verstraete, F. (2007). Quantum computational complexity of the N-representability problem: QMA complete. Physical review letters, 98(11), 110503.
- [12] Harrow, A. W., & Montanaro, A. (2013). Testing product states, quantum Merlin-Arthur games and tensor optimization. Journal of the ACM (JACM), 60(1), 1-43.
- [13] Bravyi, S., Bessen, A. J., & Terhal, B. M. (2006). Merlin-Arthur games and stoquastic complexity. arXiv preprint quant-ph/0611021.
- [14] Aharonov, D., Grilo, A. B., & Liu, Y. (2020). StoqMA vs. MA: the power of error reduction. arXiv preprint arXiv:2010.02835.
- [15] Osborne, T. J. (2012). Hamiltonian complexity. Reports on progress in physics, 75(2), 022001.
- [16] Gharibian, S., Huang, Y., Landau, Z., & Shin, S. W. (2015). Quantum hamiltonian complexity. Foundations and Trends® in Theoretical Computer Science, 10(3), 159-282.
- [17] Trakhtenbrot, B. A. (1984). A Survey of Russian Approaches to Perebor (Brute-Force Searches) Algorithms. Annals of the History of Computing, 6, 384-400.
- [18] Cook, S. A. (2023). The complexity of theorem-proving procedures. In Logic, Automata, and Computational Complexity: The Works of Stephen A. Cook (pp. 143-152).
- [19] Balcazar, J. L., Diaz, J., & Gabarro, J. (2012). Structural Complexity I. Springer Science & Business Media.
- [20] Kempe, J., & Regev, O. (2003). 3-local Hamiltonian is QMA-complete. Quantum Information and Computation, 3(3), 258-264.

¹ derandomization

- [21] Kempe, J., Kitaev, A., & Regev, O. (2005). The complexity of the local Hamiltonian problem. In FSTTCS 2004: Foundations of Software Technology and Theoretical Computer Science: 24th International Conference, Chennai, India, December 16-18, 2004. Proceedings 24 (pp. 372-383). Springer Berlin Heidelberg.
- [22] Arora, S., Lund, C., Motwani, R., Sudan, M., & Szegedy, M. (1998). Proof verification and the hardness of approximation problems. *Journal of the ACM (JACM)*, 45(3), 501-555.
- [23] Arora, S., & Safra, S. (1992). Probabilistic checking of proofs; a new characterization of NP. *Proceedings., 33rd Annual Symposium on Foundations of Computer Science*, 2-13.
- [24] Dinur, I., & Reingold, O. (2004). Assignment testers: towards a combinatorial proof of the PCP-theorem. 45th Annual IEEE Symposium on Foundations of Computer Science, 155-164.
- [25] Aharonov, D., Arad, I., & Vidick, T. (2013). Guest column: the quantum PCP conjecture. *ACM sigact news*, 44(2), 47-79.
- [26] Shtetl-Optimized » Blog Archive » The Quantum PCP Manifesto. (n.d.). Retrieved April 14, 2023, from <https://scottaaronson.blog/?p=139>
- [27] Aharonov, D., Arad, I., Landau, Z., & Vazirani, U. (2009, May). The detectability lemma and quantum gap amplification. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 417-426).
- [28] Grilo, A. B. (2018). Quantum proofs, the local Hamiltonian problem and applications (Doctoral dissertation, Université Sorbonne Paris Cité).
- [29] A quantum PCP theorem? | MyCQstate. (n.d.). Retrieved April 6, 2024, from <https://mycqstate.wordpress.com/2013/02/24/a-quantum-pcp-theorem/>
- [30] Gharibian, S., & Le Gall, F. (2022, June). 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* (pp. 19-32).
- [31] Brandao, F. G., & Harrow, A. W. (2013, June). Product-state approximations to quantum ground states. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing* (pp. 871-880).
- [32] Wigderson, A. (2019). *Mathematics and computation: A theory revolutionizing technology and science*. Princeton University Press.
- [33] Harlow, D., & Hayden, P. (2013). Quantum computation vs. firewalls. *Journal of High Energy Physics*, 2013(6), 1-56.
- [34] Chailloux, A., & Sattath, O. (2012, June). The complexity of the separable Hamiltonian problem. In *2012 IEEE 27th Conference on Computational Complexity* (pp. 32-41). IEEE.
- [35] Bittel, L., Gharibian, S., & Kliesch, M. (2023). The Optimal Depth of Variational Quantum Algorithms Is QCMA-Hard to Approximate. In *38th Computational Complexity Conference (CCC 2023)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.
- [36] Grilo, A. B., Kerenidis, I., & Sikora, J. (2015, August). QMA with subset state witnesses. In *International Symposium on Mathematical Foundations of Computer Science* (pp. 163-174). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [37] Aaronson, S., Beigi, S., Drucker, A., Fefferman, B., & Shor, P. (2008, June). The power of unentanglement. In *2008 23rd Annual IEEE Conference on Computational Complexity* (pp. 223-236). IEEE.
- [38] Yao, A. C. C. (1993, November). Quantum circuit complexity. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science* (pp. 352-361). IEEE.
- [39] Akama, S. (2015). *Elements of quantum computing. History, Theories and Engineering Applications*, Springer.
- [40] Macchiavello, C., Palma, G. M., & Zeilinger, A. (Eds.). (2000). *Quantum Computation and Quantum Information Theory: Reprint Volume with Introductory Notes for ISI TMR Network School, 12-23 July 1999, Villa Gualino, Torino, Italy*. World Scientific.
- [41] Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., ... & Weinfurter, H. (1995). Elementary gates for quantum computation. *Physical review A*, 52(5), 3457.
- [42] Watrous, J. (2018). *The theory of quantum information*. Cambridge university press.
- [43] Deutsch, D. E. (1989). Quantum computational networks. *Proceedings of the royal society of London. A. mathematical and physical sciences*, 425(1868), 73-90.
- [44] Barenco, A. (1995). 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.
- [45] Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.
- [46] Deutsch, D. E., Barenco, A., & Ekert, A. (1995). Universality in quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 449(1937), 669-677.
- [47] Dawson, C. M., & Nielsen, M. A. (2006). The Solovay-Kitaev algorithm. *Quantum Information and Computation*, 6(1), 81-95.
- [48] Cook, S. A. (1970). Alan Cobham. The intrinsic computational difficulty of functions. *Logic, methodology and philosophy of science*, *Proceedings of the 1964 International Congress*, edited by Yehoshua Bar-Hillel, *Studies in logic and the foundations of mathematics*, North-Holland Publishing Company, Amsterdam 1965, pp. 24-30. *The Journal of Symbolic Logic*, 34(4), 657-657.
- [49] Tang, C. L. (2005). *Fundamentals of quantum mechanics: for solid state electronics and optics*. Cambridge University Press.
- [50] Planck, M. (1978). Über das gesetz der energieverteilung im normalspektrum (pp. 178-191). Vieweg+ Teubner Verlag.
- [51] Einstein, A. (1965). Concerning an heuristic point of view toward the emission and transformation of light. *American Journal of Physics*, 33(5), 367.
- [52] Bohr, N. (1913). I. On the constitution of atoms and molecules. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 26(151), 1-25.

- [53] Von Neumann, J. (2013). *Mathematische grundlagen der quantenmechanik* (Vol. 38). Springer-Verlag.
- [54] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886), 802-803.
- [55] Dieks, D. G. B. J. (1982). Communication by EPR devices. *Physics Letters A*, 92(6), 271-272.
- [56] Benioff, P. (1980). 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.
- [57] Feynman, R. P. (2018). Simulating physics with computers. In *Feynman and computation* (pp. 133-153). CRC Press.
- [58] Bernstein, E., & Vazirani, U. (1993, June). Quantum complexity theory. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing* (pp. 11-20).
- [59] Simon, D. R. (1997). On the power of quantum computation. *SIAM journal on computing*, 26(5), 1474-1483.
- [60] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219).
- [61] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2), 303-332.
- [62] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505-510.
- [63] White House Earmarks New Money for A.I. and Quantum Computing - The New York Times. (n.d.). Retrieved April 7, 2024, from <https://www.nytimes.com/2020/02/10/technology/white-house-earmarks-new-money-for-ai-and-quantum-computing.html>
- [64] Shamir, A. (1992). $IP = PSPACE$. *Journal of the ACM (JACM)*, 39(4), 869-877.
- [65] Sipser, M. (1992, July). The history and status of the P versus NP question. In *Proceedings of the twenty-fourth annual ACM symposium on Theory of computing* (pp. 603-618).
- [66] Babai, L., Fortnow, L., & Lund, C. (1991). Non-deterministic exponential time has two-prover interactive protocols. *Computational complexity*, 1, 3-40.
- [67] Knill, E. (1996). Quantum randomness and nondeterminism. *arXiv preprint quant-ph/9610012*.
- [68] Schrödinger, E. (1935, October). Discussion of probability relations between separated systems. In *Mathematical Proceedings of the Cambridge Philosophical Society* (Vol. 31, No. 4, pp. 555-563). Cambridge University Press.
- [69] Jozsa, R., & Linden, N. (2003). On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 459(2036), 2011-2032.

* دانشجوی دکتری علوم کامپیوتر، انستیتو پلی تکنیک پاریس

تارنما: <https://ali-almasi.github.io>

رایانامه: ali.almasi@polytechnique.edu