ارائه ۱۳	پردازش اطلاعات کوانتومی پاییز ۱۴۰۲	دکتر احمد خونساری

مقدمه

در این ارائه به پیچیدگی محاسباتی می‌پردازیم. ابتدا «تز چرچ-تورینگ» را مطرح می‌کنیم:

> یک تابع که بر روی اعداد طبیعی تعریف شده است را می‌توان با یک روش «قابل اجرا»[1] محاسبه کرد اگر و تنها اگر بتوان آن را با یک ماشین تورینگ محاسبه کرد.

ماشین تورینگ یک مدل انتزاعی محاسبه است که در ادامه بیشتر با آن آشنا می‌شویم. این تز در مورد مبحث محاسبه‌پذیری[2] اظهار نظر می‌کند. یعنی چه توابعی را می‌توان «محاسبه» کرد و چه توابعی را نمی‌توان محاسبه کرد. شاید با «مسئله توقف»[3] آشنا باشید. از آنجا که با استفاده از ماشین تورینگ نمی‌توان این مسئله را (به صورت قابل اجرا) حل کرد، بنابراین این مسئله به صورت کلی قابل حل نیست. محاسبات کوانتومی تز چرچ-تورینگ را نقض نمی‌کنند. یعنی از یک کامپیوتر کوانتومی نمی‌توان استفاده کرد تا مسائلی که با کامپیوترهای کلاسیک «قابل حل» نیستند را حل کرد. اما به نظر می‌رسد که کامپیوترهای کوانتومی بتوانند «تز قوی چرچ-تورینگ» را نقض کنند که به صورت زیر مطرح می‌شود:

> هر فرایند الگوریتمی را می‌توان به صورت «کارا»[4] با استفاده از یک ماشین تورینگ احتمالاتی شبیه‌سازی کرد.

در اینجا منظور از «کارا» سربار چندجمله‌ای به نسبت اندازه ورودی است. یعنی، احتمال این وجود دارد که بتوان مسائلی را با کامپیوترهای کوانتومی به صورت کارا حل کرد که امکان حل کارای آن‌ها با ماشین‌های تورینگ احتمالاتی وجود نداشته باشد. به صورت خاص، مسئله تجزیه به عوامل اول و الگوریتم Shor را به خاطر بیاورید. دیدیم که هیچ الگوریتم کارایی برای حل این مسئله به صورت کلاسیک برای ما شناخته شده نیست. اما الگوریتم Shor ظاهراً با یک

---

[1] Effective
[2] Computability
[3] Halting Problem
[4] Efficient

تسریع نمایی محاسبات نسبت به هر الگوریتم کلاسیک می‌تواند این مسئله را به صورت کارا حل کند. در نتیجه سؤال اینجاست که آیا کلاس مسائلی که به صورت کارا با استفاده از کامپیوترهای کوانتومی قابل حل هستند از مسائلی که به صورت کارا قابل حل به‌وسیله کامپیوترهای کلاسیک هستند به صورت بنیادی متفاوت است؟

خودکاره متناهی

یک خودکاره متناهی[۵] یک مدل انتزاعی محاسبه است (که از ماشین تورینگ بسیار ساده‌تر است). این مدل را از طریق مؤلفه‌های زیر تعریف می‌کنیم:

۱. یک مجموعه از n_s حالت.

۲. یک الفبای ورودی به اندازه n_a.

۳. یک مجموعه از گذرها. به ازای هر حرف در الفبا می‌توان فرض کرد که یک ماتریس گذار $n_s \times n_s$ وجود دارد. یعنی در هر حالت با مشاهده هر حرف الفبا چگونه حالت تغییر خواهد کرد؟

۴. یک حالت شروع اولیه.

۵. یک (یا چند) حالت پذیرش. تبدیل کردن چند حالت پذیرش به یک حالت پذیرش کار راحتی است. بنابراین بدون از دست رفتن کلیت می‌توان فرض کرد که خودکاره فقط یک حالت پذیرش دارد.

روش کار با این خودکاره به این صورت است. خودکاره ابتدا در حالت شروع قرار دارد. سپس ما یک رشته از حروف الفبا را دریافت می‌کنیم. می‌خواهیم ببینیم که آیا این رشته مورد پذیرش است یا نه. به اولین حرف رشته نگاه می‌کنیم و با استفاده از ماتریس گذار مشخص می‌کنیم که سیستم به چه حالتی می‌رود. سپس این فرآیند را برای حرف‌های بعدی از حالت‌های بعدی به‌دست آمده دنبال می‌کنیم. اگر در پایان این فرآیند در حالت پذیرش باشیم، می‌گوییم که رشته مورد پذیرش قرار گرفته است. در غیر این‌صورت رشته رد می‌شود.

زبان مورد پذیرش یک خودکاره متناهی مجموعه تمام رشته‌هایی است که مورد پذیرش هستند. خودکاره‌ها را به صورت مناسبی می‌توان به صورت گرافیکی از طریق یک گراف جهت‌دار نمایش داد. به صورت خاص به ازای هر حالت می‌توان یک گره در نظر گرفت و به ازای هر انتقال یک یال جهت‌دار اضافه کرد. هر یال به وسیله حرف الفبای متناظرش برچسب‌گذاری می‌شود. معمولاً گره‌های متناظر حالت پذیرش را متفاوت از بقیه نمایش می‌دهند. گاهی آن‌ها را با رنگ تیره‌تر و گاهی با استفاده از دو دایره تو در تو مشخص می‌کنند.

[5] Finite automata

خودکاره متناهی قطعی: توجه کنید که برای خودکاره متناهی این شرط را اعمال نکردیم که به ازای مشاهده هر حرف الفبا، خودکاره فقط به یک حالت بعدی منتقل بشود. اما اگر این ویژگی برقرار باشد به آن خودکاره قطعی[۶] می‌گوییم. در نمایش گرافیکی خودکاره‌های قطعی، به ازای هر حرف الفبا فقط یک یال خروجی از هر گره (حالت) وجود دارد. اگر بخواهیم با استفاده از نمادگذاری ماتریسی رفتار یک خودکاره را نمایش دهیم، می‌توانیم به صورت زیر عمل کنیم.

فرض کنید $|i\rangle$ حالت شروع را نشان دهد و رشته $s_1s_2\dots s_n$ داده شده است. فرض کنید که ماتریس گذار متناظر حرف s_i با M_{s_i} نمایش داده شود. در این صورت، نقل و انتقال خودکاره را می‌توان به صورت زیر نمایش داد:

$$|f\rangle = M_{s_n}M_{s_{n-1}}\dots M_{s_1}|i\rangle. \tag{۱}$$

به مثال زیر توجه کنید. فرض کنید که یک خودکاره با دو حالت $|0\rangle$ و $|1\rangle$ داریم که $|0\rangle$ حالت شروع را نشان می‌دهد. در این خودکاره الفبا از دو حرف a و b تشکیل می‌شود که ماتریس‌های گذار آن‌ها به شکل زیر است:

$$M_a = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad M_b = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}. \tag{۲}$$

توجه کنید که مشاهده حرف a حالت را تغییر نمی‌دهد اما مشاهده حرف b باعث انتقال به حالت $|1\rangle$ می‌شود. در این حالت اگر $|1\rangle$ حالت پذیرش باشد، آنگاه زبان این خودکاره تمام رشته‌هایی است که در آن‌ها حداقل یک حرف b وجود داشته باشد. توجه کنید که در خودکاره‌های قطعی، ماتریس‌های گذار در هر ستون فقط یک درایه غیرصفر مساوی با یک دارند و بقیه درایه‌ها صفر هستند.

خودکاره متناهی غیرقطعی: خودکاره‌های متناهی غیرقطعی[۷] در هر حالت پس از مشاهده هر حرف الفبا ممکن است به بیش از یک حالت دیگر منتقل شوند. یعنی به ازای هر حرف از هر گره چندین یال خروجی وجود دارد. بنابراین ماتریس گذار معادل هر حرف یک ماتریس دلخواه است که درایه‌های آن صفر یا یک هستند. در این حالت یک رشته مورد پذیرش قرار می‌گیرد اگر حداقل یک مسیر وجود داشته باشد که با مشاهده حرف رشته با شروع از حالت اولیه به حالت پذیرش برسد. بنابراین می‌بینید که در هر حالت به صورت غیرقطعی می‌توان یکی از یال‌های خروجی را انتخاب کرد. در مثال پیشین، فرض کنید ماتریس گذار حروف a و b به شکل زیر باشد:

$$M_a = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad M_b = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{۳}$$

همچنان مشاهده a حالت را تغییر نمی‌دهد، اما مشاهده b می‌تواند حالت را تغییر ندهد و یا می‌تواند حالت را از $|0\rangle$ به $|1\rangle$ تغییر دهد. دقت کنید که زبان این خودکاره دقیقاً معادل خودکاره قبلی است و شامل تمام رشته‌هایی می‌شود که حداقل یک b در آن‌ها وجود دارد.

[6] Deterministic
[7] Nondeterministic

خودکاره احتمالاتی: خودکاره‌های تصادفی مشابه خودکاره‌های غیرقطعی هستند، با این تفاوت که هر گذار به صورت احتمالاتی اتفاق می‌افتد. به این ترتیب ماتریس‌های گذار متناظر هر حرف دارای درایه‌های اعشاری بین 0 و 1 هستند که البته جمع درایه‌های هر ستون برابر 1 است. در این شرایط پذیرش یک رشته ورودی را می‌توان به دو صورت زیر تعریف کرد:

۱. یک رشته مورد پذیرش قرار می‌گیرد اگر با اطمینان کامل (احتمال یک) یک مسیر از حالت اولیه به حالت پذیرش وجود داشته باشد.

۲. یک رشته مورد پذیرش قرار می‌گیرد اگر یک مسیر از حالت اولیه به حالت پذیرش وجود داشته باشد که احتمال وقوع آن بیش از یک آستانه از پیش تعیین‌شده باشد.

در مثال پیشین، فرض کنید ماتریس‌های گذار حروف a و b به شکل زیر تعریف شوند:

$$M_a = \begin{bmatrix} 0.9 & 0.1 \\ 0.1 & 0.9 \end{bmatrix}, \qquad M_b = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}. \tag{۴}$$

همچنان فرض کنید که $\langle 1|$ حالت پذیرش باشد. در این شرایط در صورتی که حرف b مشاهده شود، رشته حتماً مورد پذیرش قرار می‌گیرد. اما با مشاهده a خودکاره با احتمال 0.1 به حالت پذیرش منتقل می‌شود. بنابراین می‌توان زبان این خودکاره را به دو صورت تعریف کرد: (۱) اگر مسیرهای با احتمال یک در نظر گرفته شوند، مشابه دو خودکاره قبلی، زبان این خودکاره تمام رشته‌هایی است که حداقل یک حرف b در آن‌ها باشد، (۲) اگر آستانه پذیرش را 0.1 تعریف کنیم، آنگاه زبان این خودکاره تمام رشته‌هایی است که حداقل یک حرف (a یا b) در آن‌ها باشد.

خودکاره کوانتومی: در این خودکاره، ماتریس‌های گذار از نوع ماتریس‌های یکانی هستند که درایه‌های آن‌ها ممکن است اعداد مثبت و منفی مختلط باشند. در اینجا نیز پذیرش یک رشته را (مشابه خودکاره احتمالاتی) می‌توان منوط به یک آستانه کرد. بنابراین احتمال حضور در حالت پذیرش باید از یک مقدار از پیش تعیین‌شده بیشتر باشد تا رشته مورد پذیرش قرار بگیرد. فرض کنید یک خودکاره کوانتومی با دو حالت $\langle 0|$ و $\langle 1|$ داریم که در آن الفبا فقط یک حرف a را دارد. فرض کنید ماتریس متناظر این حرف به صورت زیر تعریف می‌شود:

$$M_a = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}. \tag{۵}$$

فرض کنید $\langle 1|$ حالت پذیرش باشد. بنابراین برای رشته "a" با شروع از حالت $\langle 0|$ با احتمال 0.5 ممکن است به حالت پذیرش برسیم. حال رشته "aa" را در نظر بگیرید:

$$M_a M_a |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{۶}$$

در این حالت با قطعیت به حالت پذیرش رسیدیم. بنابراین اگر آستانه را بزرگتر از 0.5 تعریف کنیم، رشته "a" در الفبا قرار نمی‌گیرد، اما رشته "aa" در الفبا خواهد بود. توجه کنید که این مسئله با خودکاره احتمالاتی تفاوت دارد. به طور خاص، اگر با دیدن یک حرف a و شروع از $\langle 0|$ می‌توان با احتمال بزرگتر از صفر به $\langle 0|$ رسید، بنابراین احتمال رسیدن به $\langle 0|$ برای دو حرف a نیز باید بیشتر از صفر باشد. اما می‌بینیم که در خودکاره کوانتومی به دلیل تداخل، این اتفاق نمی‌افتد و احتمال رسیدن به $\langle 0|$ با دو حرف a صفر است. به صورت کلی قدرت خودکاره‌های کوانتومی از خودکاره‌های احتمالاتی، قطعی و غیرقطعی کمتر است چرا که آن‌ها محدود به محاسبات معکوس‌پذیر هستند. البته اگر «اندازه‌گیری» را نیز به خودکاره کوانتومی اضافه کنیم، آنگاه می‌توانیم رفتار احتمالاتی را شبیه‌سازی کنیم و قدرت خودکاره کوانتومی حداقل به اندازه خودکاره احتمالاتی خواهد شد. یعنی، پس از یک گذر با استفاده از اندازه‌گیری به یک حالت خاص با یک احتمال مشخص منتقل شویم و در حالت برهم‌نهاده قرار نداشته باشیم. این مسئله باعث می‌شود که از تداخل جلوگیری شود.

ماشین تورینگ

ماشین‌های تورینگ خودکاره‌های متناهی هستند که یک نوار خواندن-نوشتن با اندازه بی‌نهایت هم در اختیار دارند. ماشین‌های تورینگ پس از خواندن یک حرف از روی نوار (که رشته ورودی در ابتدا بر روی آن نوشته می‌شود) می‌توانند علاوه بر تغییر حالت خودکاره محتوای نوار و وضعیت خود نسبت به آن را نیز تغییر دهند. به صورت خاص، فرض می‌شود که ماشین تورینگ یک اشاره‌گر دارد که در هر لحظه از زمان به یک نقطه خاص از نوار خواندن-نوشتن اشاره می‌کند. ماشین تورینگ می‌تواند کاراکتری که اشاره‌گر به آن اشاره می‌کند را بخواند، سپس می‌تواند محتوای آن خانه از نوار را با الفبای خود تغییر دهد و سپس اشاره‌گر را به سمت راست و یا چپ در نوار تغییر دهد. در نهایت ماشین تورینگ حالت خودکاره را تغییر می‌دهد. در ابتدا خودکاره ماشین تورینگ در حالت شروع اولیه قرار دارد و رشته ورودی بر روی نوار آن قرار گرفته است و اشاره‌گر آن به اولین حرف ورودی اشاره می‌کند. رشته ورودی مورد پذیرش قرار می‌گیرد اگر ماشین در یک حالت نهایی «توقف» کند.

این مدل انتزاعی تمام محاسبات قابل انجام را می‌تواند مدل‌سازی کند. یک روش استفاده کردن از این مدل به این ترتیب است که در ابتدا «صورت مسئله» و «پاسخ» را بر روی نوار می‌نویسیم و می‌خواهیم ببینیم که آیا آن پاسخ «درست» است یا خیر؟ یعنی در مورد مسئله تصمیم‌گیری کنیم. مجموعه تمام مسائلی که می‌توان با یک ماشین تورینگ در مورد وضعیت آن‌ها در زمان چندجمله‌ای تصمیم‌گیری کرد را با P نشان می‌دهند. در اینجا فرض شده است که خودکاره به صورت قطعی عمل می‌کند.

ماشین تورینگ غیرقطعی: اگر خودکاره مورد استفاده در ماشین تورینگ به صورت غیرقطعی عمل کند، یعنی به ازای هر حرف ورودی مجموعه‌ای از عمل‌ها امکان‌پذیر باشد آنگاه (مشابه خودکاره غیرقطعی) یک رشته ورودی مورد پذیرش قرار می‌گیرد اگر یک مسیر از حالت شروع به یک حالت پذیرش وجود داشته باشد که ماشین در آن توقف

کند. به مجموعه تمام مسائلی که طول یکی از مسیرهای آن‌ها از حالت شروع تا حالت توقف و پذیرش به صورت تابع چندجمله‌ای از اندازه ورودی مسئله باشد NP می‌گویند. توجه کنید که چون عملکرد ماشین تورینگ غیرقطعی است، اگر آن را به‌صورت قطعی دنبال کنیم، لزوماً پس از طی تعداد گام چندجمله‌ای به حالت پذیرش و توقف نمی‌رسیم. به همین دلیل $P \subseteq NP$ است.

ماشین تورینگ احتمالاتی: ماشین تورینگ احتمالاتی مانند ماشین تورینگ غیرقطعی است، با این تفاوت که از میان عملیات ممکن در هر حالت یکی از آن‌ها با یک احتمال مشخص انتخاب می‌شود (در واقع خودکاره آن‌ها از جنس خودکاره متناهی احتمالاتی است که قبلاً با آن آشنا شدیم). مشابه خودکاره متناهی احتمالاتی، در اینجا نیز پذیرش یک رشته ورودی (تصمیم‌گیری در مورد یک مسئله) را می‌توان از طریق یک آستانه احتمالاتی مشخص کرد. مثلاً، می‌توان گفت یک ماشین تورینگ احتمالاتی رشته‌هایی را می‌پذیرد که احتمال رسیدن از حالت شروع به حالت پذیرش با بررسی آن‌ها از $\frac{2}{3}$ بیشتر باشد (دقت کنید که این آستانه باید از 0.5 بیشتر باشد). در این شرایط، به تمام مسائلی که ماشین تورینگ احتمالاتی می‌تواند در زمان چندجمله‌ای به نسبت اندازه ورودی در مورد آن‌ها تصمیم‌گیری کند کلاس پیچیدگی BPP[۸] می‌گویند. به سادگی می‌توان ملاحظه کرد که گذارهای احتمالاتی حالت کلی‌تر گذارهای قطعی هستند و به این ترتیب $P \subseteq BPP$ است.

ماشین تورینگ کوانتومی: ماشین تورینگ کوانتومی از خودکاره‌های کوانتومی استفاده می‌کنند. در ماشین‌های کوانتومی (مشابه ماشین‌های تورینگ احتمالاتی) اگر پس از پردازش یک رشته احتمال توقف ماشین در حالت پذیرش بیش از یک آستانه از پیش تعیین‌شده باشد آن رشته مورد پذیرش قرار می‌گیرد. به مجموعه تمام مسائلی که می‌توان با استفاده از ماشین تورینگ کوانتومی در زمان چندجمله‌ای تصمیم‌گیری کرد کلاس پیچیدگی BQP[۹] می‌گویند. به خاطر بیاورید که از طریق «اندازه‌گیری» می‌توان به راحتی انتخاب‌های احتمالاتی را در خودکاره‌های کوانتومی شبیه‌سازی کرد و بنابراین می‌توان گفت که $BPP \subseteq BQP$ است.

رابطه کلاس‌های پیچیدگی

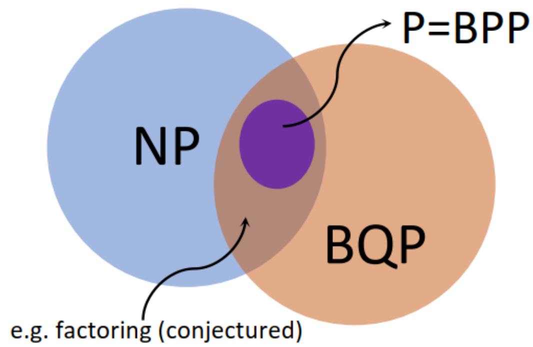
تا اینجا دیدم که روابط زیر برقرار هستند:

$$P \subseteq NP \tag{۷}$$

$$P \subseteq BPP \subseteq BQP. \tag{۸}$$

این روابط به نوعی قدرت نسبی مدل‌های محاسباتی متناظر را مشخص می‌کنند. یعنی، مثلاً، هر مسئله‌ای که در زمان چندجمله‌ای با استفاده از ماشین تورینگ قطعی بتوان در مورد آن تصمیم‌گیری کرد، می‌توان همان تصمیم را در زمان

[8] Bounded-error Probabilistic Polynomial-time
[9] Bounded-error Quantum Polynomial-time



شکل ۱: رابطه گرافیکی کلاس‌های پیچیدگی

چندجمله‌ای با استفاده از ماشین تورینگ کوانتومی نیز به‌دست آورد. اما، برعکس این ادعا لزوماً برقرار نیست. بنابراین ما علاقه‌مند هستیم که روابط این کلاس‌های پیچیدگی را به صورت دقیق‌تر و جزئی‌تر مشخص کنیم. در شکل ۱ رابطه کلاس‌های پیچیدگی به صورت نمودار ون نمایش داده شده است.

۱. یکی از مشهورترین سؤالات بی‌پاسخ علوم کامپیوتر این است که آیا $P = NP$ است یا خیر؟ یعنی آیا قدرت تصمیم‌گیری ماشین‌های تورینگ قطعی و غیرقطعی برابر است؟ بسیاری از تئورسین‌های حوزه علوم کامپیوتر اعتقاد دارند که این مسئله درست نیست و $P \neq NP$ برقرار است.

۲. حدس زده می‌شود که $P = BPP$ باشد، اما این مسئله اثبات نشده است.

۳. در مورد رابطه کلاس‌های NP و BPP دانشی نداریم. یعنی نمی‌دانیم یکی زیرمجموعه دیگری است و یا برعکس.

۴. با توجه به وجود الگوریتم Shor که مسئله تجزیه به عوامل اول را به صورت کارا حل می‌کند، اما الگوریتم کارای کلاسیکی (قطعی یا احتمالاتی) برای آن وجود ندارد، فعلاً اعتقاد بر این است که $BPP \neq BQP$. توجه کنید که حتی اگر $BPP \subseteq BQP$ برقرار باشد ولی $BPP \subsetneq BQP$ برقرار نباشد (یعنی این امکان وجود داشته باشد که بتوان در مورد تمام مسائل کلاس BQP به صورت احتمالاتی هم تصمیم‌گیری کرد) باز هم مطالعه و بررسی کامپیوترهای کوانتومی و الگوریتم‌های کوانتومی از نظر عملی برای ما مطلوب است. چرا که همچنان مثال‌هایی از الگوریتم‌هایی وجود دارند که به صورت کلاسیک در زمان فوق-چندجمله‌ای اجرا می‌شوند اما با استفاده از محاسبات کوانتومی قابل اجرا در زمان چندجمله‌ای هستند. به طور مثال اگر روزی هزار کیوبیت در اختیار داشته باشیم (که بتوانیم خطاهای آن‌ها را اصلاح کنیم) می‌توانیم مسئله تجزیه به عوامل اول را برای اعدادی حل کنیم که با استفاده از کامپیوترهای کلاسیک تا سال‌های بسیار دور قادر به حل آن‌ها نیستیم. حتی برخی متخصصان این مسئله اعتقاد دارند که یک تسریع چندجمله‌ای (مانند تسریع الگوریتم Grover) نیز وقتی

که پیشرفت کامپیوترهای کلاسیک خیلی کند و یا متوقف شود مطلوب خواهد بود. به طور خاص، پیشرفت کامپیوترهای کلاسیک را با قانون مور پیش‌بینی می‌کنند که حدس می‌زند توان محاسباتی حدود هر هجده ماه تقریباً دو برابر می‌شود. اما به نظر می‌رسد با کاهش ابعاد فیزیکی این قانون در آینده با چالش‌های جدی مواجه شود. به این ترتیب در این شرایط نه تنها تسریع‌های نمایی که تسریع‌های چندجمله‌ای کامپیوترهای کوانتومی به کار خواهند آمد و از نظر عملی توسعه آن‌ها توجیه پیدا می‌کند.

۵. اعتقاد عمومی این است که نمی‌توان مسائل خیلی سخت[10] را به صورت کارا با استفاده از ماشین تورینگ کوانتومی حل کرد. بنابراین $NP \nsubseteq BQP$ برقرار است. اما به نظر می‌رسد مسائلی وجود دارند که از کلاس NP خارج هستند اما در کلاس BQP قرار می‌گیرند. به همین دلیل حدس زده می‌شود که $BQP \nsubseteq NP$.

[10] NP-complete