نظریهٔ محاساباتِ کوانتومی

سید سجاد کاهانی

۲ اسفند ۱۳۹۸

۱ ماشین تورینگ کوانتومی

یک ماشینِ تورینگِ معمولی را تصور کنید، نوارِ این ماشینِ تورینگ می‌تواند حالت‌های بی‌شماری به خود بگیرد. هر حالتی را که (در زمانِ متناهی) می‌تواند برروی نوار ایجاد شود، می‌توان با تابعی به شکلِ $T : \mathbb{Z} \to \Sigma$ نشان داد، به شرطی که تعدادِ mهایی که $T(m) \neq b$ محدود باشد.

تعریف ۱

$$T \;\; is \;\; valid :\equiv \{m \,|\, T(m) \neq b\} \;\; is \;\; a \;\; finite \;\; set \tag{۱}$$

تعریف ۲ اگر T یک تابعِ معتبر ($valid$) باشد

$$T^{x\to s}(\xi) := \begin{cases} s & \xi = x \\ T(\xi) & \xi \neq x \end{cases} \tag{۲}$$

تعریف ۳ مجموعهٔ حالت‌هایی که نوار می‌تواند به خود بگیرد را با $\Sigma^{\#}$ نشان می‌دهیم و به این شکل تعریف می‌کنیم.

$$\Sigma^{\#} := \{T : \mathbb{Z} \to \Sigma \,|\, T \;\; is \;\; valid\} \tag{۳}$$

اما حالتِ فیزیکیِ یک ماشینِ کوانتومی به حالتِ نوارش محدود نمی‌شود، این‌که محلِ سرِ ماشین در کجای نوار است، یک پارامتر $\xi \in \mathbb{Z}$ است و همچنین، سرِ ماشین نیز حالتی از مجموعهٔ Q را به خود می‌گیرد.

تعریف ۴ حالتِ کلیِ یک ماشینِ تورینگ را تعریف می‌کنیم

$$\mathcal{C} := (q, T, \xi) \in Q \times \Sigma^{\#} \times \mathbb{Z} \tag{۴}$$

حال، برای یک ماشین تورینگ معمولی، می‌دانیم تحولِ آن با یک تابع گذار به شکلِ زیر مشخص می‌شود

$$\delta_{\text{classical}} : Q \times \Sigma \to Q \times \Sigma \times \{-1, +1\}$$

تعریف ۵ اگر بگیریم

$$\delta_{\text{classical}}(q, s) = (q', s', d)$$

می‌شود تابعِ گذار را به این شکل تعمیم داد

$$\Delta_{\text{classical}} : \mathcal{C} \to \mathcal{C}$$

$$\Delta_{\text{classical}}(q, T, \xi) := (q', T^{\xi \to s'}, \xi + d) \tag{۵}$$

در یک ماشینِ تورینگِ کوانتومی، منطقی‌ست اگر فرض کنیم در هر لحظه، ماشین در یک فضای هیلبرتی حضور دارد که پایه‌های آن $|c\rangle$ است برای $c \in \mathcal{C}$.

در این صورت، تحول‌های ماشین باید با تبدیل‌های یکانی در فضای $\mathcal{H}(\mathcal{C})$ باشند. پس برای ماشین کوانتومی تقاضا داریم

$$\Delta_{\text{quantum}} : L(\mathcal{H})$$

و

$$\Delta_{\text{quantum}}\Delta^{\dagger}_{\text{quantum}} = I$$

حالا قابلِ حدس است که اگر بگیریم

$$\delta_{\text{quantum}} : Q \times \Sigma \times Q \times \Sigma \times \{-1,+1\} \to \mathbb{C}$$

آنگاه

$$\Delta_{\text{quantum}} = \sum_{(q,T,\xi)\in\mathcal{C}} \sum_{q',s',d} \delta_{\text{quantum}}(q,s,q',s',d) \left|q', T^{\xi\to s'}, \xi+d\right\rangle \langle q,T,\xi|$$

پس $(Q,\Sigma,\delta_{quantum})$ یک ماشین تورینگ کوانتومی‌ست.
اما نکتهٔ مهمی در این میان وجود دارد که اگر محدودیتی روی مقادیری که تابعِ δ می‌تواند به خود بگیرد نگذاریم، این ماشین قادر خواهدبود هر تبدیلِ دلخواهی را در فضای محدود (مثلاً دوکیوبیتی) با خطای صفر و در مراحلِ محدود $\mathcal{O}(1)$ انجام دهد و به این طریق، از مجموعهٔ مدارِ جهانی‌که تعریف کرده‌ایم، قوی‌تر خواهد بود. (که تبدیل دلخواه را با خطای ϵ در $\mathcal{O}(\log\frac{1}{\epsilon})$ مرحله انجام می‌دهد.

تمرین

- ثابت کنید این ماشین می‌تواند عملگر دلخواهِ دوکیوبیتی را در زمانِ محدود، به دقت شبیه‌سازی کند.

برای همین در تعریف‌های رسمی‌تر مقادیرِ این تابع را به مجموعهٔ محدودی مانند $\{0,\pm1,\pm i,\pm\frac{1}{\sqrt{2}},\pm\frac{i}{\sqrt{2}}\}$ یا مجموعهٔ همهٔ اعدادِ محاسبه پذیر محدود می‌شود.[۱]

تمرین

- چه شرطی برروی δ لازم است تا Δ یکانی شود؟

۲ پذیرش زبان

اگر حالتِ اولیهٔ ماشین به این شکل باشد که در آن l ورودی‌ایست که می‌خواهیم آن را تشخیص دهیم.

$$|\psi_l\rangle := (q_0, l, 0)$$

قابلِ درک است که اندازه‌گیری متعامد وجود دارد که مشخص می‌کند

۱. A: کار ماشین تمام شده و ورودی پذیرفته شده.

۲. R: کار ماشین تمام شده و ورودی رد شده.

۳. N: کار ماشین تمام نشده.

که هرکدام از A و R و N یک عملگرِ تصویر هستند و $A + R + N = 1$

تعریف ۶ تعریف می‌کنیم ماشینِ تورینگِ کوانتومیِ (Q, Σ, δ) ورودی l را با احتمال p در زمان t می‌پذیرد، اگر

$$| \langle \phi_l | \Delta^{-t} A \Delta^{t} | \phi_l \rangle |^2 = p$$

و به طور مشابه، رد کردن را نیز تعریف می‌کنیم.

تعریف ۷ یک زبان عضو کلاس $\mathcal{EQP}$ است اگر ماشین تورینگ کوانتومی در زمانِ چندجمله‌ای هر کلمه از آن زبان با احتمال 1 بپذیرد و هرکلمه خارج از زبان را با احتمال 1 رد کند.

تعریف ۸ یک زبان عضو کلاس $\mathcal{BQP}$ است ااگر ماشین تورینگ کوانتومی در زمانِ چندجمله‌ای هر کلمه از آن زبان با احتمال $2/3$ بپذیرد و با احتمال $1/3$ رد کند. همچنین هر کلمه خارج از زبان را نیز با احتمال $2/3$ رد کند و با احتمال $1/3$ بپذیرد.

[۲]

تمرین

- می‌توانید نشان دهید یک ماشین تورینگ معمولی با یک تورینگ ماشین کوانتومی قابل شبیه‌سازی است. این شبیه‌سازی فضا یا زمانِ بیشتری می‌خواهد؟
- آیا می‌توان هر مدار کوانتومی را با ماشین تورینگ شبیه‌سازی کرد؟ پیچیدگیِ این شبیه‌سازی چقدر خواهد بود؟ (راهنمایی: دو گیتِ H و CNOT را شبیه‌سازی کنید.)

۳ مدار تورینگ کوانتومی

می‌خواهیم مداری هم‌ارزِ یک ماشینِ تورینگِ کوانتومی برای nمرحله بسازیم. یک ماشین در nمرحله حداکثر خانه‌های در بازهٔ $\{-n, \ldots, 0, \ldots, +n\}$ را تغییر می‌دهد.

اگر به ازای هر خانهٔ نوار تعریف کنیم $|t_m\rangle$ علامتی که برروی خانهٔ mاِم نوار نوشته شده و آن را به این شکل مقداردهیِ اولیه کنیم

$$|t_m\rangle := |b\rangle$$

و تعریف می‌کنیم

$$\mathcal{T} := \mathcal{H}(\Sigma) \Rightarrow |t_m\rangle \in \mathcal{T}$$

همچنین، یک کیودیت دیگر به ازای هر خانهٔ نوار تعریف می‌کنیم به نامِ $|s_m\rangle$ که برابرِ $|0\rangle$ است، اگر نشانه‌گرِ سر روی خانهٔ mام نباشد ($m \neq \xi$) و اگر باشد این کیودیت برابرِ $|q\rangle$ خواهدبود. پس آن را به این شکلِ مقداردهیِ اولیه می‌کنیم

$$|s_m\rangle := \begin{cases} |0\rangle & m \neq 0 \\ |q_0\rangle & m = 0 \end{cases}$$

و به طورِ مشابه

$$\mathcal{S} := \mathcal{H}(Q + \{0\}) \Rightarrow |s_m\rangle \in \mathcal{S}$$

به ازای هر خانه یک کیوبیت کمکی به نامِ $|r_m\rangle$ نیز تعریف می‌کنیم

$$\mathcal{R} := \mathcal{H}(\{0,1\}) \Rightarrow |r_m\rangle \in \mathcal{R}$$

حالا تحولِ G را برروی سه خانهٔ مجاورِ نوار، $\mathcal{T} \otimes \mathcal{S} \otimes \mathcal{R} \otimes \mathcal{T} \otimes \mathcal{S} \otimes \mathcal{R} \otimes \mathcal{T} \otimes \mathcal{S} \otimes \mathcal{R}$ به این شکل تعریف می‌کنیم

$$\begin{cases} G\,|t_{m-1}\,0\,0\,t_m\,q\,0\,t_{m+1}\,0\,0\rangle & = \sum_{q',s'} \delta_{\text{quantum}}(q,m,q',s',+1)\,|t_{m-1} 0\,0\,s'\,0\,0\,t_{m+1}\,q'\,1\rangle \\ & \quad + \sum_{q',s'} \delta_{\text{quantum}}(q,m,q',s',-1)\,|t_{m-1}\,q'\,1\,s'\,0\,0\,t_{m+1}\,0\,0\rangle \\ G\,|t_{m-1}\,s_{m-1}\,1\,t_m\,s_m\,0\,t_{m+1}\,s_{m+1}\,0\rangle & = |t_{m-1}\,s_{m-1}\,1\,t_m\,s_m\,0\,t_{m+1}\,s_{m+1}\,0\rangle \\ G\,|t_{m-1}\,s_{m-1}\,0\,t_m\,s_m\,0\,t_{m+1}\,s_{m+1}\,1\rangle & = |t_{m-1}\,s_{m-1}\,0\,t_m\,s_m\,0\,t_{m+1}\,s_{m+1}\,1\rangle \\ G\,|t_{m-1}\,s_{m-1}\,0\,t_m\,s_m\,1\,t_{m+1}\,s_{m+1}\,0\rangle & = |t_{m-1}\,s_{m-1}\,0\,t_m\,s_m\,0\,t_{m+1}\,s_{m+1}\,0\rangle \end{cases}$$

[۳]

تمرین

- ثابت کنید G می‌تواند یک تبدیلِ یکانی باشد.
- اگر ضمانت دهیم که δ می‌تواند تنها مقادیرِ $\{0, \pm 1, \pm i, \pm\frac{1}{\sqrt{2}}, \pm\frac{i}{\sqrt{2}}\}$ را به خود بگیرد، آیا می‌توانید ثابت کنید که مدارِ آن با گیت‌های معمول قابلِ ساختن است؟

References

[1] Ethan Bernstein and Umesh Vazirani. "Quantum complexity theory". In: *SIAM Journal on computing* 26.5 (1997), pp. 1411–1473.

[2] Christian Westergaard. "Computational equivalence between quantum Turing machines and quantum circuit families". MA thesis. University of Copenhagen, Denmark, 2005.

[3] A Chi-Chih Yao. "Quantum circuit complexity". In: *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. IEEE. 1993, pp. 352–361.