درس نهم : مسئله زیرگروه های پنهان

۱ مقدمه

دراین درس می خواهیم نشان دهیم که تمامی مسئله هایی که تا کنون حل کرده ایم در یک چارچوب واحد قابل صورت بندی هستند و همه آنها را می توان به عنوان مثالهایی از یک مسئله کلی تر موسوم به مسئله زیر گروه های پنهان فهمید. خواننده‌ای که با نظریه گروه آشنایی ندارد می تواند به ضمیمه این درس مراجعه کند. کسی که طالب فهم وسیع تر و عمیق تری از این مطالب است می بایست به یک کتاب نظریه گروه و یا به درسنامه نظریه گروه مراجعه کند.

۲ مسئله زیرگروه های پنهان

نخست مسئله زیر گروه های پنهان را معرفی می کنیم.

تعریف مسئله زیرگروه های پنهان: فرض کنید که G یک گروه متناهی (درحالت کلی غیرآبلی) و H زیرگروهی از G است. $f : G \longrightarrow X$ یک تابع است که به صورت $|g, y\rangle \longrightarrow |g, f(g)\oplus y\rangle$ روی حالت ها عمل می کند. این تابع دارای این خاصیت است که روی هم مجموعه های H مقدارش ثابت است، شکل ??. می خواهیم با چند بارخواندن تابع مجموعه مولدهای H را تشخیص دهیم.

قبل از آنکه نشان دهیم چرا مسایل متفاوتی که تا کنون حل کرده ایم همه حالت های خاصی از این مسئله هستند، نشان می دهیم که چگونه می توان برای گروه های آبلی این مسئله را با آلگوریتم های کوانتومی حل کرد.

۱.۲ حل مسئله زیر گروه های پنهان برای گروه های آبلی با آلگوریتم های کوانتومی

مرحله اول یک ترکیب خطی از همه حالت ها به شکل زیرتهیه می کنیم:

$$|\Psi_0\rangle := |0,0,0\rangle = \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle. \tag{1}$$

مرحله دوم تابع را فرامی خوانیم

$$|\Psi^0\rangle \longrightarrow |\Psi^1\rangle = \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g, f(g)\rangle. \tag{2}$$

مرحله سوم ثبت کننده دوم را اندازه می گیریم . فرض کنید که دراین اندازه گیری مقدار $f(g_0)$ را بدست آوردیم. دراین صورت ثبت کننده اول به حالت زیرافکنده می شود:

$$|\Phi\rangle = \frac{1}{|H|}\sum_{h\in H}|g_0 h\rangle. \tag{3}$$

برای گروه های آبلی نماد زیر را بکارمی بریم

$$|\Phi\rangle = \frac{1}{|H|}\sum_{h\in H}|g_0 + h\rangle. \tag{4}$$

مرحله چهارم: روی ثبت کننده اول تبدیل فوریه انجام می دهیم دراین قسمت ازآبلی بودن گروه استفاده اساسی می کنیم.

$$\begin{aligned} |\Phi\rangle &= \frac{1}{\sqrt{|H||G|}}\sum_{h\in H,\mu}\rho^{\mu}(g_0+h)|\mu\rangle \\ &= \frac{1}{\sqrt{|H||G|}}\sum_{h\in H,\mu}\rho^{\mu}(g_0)\rho^{\mu}(h)|\mu\rangle \\ &= \frac{1}{\sqrt{|H||G|}}\sum_{h\in H,\mu}e^{\frac{2\pi i\mu g_0}{|G|}}e^{\frac{2\pi i\mu h}{|G|}}|\mu\rangle. \end{aligned} \tag{5}$$

احتمال یافتن مقدار μ برابراست با

$$P(\mu) = \frac{1}{|H||G|}\mid\sum_{h\in H}e^{\frac{2\pi i\mu h}{|G|}}\mid^2 . \tag{6}$$

تنهاآن مقدارهای μ احتمال یافتن شان قابل ملاحظه است که $\frac{\mu h}{|G|}$ یک مقدارصحیح باشد. به عبارت دیگر

$$\mu = \frac{m|G|}{h} \qquad \text{یا} \qquad \frac{\mu}{|G|} = \frac{m}{h}. \tag{7}$$

ازاین رابطه آخری می توانیم مقادیر h و درنتیجه مولدهای H را بیابیم.

به یک نکته باید دقت کنیم وآن اینکه μ و $|G|$ ممکن است نسبت به هم اول نباشند. اما می دانیم که هر گروه آبلی که تعداد مولد های آن محدود باشد ساختمان اش عبارت است از

$$G = Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times Z_{p_3^{\alpha_3}} \times \cdots Z_{p_m^{\alpha_m}}. \tag{8}$$

درنتیجه خواهیم داشت

$$e^{\frac{2\pi i\mu h}{|G|}} = \prod_{i=1}^{M} e^{\frac{2\pi i l'_i h_i}{p_i^{\alpha_i}}}. \tag{9}$$

۳ مثال هایی از مسئله زیرگروه پنهان

۱.۳ مسئله دویچ

دراین مسئله گروه G عبارت است از گروه Z_2. تابع $f : Z_2 \longrightarrow R$ داده شده است. G دوزیرگروه دارد یکی $H_0 = \{0\}$ و دیگری $H_1 = \{0, 1\}$. هم مجموعه های H_0 عبارتند از $\{0\}, \{1\}$. هم مجموعه های H_1 عبارتنداز $\{0, 1\}$. اگر زیرگروه مورد نظر، H_0 باشد آنگاه تابع متوازن است. اگر زیرگروه مورد نظر، H_1 باشد آنگاه تابع ثابت است. بنابراین توانسته ایم مسئله دویچ را به صورت حالت خاصی از مسئله زیرگروه های پنهان معرفی کنیم.

۲.۳ مسئله سایمون

دراین مسئله گروه G عبارت است از $Z_2^{\times n}$ و $f : Z_2^{\times n} :\longrightarrow Z_2^{\times n}$. زیرگروه H عبارت است از

$$H = \{0, a\} \tag{10}$$

که درآن a یک عنصردلخواه است. می دانیم که $a + a = 0$. بنابراین H یک زیرگروه است. هم مجموعه های H به شکل زیرهستند:

$$[x] = x + H = \{x, x + a\}. \tag{11}$$

تابع f روی این هم مجموعه ها ثابت است ومی خواهیم با خواندن تابع زیرگروه H یا a راپیداکنیم.

۳.۳ پیداکردن دوره تناوب توابع

دراینجا گروه G عبارت است از $G = Z_N = Z_{2^n}$. تابع f به شکل زیرتعریف شده است $f : Z_N \longrightarrow X$ که درآن X هرمجموعه متناهی است که تعداد اعضای آن از N کمتراست. دراین جا زیرگروه H عبارت است از $H = rZ = \{0, r, 2r, \cdots\}$. متناوب بودن تابع f به این معناست که تابع f روی هم مجموعه های H ثابت است.

۴.۳ لگاریتم گسسته

نخست مسئله لگاریتم گسسته را معرفی می کنیم. سه عدد b ، a و N داده شده اند. کوچکترین عدد s را چنان پیدا کنید که درشرط $b = a^s \quad mod \quad N$ صدق کند. می خواهیم این مسئله را به صورت حالت خاصی از مسئله زیرگروه های پنهان بررسی

کنیم. تابع $f(x,y)$ را به شکل زیرتعریف می کنیم:

$$f(x,y) := a^x b^y \tag{12}$$

فرض کنید که این تابع متناوب باشد، یعنی

$$f(x+k, y+l) = f(x,y), \tag{13}$$

ویا

$$a^{x+k}b^{y+l} = a^x b^y \quad \longrightarrow \quad a^k b^l = 1, \quad \longrightarrow \quad k = -ls. \tag{14}$$

بنابراین تابع f دارای این خاصیت است که

$$f(x,y) = f(x-ls, y+l) \tag{15}$$

که ازآن نتیجه می گیریم $(-ls, l)$ دوره تناوب این تابع است. حال که مسئله لگاریتم گسسته را به صورت مسئله پیداکردن دوره تناوب بازنویسی کرده ایم می توانیم آن رابه صورت حالت خاصی از مسئله زیرگروه های پنهان صورت بندی کنیم. گروه G را $Z_{2^m} \times Z_{2^n}$ می گیریم. H را زیرگروهی می گیریم که توسط $\{(-s,1)\}$ تولید می شود. دراین صورت f روی هم مجموعه های این زیرگروه یعنی روی مجموعه هایی به صورت

$$\{(x,y), (x-s, y+1), (x-2s, y+2), \cdots\} \tag{16}$$

ثابت است. بنابراین مسئله زیرگروه پنهان لگاریتم گسسته را به صورت حالت خاص نیز دربرمی گیرد.