پردازش اطلاعات کوانتومی

پاییز ۱۴۰۱

ارائه ۱۲

دکتر احمد خونساری

۱ مقدمه

در این ارائه به الگوریتم Shor می‌پردازیم.

۲ یافتن دوره تناوب

پیش از اینکه به الگوریتم Shor بپردازیم به مفهوم تابع تناوبی و یافتن دوره تناوب می‌پردازیم. تابع زیر را در نظر بگیرید:

$$f(x) = a^x \mod N. \tag{۱}$$

فرض کنید که a و N هر دو اعداد صحیح مثبت هستند و $N < a$ است. ضمناً فرض می‌کنیم که a و N مقسوم‌الیه مشترک بزرگتر از یک ندارند. دقت کنید که $f(x)$ یکی از اعداد 0 تا $N-1$ است اما x به صورت دلخواه می‌تواند بزرگ شود. بنابراین قابل انتظار است که تابع $f(x)$ در یک نقطه شروع به تکرار خود کند و بنابراین می‌شود ادعا کرد که این تابع تناوبی است. دوره تناوب این تابع را با r نمایش می‌دهیم و آن را به صورت زیر تعریف می‌کنیم. دوره تناوب تابع $f(x)$ کوچکترین عدد صحیح غیرصفر است که به ازای آن عبارت زیر برقرار شود:

$$a^r \mod N = 1. \tag{۲}$$

مثال: فرض کنید $a = 3$ و $N = 7$ باشد. جدول ۱ مقادیر مختلف تابع $f(x)$ به ازای مقادیر افزایشی x را نشان می‌دهد. ملاحظه می‌کنید که به ازای $x = 6$ حاصل تابع برابر یک می‌شود و بنابراین دوره تناوب تابع برابر شش است. □

یافتن دوره تناوب $f(x)$ در حالت کلی مسئله بسیار سختی است. ایده Shor برای یافتن این مقدار استفاده از «تخمین فاز کوانتومی» است که در ارائه قبلی با آن آشنا شدیم. به یاد بیاورید که اگر $|\psi\rangle$ بردار ویژه عملگر یکانی U باشد، با استفاده از تخمین فاز می‌توان مقدار θ در مقدار ویژه $e^{2i\pi\theta}$ را تخمین زد. فرض کنید U یک عملگر یکانی باشد که به صورت زیر عمل می‌کند:

$$U|y\rangle = |ay \mod N\rangle. \tag{۳}$$

جدول ۱: تناوبی بودن تابع $f(x)$

x	$f(x)$
1	$3^1 \mod 7 = 3$
2	$3^2 \mod 7 = 2$
3	$3^3 \mod 7 = 6$
4	$3^4 \mod 7 = 4$
5	$3^5 \mod 7 = 5$
6	$3^6 \mod 7 = 1$
7	$3^7 \mod 7 = 3$
8	$3^8 \mod 7 = 2$
9	$3^9 \mod 7 = 6$
10	$3^{10} \mod 7 = 4$
$\vdots$	$\vdots$

به دو نکته توجه کنید:

۱. اگر عملگر U را r مرتبه بر روی $|1\rangle$ اعمال کنیم آنگاه خروجی همان $|1\rangle$ می‌شود:

$$U^r|1\rangle = |1\rangle. \tag{۴}$$

۲. حالت زیر یک بردار ویژه عملگر U است:

$$|u_0\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |a^k \mod N\rangle. \tag{۵}$$

برای آنکه دلیل این مطلب را متوجه شوید دقت کنید جمع فوق شامل $|1\rangle$ و تمام حالت‌های ممکنی است که از اعمال چندباره عملگر U بر روی $|1\rangle$ بدست می‌آیند. به این ترتیب اگر U به $|u_0\rangle$ اعمال شود دوباره تمام حالت‌های ممکن فوق تولید می‌شوند و حالت تغییر نمی‌کند.

اما مقدار ویژه بردار $|u_0\rangle$ برابر عدد یک است. به این ترتیب نمی‌توان اطلاعات زیادی را استخراج کرد و تخمین‌زدن آن کمکی به ما نمی‌کند. بنابراین سعی می‌کنیم آن را طوری تغییر دهیم که مقدار ویژه متناظر آن حاوی اطلاعاتی از دوره تناوب باشد. فرض کنید بتوانیم حالت زیر را ایجاد کنیم:

$$|u_1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2ik\pi}{r}} |a^k \mod N\rangle. \tag{۶}$$

اگر عملگر U را بر این حالت اعمال کنیم به نتیجه زیر می‌رسیم:

$$U|u_1\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2ik\pi}{r}} U|a^k \mod N\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2ik\pi}{r}} |a^{k+1} \mod N\rangle \tag{۷}$$

$$= \frac{e^{\frac{2i\pi}{r}}}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2i(k+1)\pi}{r}} |a^{k+1} \mod N\rangle = \frac{e^{\frac{2i\pi}{r}}}{\sqrt{r}}\sum_{k=1}^{r} e^{-\frac{2ik\pi}{r}} |a^{k} \mod N\rangle \tag{۸}$$

$$= \frac{e^{\frac{2i\pi}{r}}}{\sqrt{r}}\left(e^{-\frac{2ir\pi}{r}}|a^r \mod N\rangle + \sum_{k=1}^{r-1} e^{-\frac{2ik\pi}{r}} |a^{k} \mod N\rangle\right) \tag{۹}$$

$$= \frac{e^{\frac{2i\pi}{r}}}{\sqrt{r}}\left(|1\rangle + \sum_{k=1}^{r-1} e^{-\frac{2ik\pi}{r}} |a^{k} \mod N\rangle\right) = \frac{e^{\frac{2i\pi}{r}}}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2ik\pi}{r}} |a^{k} \mod N\rangle \tag{۱۰}$$

$$= e^{\frac{2i\pi}{r}}|u_1\rangle. \tag{۱۱}$$

نکته‌ای که در این محاسبات باید به خاطر داشته باشید این است که:

$$e^{\frac{-2i\pi\times 0}{r}} = e^{\frac{-2i\pi\times r}{r}} = 1 \tag{۱۲}$$

$$|a^0 \mod N\rangle = |a^r \mod N\rangle = |1\rangle. \tag{۱۳}$$

این بار می‌بینیم که مقدار ویژه حاوی اطلاعاتی در مورد r است. دقت کنید که به راحتی می‌توانیم عبارات فوق را با افزودن یک عدد صحیح در توان ضرایب حالت‌های پایه گسترش دهیم. به صورت خاص می‌توان به راحتی ملاحظه کرد که معادلات زیر به ازای هر مقدار عدد صحیح s برقرار هستند:

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2isk\pi}{r}} |a^k \mod N\rangle, \tag{۱۴}$$

$$U|u_s\rangle = e^{\frac{2is\pi}{r}}|u_s\rangle. \tag{۱۵}$$

دقت کنید که به ازای $0 \le s \le r-1$ ما s بردار «متفاوت» بدست می‌آوریم (N ریشه متمایز عدد یک در ارائه قبل را به خاطر بیاورید) که اطلاعات دوره تناوب را برای ما می‌توانند استخراج کنند. این تعریف ممکن است خیلی ناگهانی به نظر برسد، اما در حقیقت به صورت ساده‌ای از ویژگی‌های تبدیل فوریه کوانتومی قابل حصول است. به این منظور به دو ویژگی «معکوس کردن دوره تناوب» و «تبدیل جابه‌جاسازی [1] به فاز» که در منابع کمکی معرفی می‌شود توجه کنید. حال به این نکته دقت کنید که به جز زمانی که $k=0$ است، به ازای هر k مقادیر مختلف s باعث می‌شوند که $|a^k \mod N\rangle$ حول مبدأ دوران پیدا کند. در واقع مقادیر مختلف s باعث می‌شوند که این بردارها با فاصله مساوی از هم بر روی دایره واحد توزیع شوند و به این ترتیب اگر آنها را جمع کنیم همگی یکدیگر را خنثی می‌کنند و فقط $|a^0$

[1] Offset

$\bmod N\rangle$ها باقی می‌مانند. به صورت خاص می‌توان نوشت:

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle. \quad (۱۶)$$

بنابراین می‌توان گفت که حاصل برهم‌نهی بردارهای $|u_s\rangle$ برابر بردار $|1\rangle$ است و توجه کنیم که مقدار ویژه تمام این بردارها برابر $e^{\frac{2is\pi}{r}}$ است. بنابراین اگر ما سعی کنیم مقدار ویژه عملگر U به ازای بردار ویژه $|1\rangle$ را تخمین بزنیم می‌توانیم مقدار $\frac{s}{r}$ را به ازای $0 \leq s \leq r-1$ بدست بیاوریم. روش‌های کارامد کلاسیکی وجود دارند که می‌توانند مقدار r را از طریق مشاهده نتایج اندازه‌گیری بدست آورند. در این روش از مفهوم کسر مسلسل [۲] استفاده می‌شود.

۱.۲ شبیه‌سازی

به عنوان مثال شبیه‌سازی تابع زیر را در نظر می‌گیریم:

$$f(x) = 2^x \mod 5. \quad (۱۷)$$

بنابراین $a = 2$ و $N = 5$ است. می‌توان لاحظه کرد که چهار دوره تناوب این تابع است. در گام اول باید بتوانیم مدار یکانی را طراحی کنیم که بتواند عملیات زیر را انجام دهد:

$$U|y\rangle = |2 \times y \mod 5\rangle \quad (۱۸)$$

و به خاطر داشته باشید که ما عملیات را با بردار ویژه $|1\rangle$ شروع می‌کنیم. بنابراین باید تبدیل‌های زیر بوسیله مدار ایجاد شود:

$$U|1\rangle = |2 \times 1 \mod 5\rangle = |2\rangle \quad (۱۹)$$

$$U|2\rangle = |2 \times 2 \mod 5\rangle = |4\rangle \quad (۲۰)$$

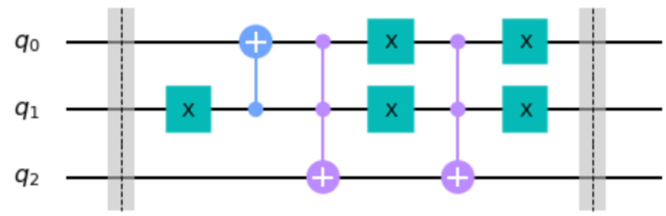
$$U|4\rangle = |2 \times 4 \mod 5\rangle = |3\rangle \quad (۲۱)$$

$$U|3\rangle = |2 \times 3 \mod 5\rangle = |1\rangle. \quad (۲۲)$$

توجه کنید که مدار شکل ۱ این کار را انجام می‌دهد. آیا می‌توانید آن را بررسی کنید؟ برای اینکه شبیه‌سازی را شروع کنیم ابتدا کتابخانه‌های مورد نیاز را وارد می‌کنیم:

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import pi
```

[2] Continued fraction



شکل ۱: مدار $U|y\rangle = |2 \times y \mod 5\rangle$

```
from qiskit import QuantumCircuit, Aer, execute
from qiskit.visualization import plot_histogram
from math import gcd
from numpy.random import randint
import pandas as pd
from fractions import Fraction
```

به خاطر بیاورید که برای محاسبه فاز ما تعدادی کیوبیت را برای تخمین تخصیص می‌دهیم. سپس به ازای کیوبیت j-ام مدار یکانی را 2^{j-1} بار اعمال می‌کنیم (ارائه قبلی را ببینید). به این منظور یک تابع می‌نویسیم که یک مقدار «توان» دریافت می‌کند و یک مدار «کنترل‌شده» می‌سازد که به تعداد توان مدار U را اعمال می‌کند:

```
def c_2power_mod5(power):
    U = QuantumCircuit(3)
    for iteration in range(power):
        U.x(1)
        U.cx(1, 2)
        U.ccx(2, 1, 0)
        U.x(2)
        U.x(1)
        U.ccx(2, 1, 0)
        U.x(2)
        U.x(1)
    U = U.to_gate()
    U.name = "[2^%i mod 5]" %power
    c_U = U.control()
    return c_U
```

سپس مدار تخمین فاز را به صورت زیر می‌سازیم:

```
n_count = 4
qc = QuantumCircuit(n_count + 3, n_count)
for q in range(n_count):
    qc.h(q)
```

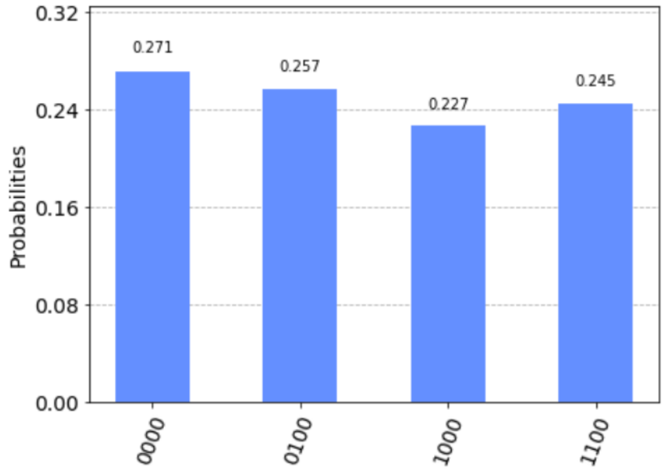
```
qc.x(n_count + 3 - 1)
for q in range(n_count):
    qc.append(c_2power_mod5(2**q), [q] + [i+n_count for i in range(3)])
qc = add_qft_inv(qc, n_count, use_barrier=False)
qc.barrier()
qc.measure(range(n_count), range(n_count))
```

در این کد از «چهار کیوبیت» برای تخمین فاز استفاده شده است. «سه» کیوبیت هم برای ورودی بردار ویژه $|1\rangle$ در نظر گرفته شده است. سپس به تمام کیوبیت‌های متناظر مقدار تخمین فاز یک دریچه هادامارد اعمال شده است. سپس کیوبیت آخر NOT شده است تا ورودی $|1\rangle$ برای مدارها را درست کند. سپس هر کیوبیت تخمین به عنوان کیوبیت کنترلی به مدار U اعمال می‌شود. به صورت خاص کیوبیت شماره q به تعداد 2^q بار مورد استفاده قرار می‌گیرد. توجه کنید این مسئله ممکن است نگرانی‌هایی در مورد پیاده‌سازی چندجمله‌ای ایجاد کند. مدار $U^{2^j}|y\rangle = |a^{2^j}y \mod N\rangle$ نیاز به محاسبه $a^{2^j}y \mod N$ دارد. روش‌های کلاسیک کارامدی (به نام repeated squaring) برای محاسبه این مقدار وجود دارد. پیاده‌سازی این روش به صورت کوانتومی با چالش‌هایی روبروست که در اینجا به آنها نمی‌پردازیم. سپس از تابع تولید مدار تبدیل معکوس فوریه که در ارائه قبلی معرفی شده استفاده کرده‌ایم. در نهایت نیز کیوبیت‌های تخمین اندازه‌گیری شده‌اند. به خاطر داشته باشید که فاز نهایی به صورت $\frac{r}{s} \times 2^4$ مشاهده می‌شود که ضریب 2^4 به دلیل استفاده از چهار کیوبیت تخمین است. شکل مدار در پیوست آمده است. اگر این مدار را به شکل زیر شبیه‌سازی کنیم به نتایج شکل ۲ می‌رسیم.

```
backend = Aer.get_backend('qasm_simulator')
results = execute(qc, backend, shots=1000).result()
counts = results.get_counts()
plot_histogram(counts)
```

می‌بینیم که خروجی‌های 0، 4، 8 12 تقریباً به صورت برابر مشاهده شده‌اند. اگر این اعداد را بر $2^4 = 16$ تقسیم کنیم به مقادیر 0، 0.25، 0.5 0.75 می‌رسیم. حال باید سعی کنیم کوچکترین r را تخمین بزنیم که حاصل $\frac{s}{r}$ برای $0 \leq s \leq r-1$ به کسرهای مشاهده‌شده نزدیک باشد. با استفاده از قطعه کد زیر می‌توان فازها را از طریق کتابخانه‌های پایتون پردازش کرد و r را بدست آورد:

```
measured_phases = []
for output in counts:
    decimal = int(output, 2)
    phase = decimal/(2**n_count)
    measured_phases.append(phase)
denominators = {}
for phase in measured_phases:
    frac = Fraction(phase).limit_denominator(5)
```



شکل ۲

```
    if frac.denominator not in denominators:
        denominators[frac.denominator] = 1
    else:
        denominators[frac.denominator] += 1
print(denominators)
```

با اجرای کد فوق مقدار $r = 1$ یکبار، $r = 4$ دو مرتبه و $r = 2$ یکبار محاسبه می‌شود. می‌بینیم که دوره تناوب اصلی که چهار است بیشتر به داده‌ها نزدیک است و امکان حدس زدن آن بوجود می‌آید.

۳ تجزیه به عوامل اول

حال که تا حد خوبی با یافتن دوره تناوب آشنا شدیم به بحث تجزیه اعداد به عوامل اول می‌پردازیم. سخت‌ترین و جالب‌ترین حالت مسئله تجزیه به عوامل اول وقتی است که عدد مد نظر حاصل ضرب دو عدد اول نزدیک به هم باشد (یعنی عوامل اول تا آنجا که ممکن است بزرگ هستند). فرض کنید عدد A به ما داده شده است که حاصلضرب دو عدد اول P و Q ناشناخته است و هدف ما یافتن این دو عدد است. بهترین الگوریتم‌های کلاسیک در زمان نمایی اجرا می‌شوند. به این ترتیب با الگوریتم‌های کلاسیک حداکثر می‌توان مسئله را برای اعداد دویست رقمی حل کرد و حل آن برای اعداد بزرگتر (مثلاً هزار رقمی) فعلاً عملاً غیرممکن است.

ابتدا مبحث را با یک مثال بررسی می‌کنیم. فرض کنید که عدد $A = 21$ به ما داده شده است. به این منظور کافی است که معادله زیر را حل کنیم و یک پاسخ غیربدیهی پیدا کنیم:

$$X^2 = 1 \mod 21. \tag{۲۳}$$

دقت کنید که $X = 1$ یا $X = -1$ پاسخ‌های بدیهی هستند و برای حل مسئله کمکی به ما نمی‌کنند. اما اگر عدد هشت را امتحان کنیم آنگاه به نتیجه زیر می‌رسیم:

$$8^2 = 64 = 3 \times 21 + 1 = 1 \mod 21 \tag{۲۴}$$

$$(8+1)(8-1) = 9 \times 7 = 0 \mod 21. \tag{۲۵}$$

می‌بینیم که عدد هشت معادله (۲۳) را ارضا می‌کند. ثانیاً با استفاده از اتحاد $x^2 - y^2 = (x+y)(x-y)$ می‌توان آن را ساده‌سازی نیز کرد. نتیجه این است که عدد 21 با اعداد 7 و 9 عامل اول مشترک غیر یک دارد، چرا که باقیمانده حاصلضرب آنها به پیمانه 21 برابر صفر است. برای پیدا کردن عامل مشترک می‌توان از الگوریتم اقلیدس استفاده کرد که الگوریتم بسیار کارامدی است. اگر این کار را انجام دهیم به نتیجه زیر می‌رسیم:

$$\gcd(21, 9) = 3, \tag{۲۶}$$

$$\gcd(21, 7) = 7, \tag{۲۷}$$

که در واقع دو عامل اول عدد 21 را پیدا کردیم. بنابراین با پیدا کردن عدد 8 ادامه راه راحت است. حال به این مسئله می‌پردازیم که چگونه می‌توان چنین عددی را پیداکرد که معادله (۲۳) را ارضا کند. در این راستا از الگوریتم یافتن دوره تناوب استفاده می‌شود.

به این منظور ابتدا یک عدد تصادفی (مثلاً a) انتخاب می‌شود. سپس دوره تناوب تابع زیر محاسبه می‌شود:

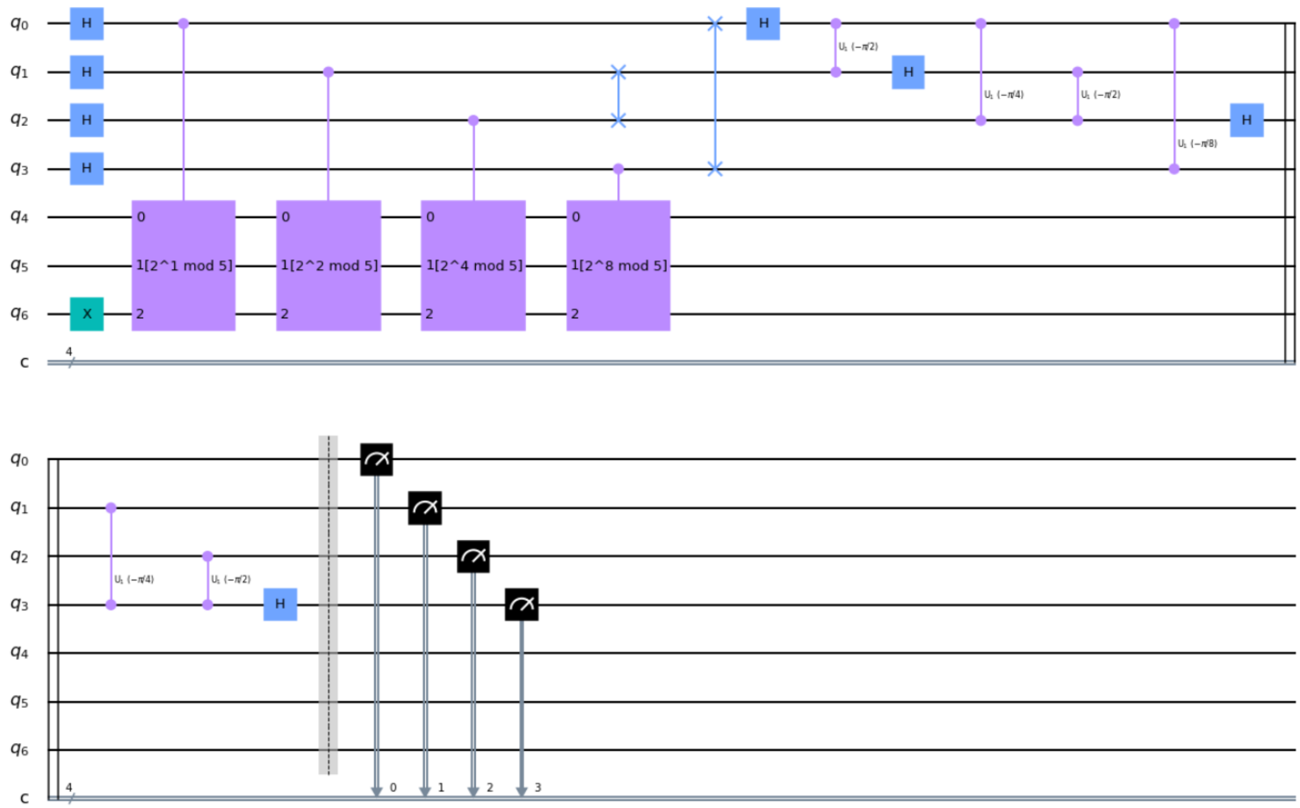
$$a^x = 1 \mod A. \tag{۲۸}$$

فرض کنید r دوره تناوب این تابع باشد. اگر خوش‌شانس باشیم ممکن است r یک عدد زوج باشد، به این ترتیب می‌توان نوشت:

$$a^r = (a^{r/2})^2 = 1 \mod A. \tag{۲۹}$$

به این ترتیب اگر $a^{r/2} \neq \pm 1 \mod A$ برقرار نباشد، آنگاه $a^{r/2}$ عدد مطلوب ماست که از طریق آن می‌توان عملیات تجزیه به عوامل اول را انجام داد. به صورت رسمی‌تر،اگر a را به صورت تصادفی از بازه 0 تا $A-1$ انتخاب کنیم و $\gcd(x, N) = 1$ باشد، آنگاه با احتمال حداقل 0.5 دوره تناوب $a^x \mod A$ یک عدد زوج است و $a^{r/2}$ یک پاسخ غیربدیهی برای معادله (۲۳) است.

پیوست


q0
q1
q2
q3
q4
q5
q6
c
H
X
0
1[2^1 mod 5]
2
1[2^2 mod 5]
1[2^4 mod 5]
1[2^8 mod 5]
U1 (−π/2)
U1 (−π/4)
U1 (−π/8)
4
0
1
2
3

شکل ۳