Computação Quântica
Aula 10

Murilo V. G. da Silva

DINF/UFPR

Fatoração

Problema (1): fatorar N em primos $p_1, p_2, ..., p_k$ tal que $p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k} = N$

Problema (2): fatorar N em primos p_1, p_2 sabendo que $p_1 \cdot p_2 = N$

- Nota: se existe algoritmo polinomial para (2), então também existe algoritmo polinomial para (1)
- A dificuldade de (2) é a base do sistema RSA
- Algoritmo clássico para (2):
  - $\mathcal{O}(2^{\sqrt[3]{n}})$ (aleatorizado)
- O Algoritmo de Shor é um Algoritmo Quântico Polinomial para (2)

Algoritmo de Shor

Ideia:

- Reduzindo o problema de fatoração para o seguinte problema:
  - encontrar raíz não trivial de 1 módulo n
- Reduzir o da raíz não trivial para o seguinte problema:
  - detectar o período da função $f(x) = b^x \pmod{n}$, para um b apropriado

    (obs: talvez não seja óbvio ver isso, mas essa função é periódica)

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?
- Faça o teste para $x = 8$
  - $8^2 = 64 \equiv 1 \pmod{21}$
- Mais algum outro valor? $x = -8$
  - $-8 \equiv ? \pmod{21}$
  - $-8 \equiv 13 \pmod{21}$
  - $13^2 = 169 \equiv 1 \pmod{21}$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?
  - algum fator de 21 divide $(8+1)$
  - algum fator de 21 divide $(8-1)$

  Como encontrar estes fatores?
  - $\text{mdc}(21, 8+1) = 3$
  - $\text{mdc}(21, 8-1) = 7$

Com isso $21 = 3 \cdot 7$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21?

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \bmod 21$ para $x = 0, 1, 2, 3, ...$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \bmod (21)$
- $x = 1 \quad 2^1 \equiv 2 \bmod (21)$
- $x = 2 \quad 2^2 \equiv 4 \bmod (21)$
- $x = 3 \quad 2^3 \equiv 8 \bmod (21)$
- $x = 4 \quad 2^4 \equiv 16 \bmod (21)$
- $x = 5 \quad 2^5 \equiv 11 \bmod (21)$
- $x = 6 \quad 2^6 \equiv 1 \bmod (21)$

Note que $2^6 = (2^3)^2 = 8^2$

Por que o valor $x = 6$ deu certo? (obs: x é chamado de ordem do subgrupo de $(\mathbb{Z}_{21}, \times)$ gerado por 2)

(1) Por que o valor x é par (tornou possível fazer o truque de dividir por 2)
(2) Por que $\frac{x}{2}$ não é raiz trivial como 1 ou 20 (lembrando que $-1 \equiv 20 \pmod{21}$)

Foi muita sorte?

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)
- Precisamos encontrar um inteiro a par tal que $f(a) = b^{a/2} \bmod 21$ era uma raíz não trivial de 1 (mod 21)

O teorema abaixo mostra, mesmo "chutando", temos boa probabilidade de encontrar b com as propriedades que queremos:

Teorema

Seja N ímpar, $N = PQ$, para P, Q primos distintos e seja b aleatório em $\{0, ..., N-1\}$
Se $\text{mdc}(b, N) = 1$, então a probabilidade da ordem a de $f(x) = b^x \pmod N$ é par e que $a/2$ seja uma raíz não trivial de 1 (mod N) é $\geq 1/2$

A probabilidade é boa, mas veja que temos uma condição a mais neste teorema: o teorema só funciona quando o valor b que chutamos tem a propriedade $\text{mdc}(b, N) = 1$.

Isso é um problema?

- Não! Caso chutemos b tal que Se $\text{mdc}(b, N) \neq 1$ já encontramos um fator de N

Raízes de 1 módulo N

Moral da história:
Chutamos um b e descobrimos a ordem do subgrupo de $(\mathbb{Z}_N, \times)$ gerado por b.

- Em outras palavras, queremos o período da função periódica $f(x) = b^x \pmod N$
- O período pode ser exponencialmente grande, portanto o número de queries que precisaríamos fazer em f para encontrar uma colisão (observe que encontrada uma colisão temos informação para encontrar o período de f).
- Entretanto, de maneira quântica, vamos usar a propriedade que QFT tem ao termos como entrada uma sobreposição descrita por uma função periódica, mesmo que este seja exponencialmente grande para encontrar este período!

Finalizando o Algoritmo de Shor

Recapitulando:

- Vimos que fatorar $N = P \cdot Q$ é equivalente a:
  encontar x tal que $x^2 \equiv 1 \pmod{N}$
  (para raízes não triviais da equação acima)
- Vimos também que encontrar x acima é equivalente a
  encontrar o período r da função $f(x) = b^x \pmod{N}$
  para algum b adequado que pode ser encontrado com probabilidade exponencialmente alta

Ideia geral do Algoritmo de Shor:

(1) Dado o inteiro N que queremos fatorar
(2) "chutamos" b e construímos a função $f(x) = b^x \pmod{N}$
(3) Encontramos o período k de f e usamos para recuperar os fatores de N

Ideia era que, para uma base b adequada, pegamos o perído k e fazemos

- $r = k/2$
- $mdc(b^r + 1, N)$ e $mdc(b^r - 1, N)$ são os fatores de N

Objetivo agora: Calcular o período de $f(x)$ em tempo polinomial usando a QFT

(Obs: este período pode ser potencialmente grande e a QFT é fundamental aqui)

- **Usaremos: Invariância da QFT a sobreposições circulares, se o objetivo é amostrar**
- **Usaremos: O comportamento da QFT em uma sobreposições periódica de período r**

Relembrando: QFT e sobreposições circulares

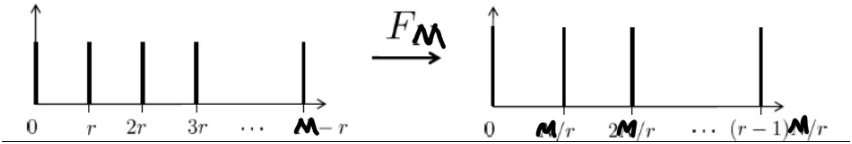
Recapitulando:

- Seja $|\Phi'\rangle$ o vetor obtido de "shift circular" de k posições de $|\Phi\rangle$
- Seja α'_i as amplitudes de $|\Phi'\rangle$ e α_i as amplitudes de $|\Phi\rangle$
- Seja $F_M |\Phi\rangle = |\Psi\rangle$ e $F_M |\Phi'\rangle = |\Psi'\rangle$
- Então $\alpha'_i = \omega^{ik}\alpha_i$, e portanto $|\alpha_i|^2 = |\alpha'_i|^2$.

Ou seja, se o objetivo é fazer uma medida após a QFT, um shift circular não altera a distribuição de probabilidade dos estados resultantes

Relembrando: QFT e funções periódicas

Recapitulando:

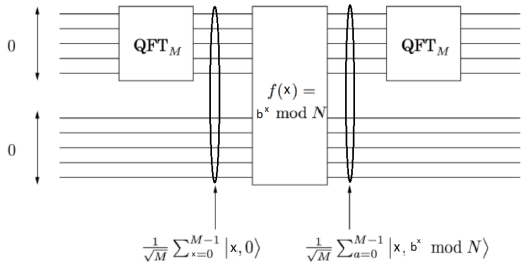


Teorema: Aplicando F_M ao vetor $|\Phi\rangle$, o vetor resultante tem amplitudes β_k:

- iguais a $\frac{1}{\sqrt{r}}$, para $k = 0, \frac{M}{r}, \frac{2M}{r}, \frac{3M}{r}, ..., \frac{(r-1)M}{r}$.
- iguais a zero para as demais posições do vetor de amplitudes.

- Ou seja $$\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle \xrightarrow{QFT_M} \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |j\tfrac{M}{r}\rangle$$

Detectando o período da função $f(x) = b^x \pmod N$

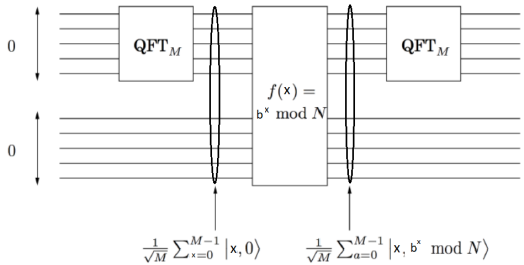


- O que acontece quando medimos o segundo registrador saindo de $f(x)$?
- Se obtivermos y, o primeiro registrador colapsa em uma sobreposição de todos os estados x tal que $f(x) = y$.
- Seja r o período de f e seja a o menor não negativo tal que $f(a) = y$.

Para um exemplo concreto, digamos que $a = 3$ e $r = 7$: Neste caso a sobreposição será $|3\rangle + |10\rangle + |17\rangle + |24\rangle + \ldots + |M - r + 3\rangle$

De maneira geral a sobreposição será no primeiro registrador será: $|a\rangle + |r + a\rangle + |2r + a\rangle + |3r + a\rangle + \ldots + |M - r + a\rangle$

Detectando o período da função $f(x) = b^x \pmod N$



- Como vimos, a sobreposição no primeiro registrador após medir o segundo na saída da função f é $|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \ldots + |M-r+a\rangle$ (slide anterior)
- Ou seja, a sobreposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.
- Ao medirmos esta sobreposição, a distribuição de saída é a mesma da sobreposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$ (propriedade da QFT com sobreposições circulares com "shift" de a posições)
- Após a QFT, a sobreposição tem período M/r (propriedade da QFT com sobreposição de período r)
- Ao medir a saída da segunda QFT, obtemos algum valor $k\frac{M}{r}$ (estamos assumindo M múltiplo de r, mas em análise mais fina escolha $M > 2N^2$ e portanto $M > 2r^2$)
- Coletando várias amostras desta saída $s_1, s_2, \ldots$, encontramos dois valores s_i e s_j tal que $\text{mdc}(s_i, s_j) = r$. (podemos mostrar que isso acontece com probabilidade exponencialmente grande)