# Computação Quântica
# Aula 16

Murilo V. G. da Silva

DINF/UFPR

# Finalizando o Algoritmo de Shor

Aula passada:

- Vimos que fatorar $N = P \cdot Q$ é equivalente a:

# Finalizando o Algoritmo de Shor

Aula passada:

- Vimos que fatorar $N = P \cdot Q$ é equivalente a:

  encontar $x$ tal que $x^2 \equiv 1 \pmod{N}$

# Finalizando o Algoritmo de Shor

Aula passada:

- 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)

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

# Finalizando o Algoritmo de Shor

Aula passada:

- 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 $f(x) = b^x \pmod{N}$

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

Mais precisamente,

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

Mais precisamente,

(1) Dado o inteiro $N$ que queremos fatorar

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

Mais precisamente,

(1) Dado o inteiro $N$ que queremos fatorar

(2) "chutamos" $b$ e construímos a função $f(x) = b^x \pmod{N}$

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

Mais precisamente,

(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 $N$

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

Mais precisamente,

(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

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

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

Mais precisamente,

(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

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

Aula de hoje: Calcularemos o período de $f(x)$ em tempo polinomial usando a QFT

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

Mais precisamente,

(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

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

Aula de hoje: Calcularemos 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 superposições circulares, se o objetivo é amostrar**

# Finalizando o Algoritmo de Shor

Aula passada:

- 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

Mais precisamente,

(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

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

Aula de hoje: Calcularemos 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 superposições circulares, se o objetivo é amostrar**
- **Usaremos: O comportamento da QFT em uma superposições periódica de período $r$**

# Relembrando: QFT e superposições circulares

Lembrando que:

# Relembrando: QFT e superposições circulares

Lembrando que:

- Seja $|\Phi'\rangle$ o vetor obtido de "shift circular" de $k$ posições de $|\Phi\rangle$

# Relembrando: QFT e superposições circulares

Lembrando que:

- Seja $|\Phi'\rangle$ o vetor obtido de "shift circular" de $k$ posições de $|\Phi\rangle$
- Seja $\alpha'_i$ as amplitudes de $|\Phi'\rangle$ e $\alpha_i$ as amplitudes de $|\Phi\rangle$

# Relembrando: QFT e superposições circulares

Lembrando que:

- Seja $|\Phi'\rangle$ o vetor obtido de "shift circular" de $k$ posições de $|\Phi\rangle$
- Seja $\alpha'_i$ as amplitudes de $|\Phi'\rangle$ e $\alpha_i$ as amplitudes de $|\Phi\rangle$
- Seja $F_M |\Phi\rangle = |\Psi\rangle$ e $F_M |\Phi'\rangle = |\Psi'\rangle$

# Relembrando: QFT e superposições circulares

Lembrando que:

- Seja $|\Phi'\rangle$ o vetor obtido de "shift circular" de $k$ posições de $|\Phi\rangle$
- Seja $\alpha'_i$ as amplitudes de $|\Phi'\rangle$ e $\alpha_i$ 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 $|\alpha_i|^2 = |\alpha'_i|^2$.

# Relembrando: QFT e superposições circulares

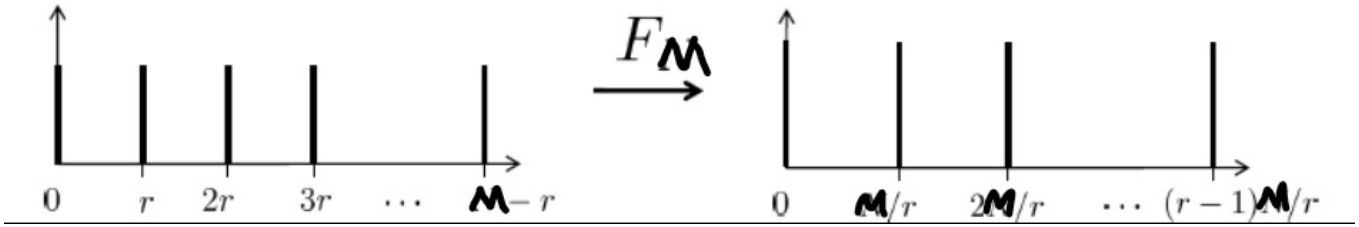
Lembrando que:

- Seja $|\Phi'\rangle$ o vetor obtido de "shift circular" de $k$ posições de $|\Phi\rangle$
- Seja $\alpha'_i$ as amplitudes de $|\Phi'\rangle$ e $\alpha_i$ 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

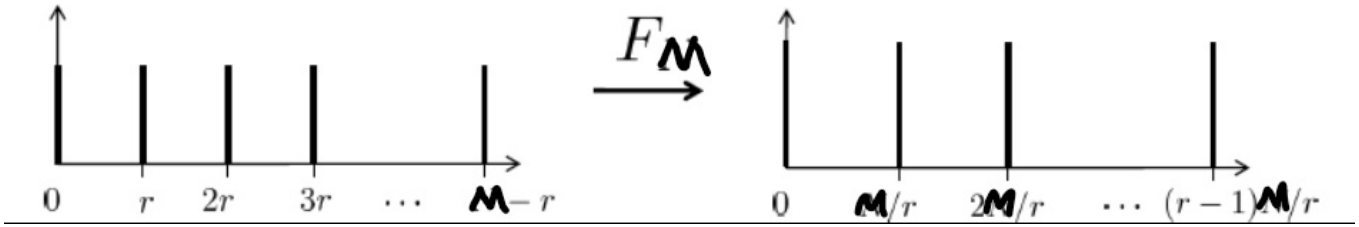
# Relembrando: QFT e funções periódicas

Lembrando que:



# Relembrando: QFT e funções periódicas

Lembrando que:

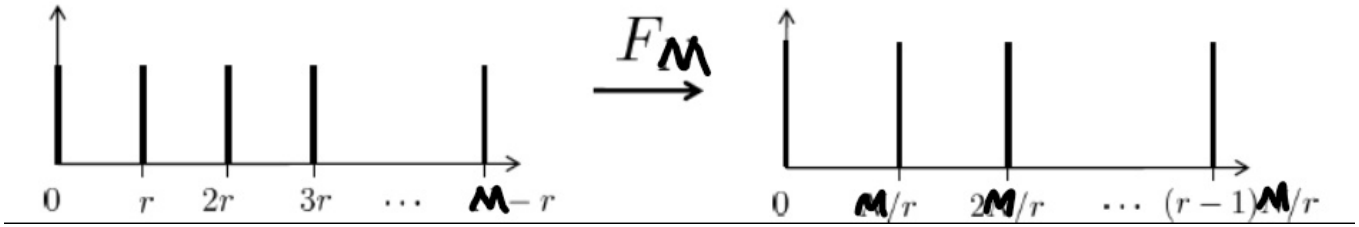



Teorema: Aplicando $F_M$ ao vetor $|\Phi\rangle$, o vetor resultante tem amplitudes $\beta_k$:

- iguais a $\frac{1}{\sqrt{r}}$, para $k = 0, \frac{M}{r}, \frac{2M}{r}, \frac{3M}{r}, ..., \frac{(r-1)M}{r}$.

# Relembrando: QFT e funções periódicas

Lembrando que:

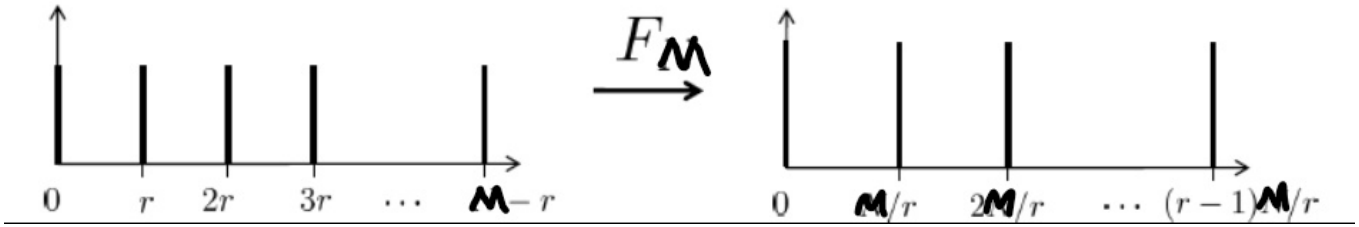



Teorema: Aplicando $F_M$ ao vetor $|\Phi\rangle$, o vetor resultante tem amplitudes $\beta_k$:

- 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.

# Relembrando: QFT e funções periódicas

Lembrando que:

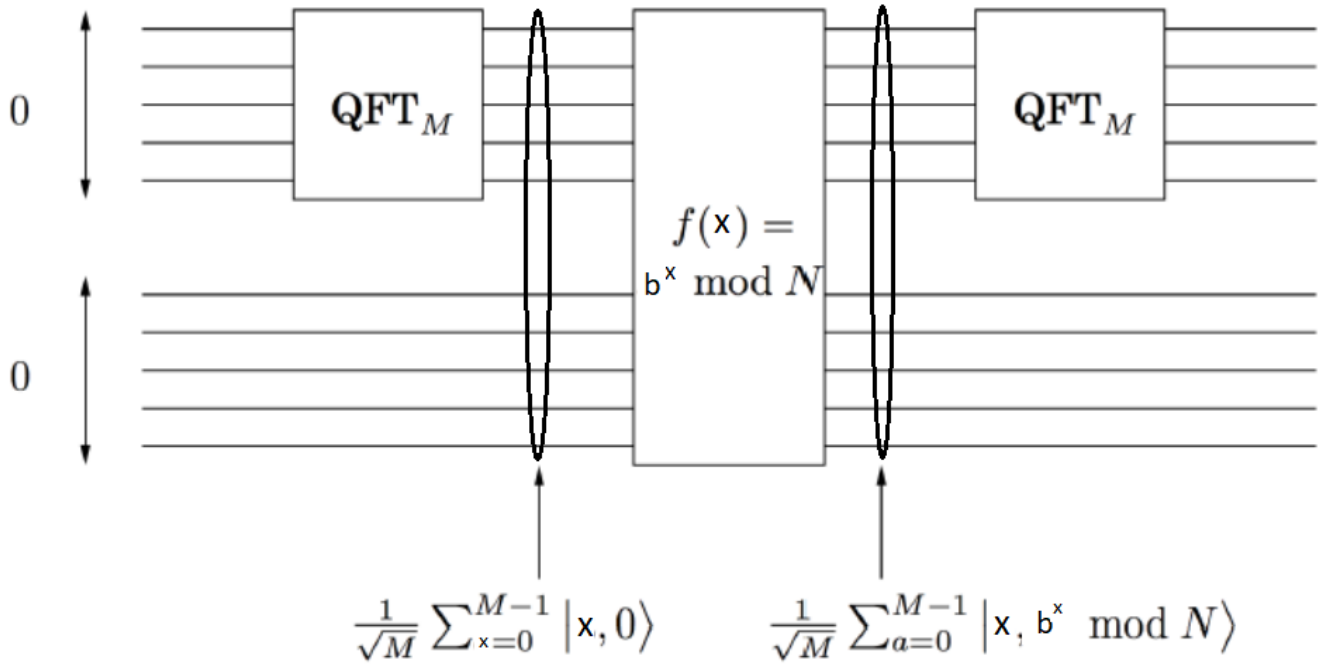



Teorema: Aplicando $F_M$ ao vetor $|\Phi\rangle$, o vetor resultante tem amplitudes $\beta_k$:

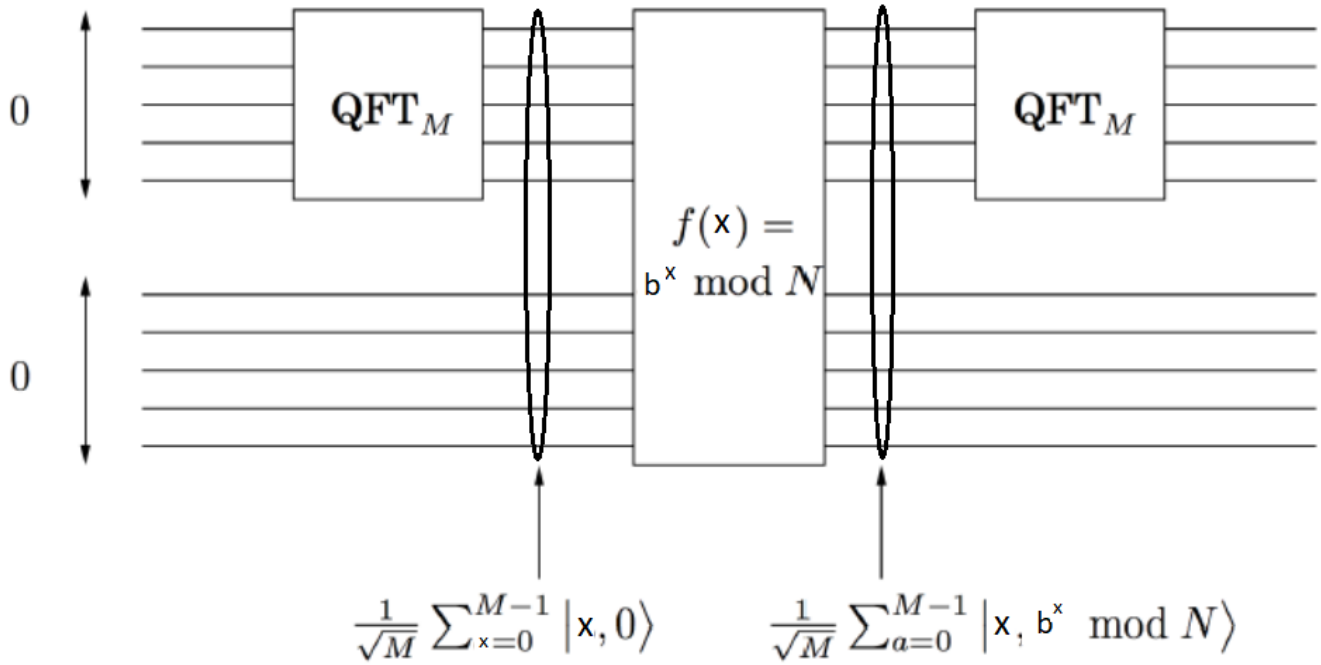
- iguais a $\frac{1}{\sqrt{r}}$, para $k = 0, \frac{M}{r}, \frac{2M}{r}, \frac{3M}{r}, ..., \frac{(r-1)M}{r}$.
- iguais a zero para as demais posições do vetor de amplitudes.

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

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

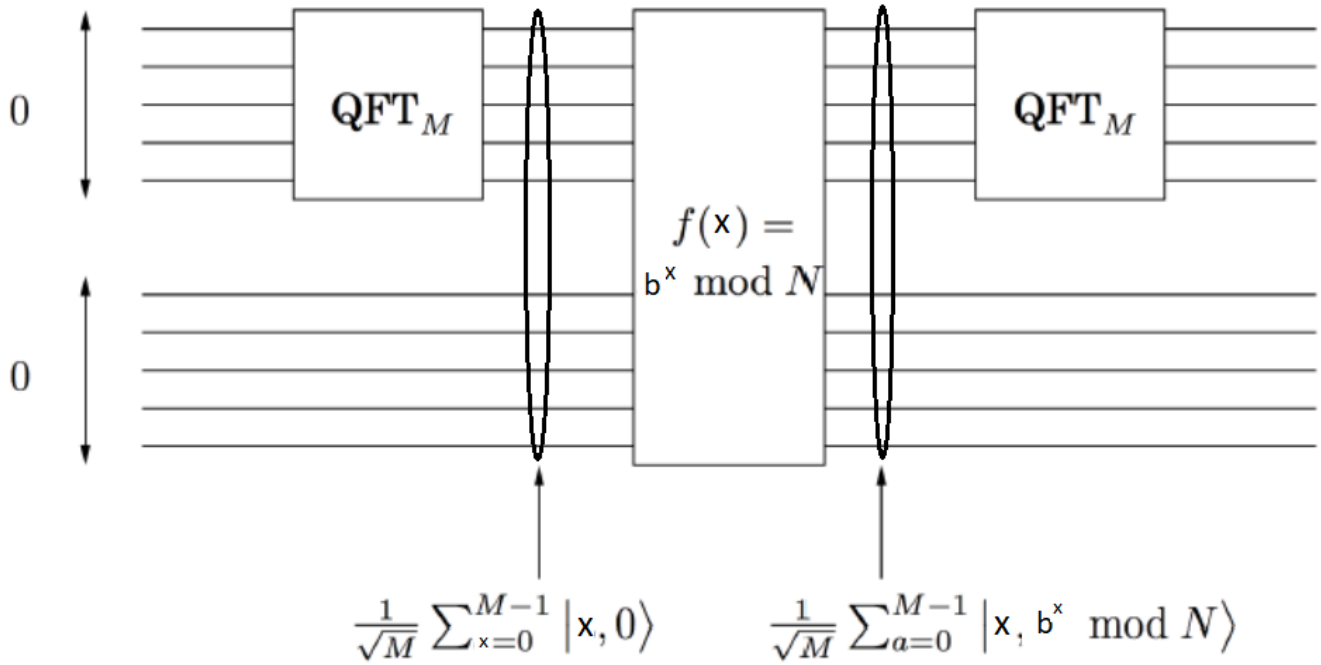


# Detectando o período da função $f(x) = b^x \pmod N$



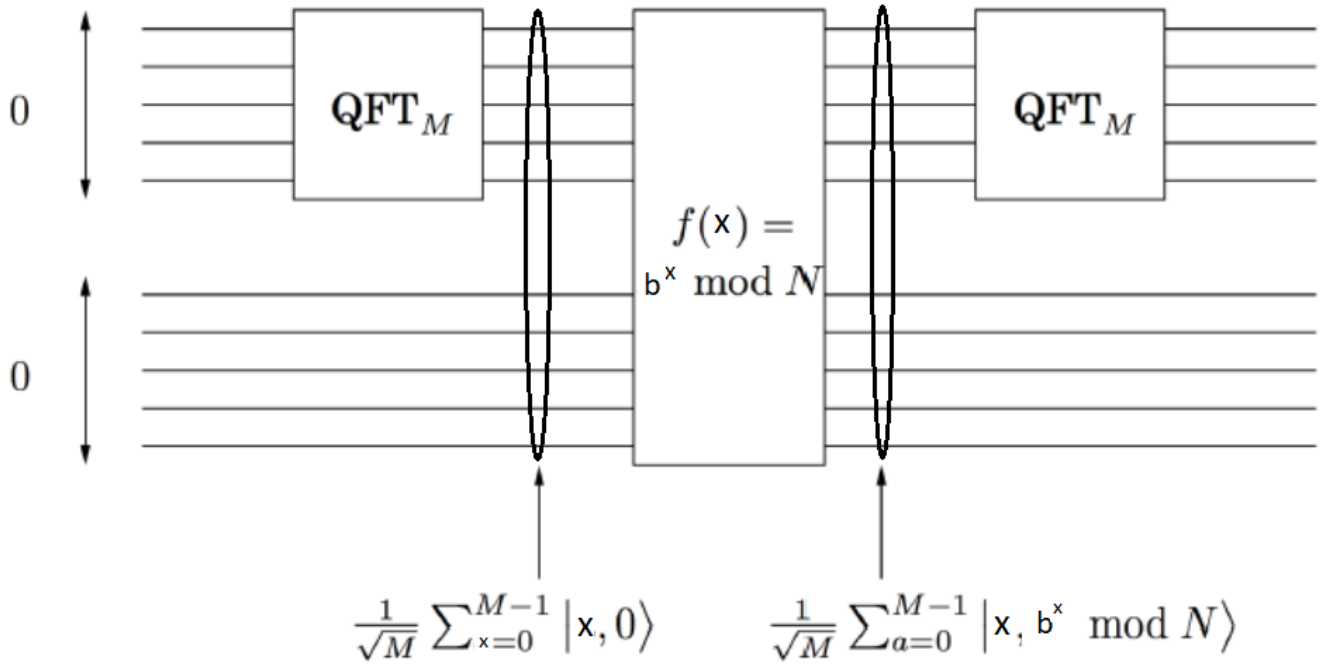

- O que acontece quando medimos o segundo registrador saindo de $f(x)$?

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



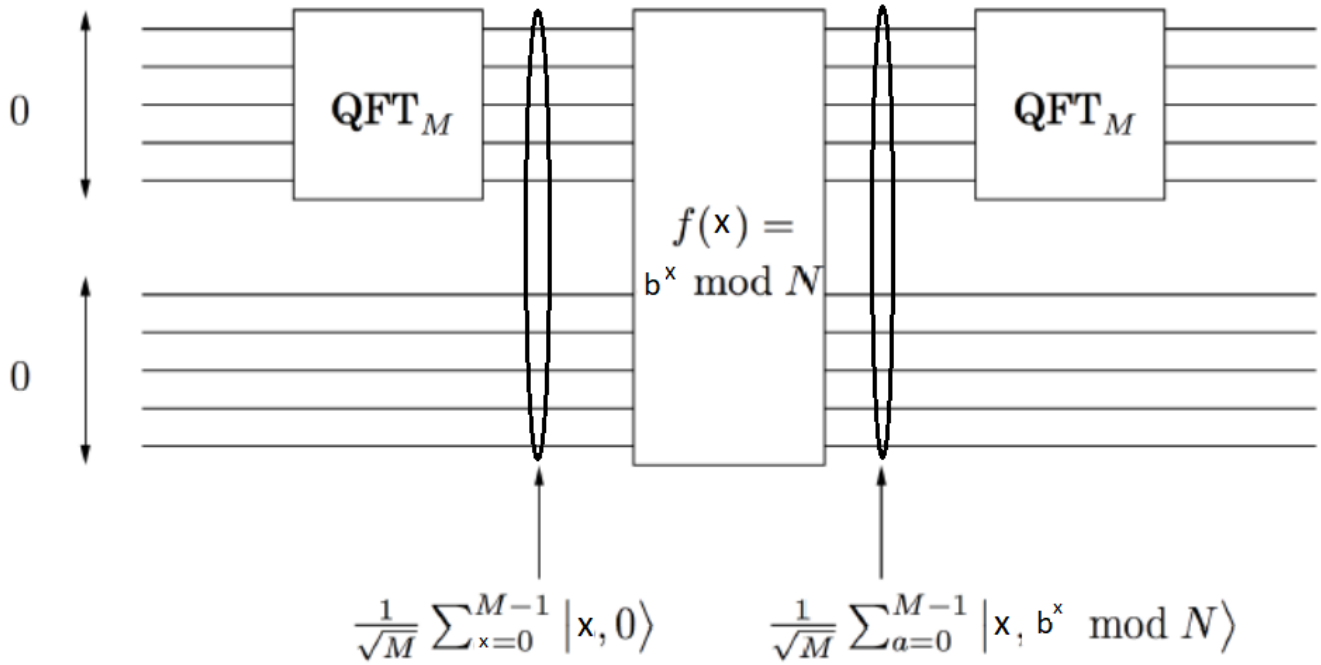

- O que acontece quando medimos o segundo registrador saindo de $f(x)$?
- Se obtivermos $y$, o primeiro registrador colapsa em uma superposição de todos os estados $x$ tal que $f(x) = y$.

# 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 superposição 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 $f(a) = y$.

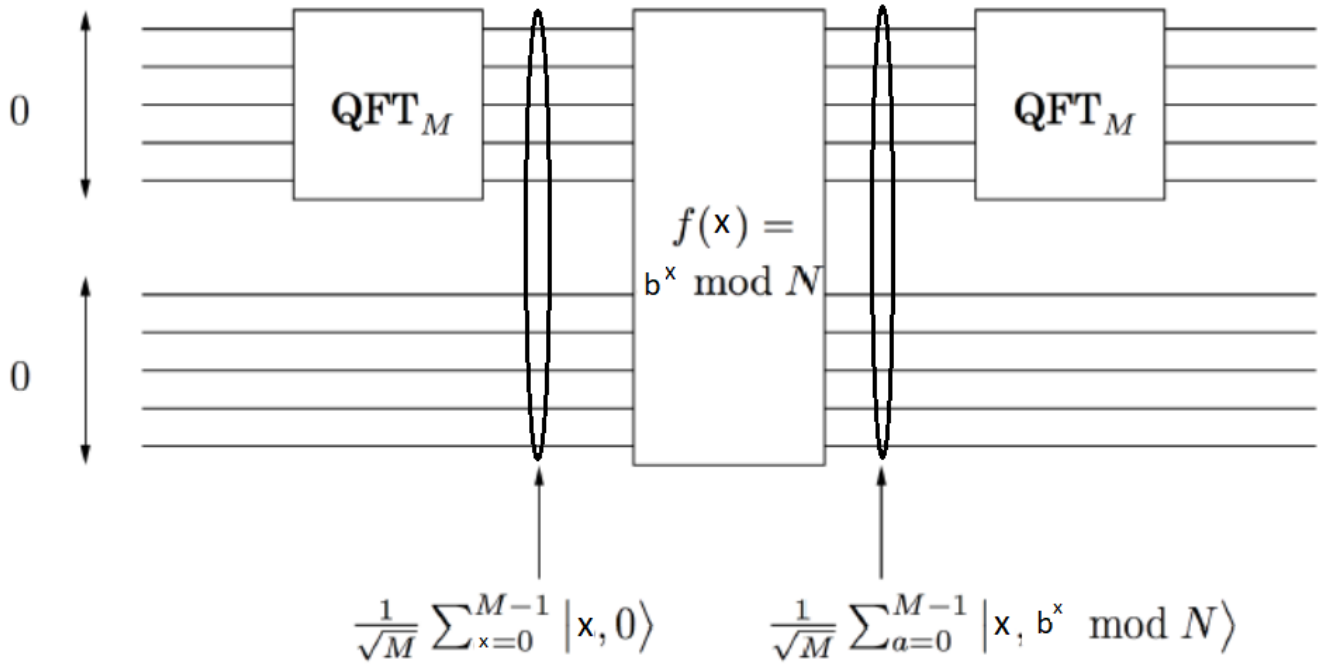
# Detectando o período da função $f(x) = b^x \pmod N$




- O que acontece quando medimos o segundo registrador saindo de $f(x)$?
- Se obtivermos $y$, o primeiro registrador colapsa em uma superposição 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 $r = 7$:

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

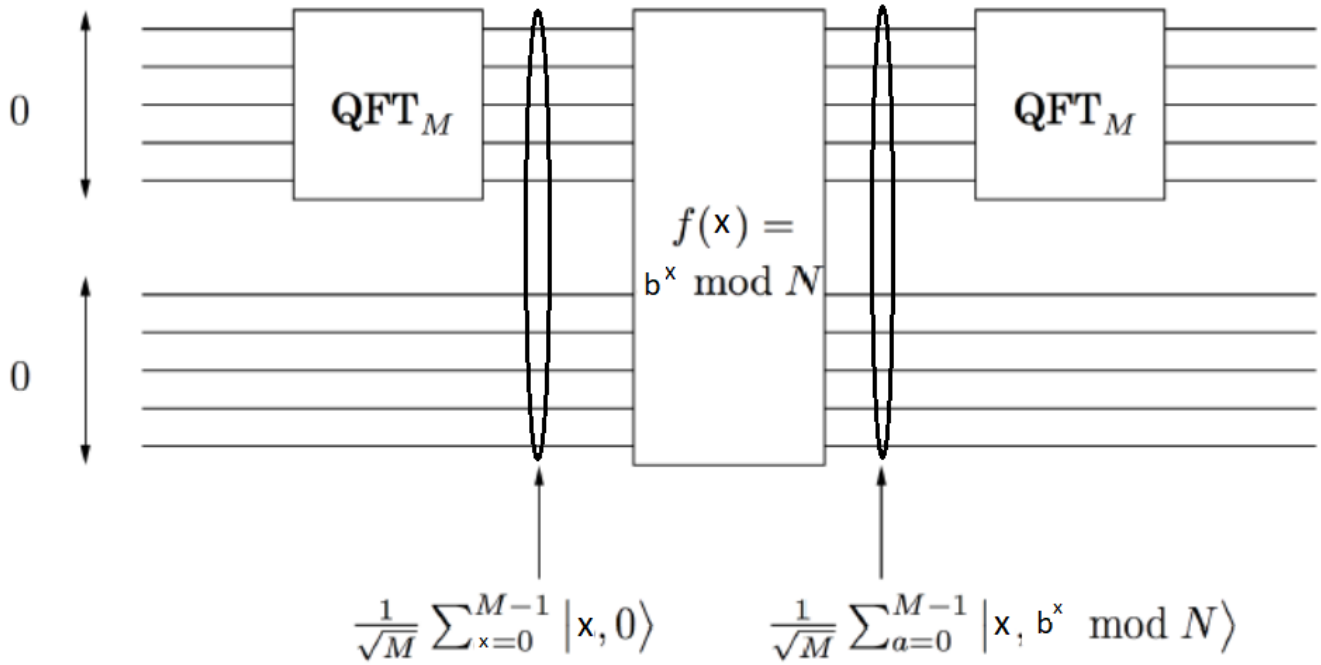



- O que acontece quando medimos o segundo registrador saindo de $f(x)$?
- Se obtivermos $y$, o primeiro registrador colapsa em uma superposição de todos os estados $x$ tal que $f(x) = y$.
- Seja $r$ o período de $f$ e seja $a$ o menor não negativo tal que $f(a) = y$.

Para um exemplo concreto, digamos que $a = 3$ e $r = 7$:

Neste caso a superposição será $|3\rangle + |10\rangle + |17\rangle + |24\rangle + \ldots + |M - r + 3\rangle$

# 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 superposição 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 $f(a) = y$.

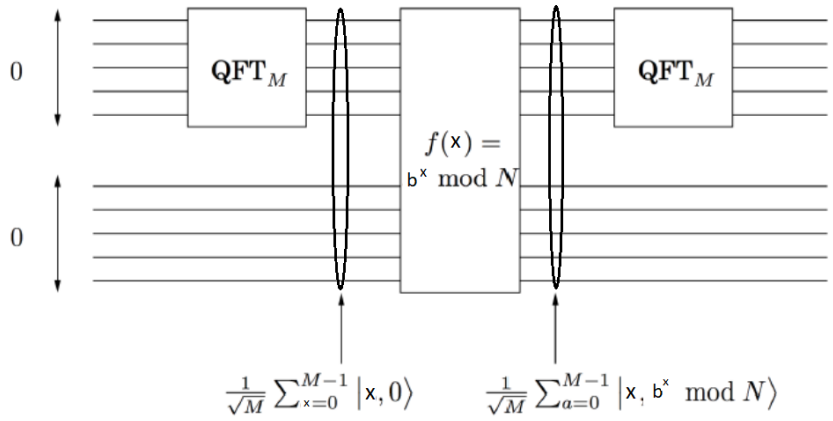
Para um exemplo concreto, digamos que $a = 3$ e $r = 7$:

Neste caso a superposição será $|3\rangle + |10\rangle + |17\rangle + |24\rangle + \ldots + |M - r + 3\rangle$

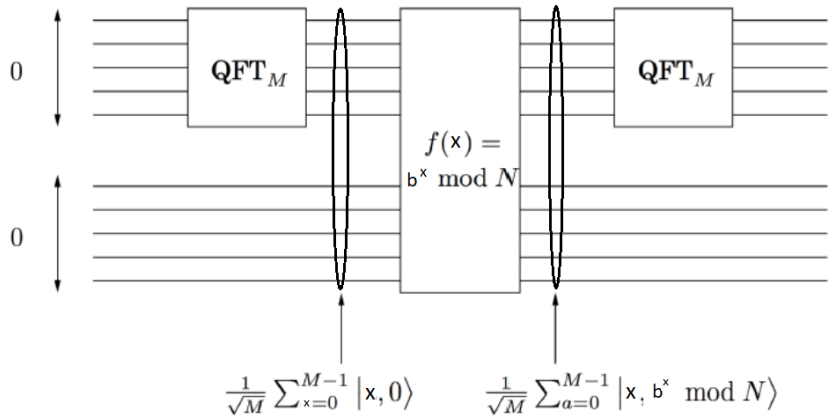
De maneira geral a superposição será no primeiro registrador será:

$|a\rangle + |r + a\rangle + |2r + a\rangle + |3r + a\rangle + \ldots + |M - r + a\rangle$

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

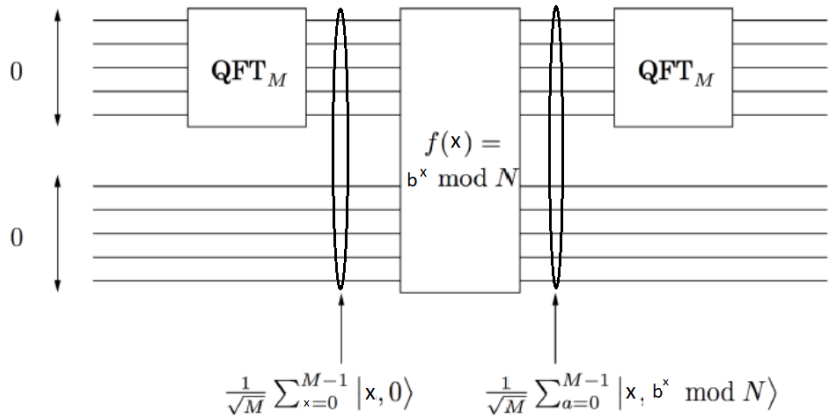


# Detectando o período da função $f(x) = b^x \pmod N$



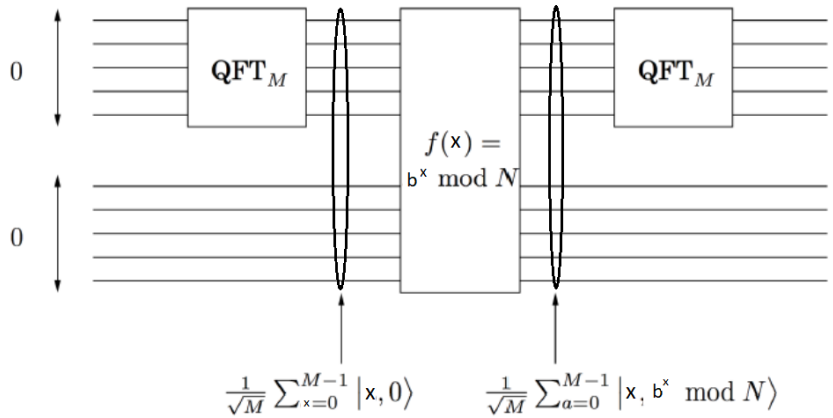

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r + a\rangle + |2r + a\rangle + |3r + a\rangle + \ldots + |M - r + a\rangle$

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



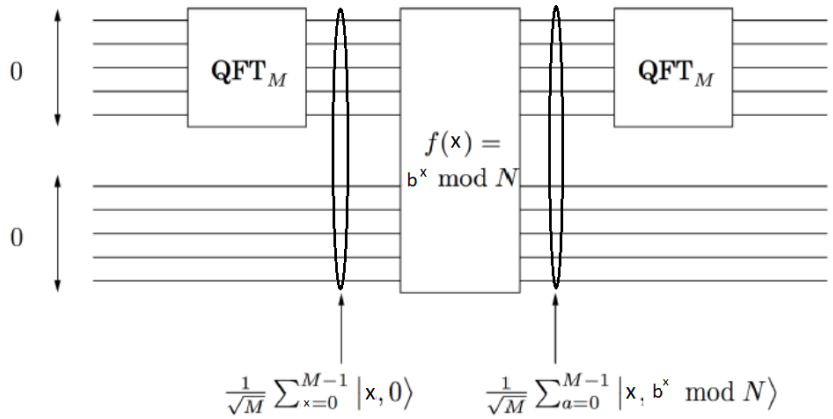

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r + a\rangle + |2r + a\rangle + |3r + a\rangle + \ldots + |M - r + a\rangle$ (slide anterior)

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



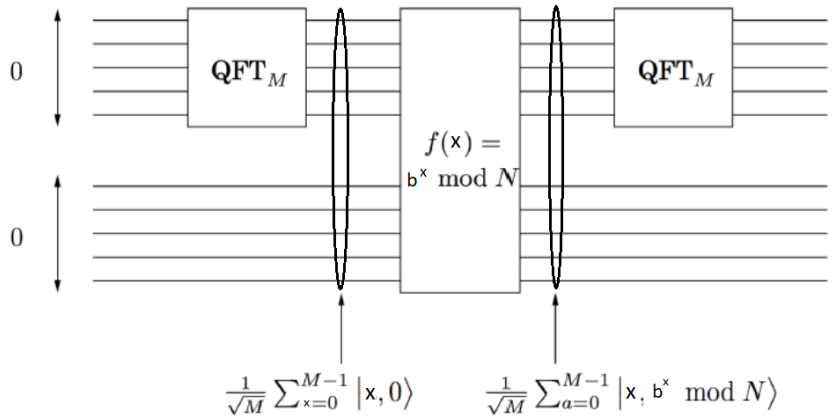

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \ldots + |M-r+a\rangle$ (slide anterior)
- Ou seja, a superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.

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



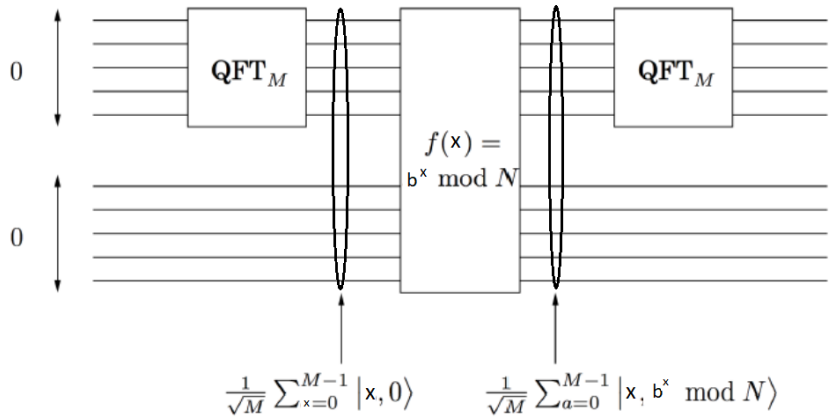

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \ldots + |M-r+a\rangle$ (slide anterior)
- Ou seja, a superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.
- Ao medirmos esta superposição, a distribuição de saída é a mesma da superposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$

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



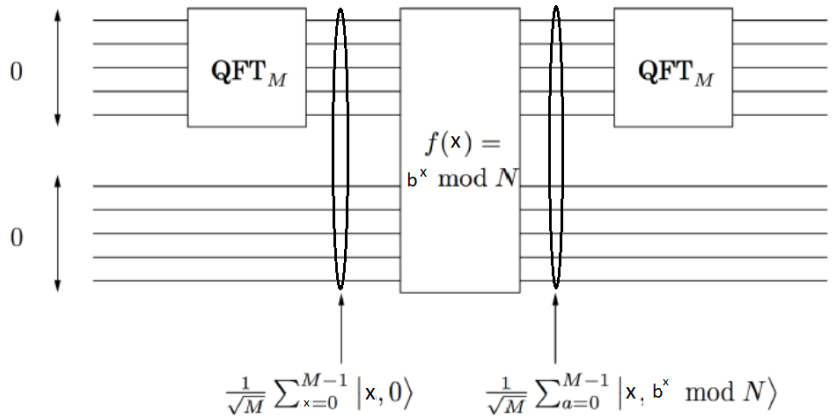

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \ldots + |M-r+a\rangle$ (slide anterior)
- Ou seja, a superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.
- Ao medirmos esta superposição, a distribuição de saída é a mesma da superposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$ (propriedade da QFT com superposições circulares com "shift" de $a$ posições)

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



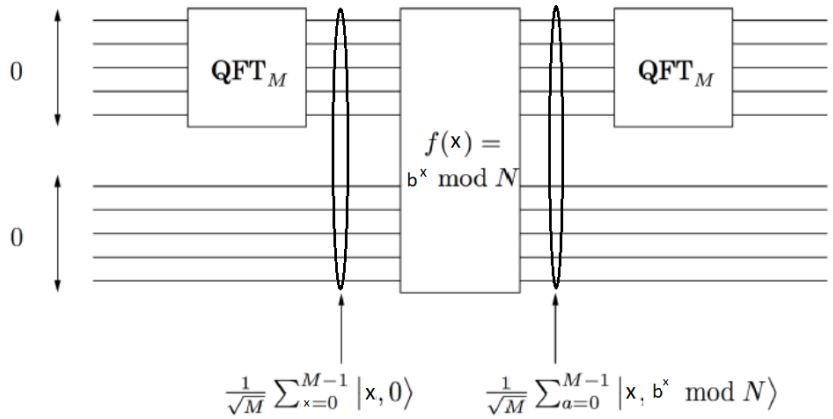

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \ldots + |M-r+a\rangle$ (slide anterior)
- Ou seja, a superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.
- Ao medirmos esta superposição, a distribuição de saída é a mesma da superposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$ (propriedade da QFT com superposições circulares com "shift" de $a$ posições)
- Após a QFT, a superposição tem período $M/r$

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



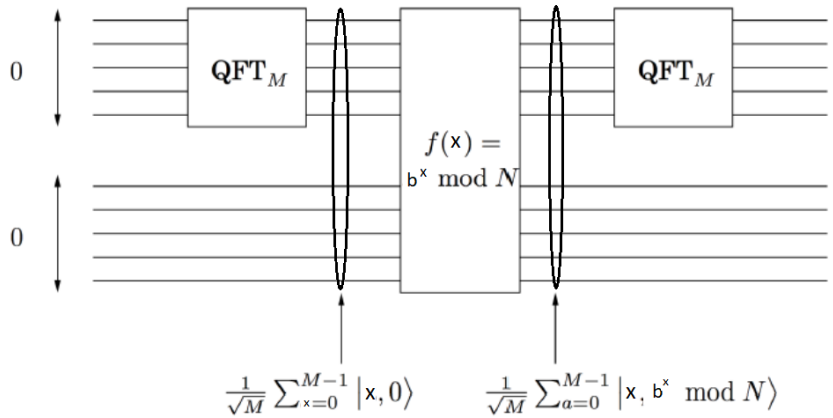

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \ldots + |M-r+a\rangle$ (slide anterior)
- Ou seja, a superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.
- Ao medirmos esta superposição, a distribuição de saída é a mesma da superposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$ (propriedade da QFT com superposições circulares com "shift" de $a$ posições)
- Após a QFT, a superposição tem período $M/r$ (propriedade da QFT com superposição de período $r$)

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



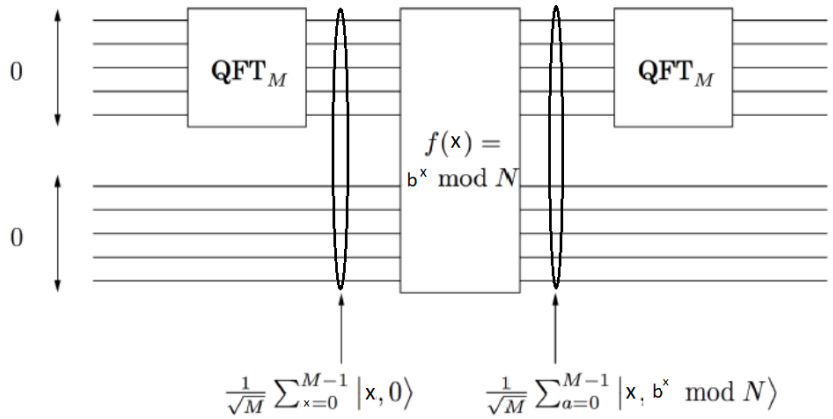

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \ldots + |M-r+a\rangle$ (slide anterior)
- Ou seja, a superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.
- Ao medirmos esta superposição, a distribuição de saída é a mesma da superposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$ (propriedade da QFT com superposições circulares com "shift" de $a$ posições)
- Após a QFT, a superposição tem período $M/r$ (propriedade da QFT com superposição de período $r$)
- Ao medir a saída da segunda QFT, obtemos algum valor $k\frac{M}{r}$

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



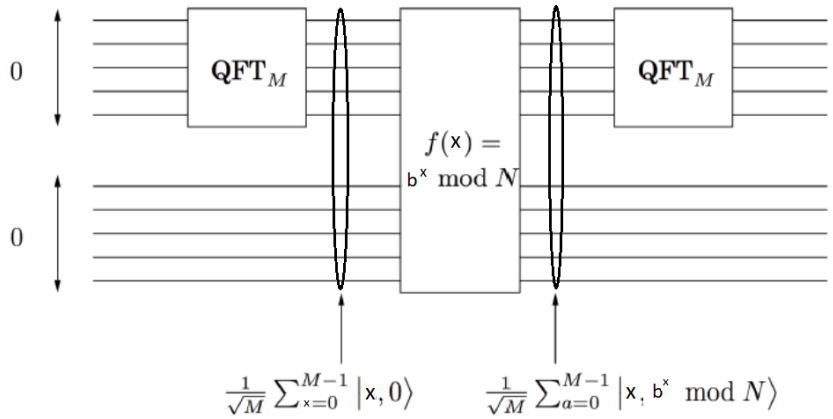

- Como vimos, a superposição no primeiro registrador após medir o segundo na saída da função $f$ é $|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \ldots + |M-r+a\rangle$ (slide anterior)
- Ou seja, a superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.
- Ao medirmos esta superposição, a distribuição de saída é a mesma da superposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$ (propriedade da QFT com superposições circulares com "shift" de $a$ posições)
- Após a QFT, a superposição tem período $M/r$ (propriedade da QFT com superposição 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 $M > 2r^2$)

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




- Como vimos, a superposição 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 superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+a\rangle$.
- Ao medirmos esta superposição, a distribuição de saída é a mesma da superposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$ (propriedade da QFT com superposições circulares com "shift" de $a$ posições)
- Após a QFT, a superposição tem período $M/r$ (propriedade da QFT com superposição 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 $\mathrm{mdc}(s_i, s_j) = r$.

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




- Como vimos, a superposição 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 superposição é $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr + a\rangle$.
- Ao medirmos esta superposição, a distribuição de saída é a mesma da superposição $\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$ (propriedade da QFT com superposições circulares com "shift" de $a$ posições)
- Após a QFT, a superposição tem período $M/r$ (propriedade da QFT com superposição 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)