# Peter W. Shor - Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.

19 listopada 2004 roku

# Wstęp czyli (próba) odpowiedzi na pewne pytania

- (Silna) Teza Church'a

# Wstęp czyli (próba) odpowiedzi na pewne pytania

- (Silna) Teza Church'a
- Co to znaczy 'zasoby' i 'fizyczna maszyna liczaca' ?

# Wstęp czyli (próba) odpowiedzi na pewne pytania

- (Silna) Teza Church'a
- Co to znaczy 'zasoby' i 'fizyczna maszyna liczaca' ?
- Dlaczego obliczenia kwantowe ?

# Wstęp czyli (próba) odpowiedzi na pewne pytania

- (Silna) Teza Church'a
- Co to znaczy 'zasoby' i 'fizyczna maszyna liczaca' ?
- Dlaczego obliczenia kwantowe ?
- Dlaczego akurat faktoryzacja liczb i problem dyskretnego logarytmu ?

# Stan układu - Fizyka klasyczna

- Stan każdej cząstki opisuje się jednoznacznie poprzez podanie jej wektora stanu tzn. zbioru liczb opisujących jej fizyczne właściwości: położenie, pęd, ładunek elektryczny itp.

# Stan układu - Fizyka klasyczna

- Stan każdej cząstki opisuje się jednoznacznie poprzez podanie jej wektora stanu tzn. zbioru liczb opisujących jej fizyczne właściwości: położenie, pęd, ładunek elektryczny itp.
- Stan układu to po prostu podanie wektora stanu zawierającego opis wszystkich cząstek

# Stan układu - Fizyka klasyczna

- Stan każdej cząstki opisuje się jednoznacznie poprzez podanie jej wektora stanu tzn. zbioru liczb opisujących jej fizyczne właściwości: położenie, pęd, ładunek elektryczny itp.
- Stan układu to po prostu podanie wektora stanu zawierającego opis wszystkich cząstek
- Mając podany wektor stanu układu oraz jego równanie ruchu (hamiltonian) możemy powiedzieć wszystko o jego przyszłości i przeszłości.

# Stan układu - Fizyka klasyczna

- Stan każdej cząstki opisuje się jednoznacznie poprzez podanie jej wektora stanu tzn. zbioru liczb opisujących jej fizyczne właściwości: położenie, pęd, ładunek elektryczny itp.
- Stan układu to po prostu podanie wektora stanu zawierającego opis wszystkich cząstek
- Mając podany wektor stanu układu oraz jego równanie ruchu (hamiltonian) możemy powiedzieć wszystko o jego przyszłości i przeszłości.
- Bardzo dobrze sprawdza się w przypadku ’dużych’ zjawisk fizycznych.

# Stan układu - Fizyka kwantowa

- Stanu cząstki nie znamy z całkowitą pewnością - znamy natomiast rozkład prawdopodobieństwa stanów, opisujemy go za pomocą wektora stanu. Jest to wektor z pewnej zespolonej przestrzeni liniowej (Hilberta) postaci:

$$p_1|s_1\rangle + p_2|s_2\rangle + \cdots + p_n|s_n\rangle,$$

o jednostkowej długości. $s_i$ są to możliwe stany układu, a $p_i^2$ prawdopodobieństwa ich zaobserwowania, a więc:

$$\sum_{i=0}^{n} |p_i|^2 = 1$$

# Stan układu - Fizyka kwantowa

- Stanu cząstki nie znamy z całkowitą pewnością - znamy natomiast rozkład prawdopodobieństwa stanów, opisujemy go za pomocą wektora stanu. Jest to wektor z pewnej zespolonej przestrzeni liniowej (Hilberta) postaci:

$$p_1|s_1\rangle + p_2|s_2\rangle + \cdots + p_n|s_n\rangle,$$

o jednostkowej długości. $s_i$ są to możliwe stany układu, a $p_i^2$ prawdopodobieństwa ich zaobserwowania, a więc:

$$\sum_{i=0}^{n} |p_i|^2 = 1$$

- Stan układu składającego się z n kubitów definiujemy poprzez podanie wektora stanu w $2^n - 1$ wymiarowej przestrzeni.

# Stan układu - Fizyka kwantowa

- Stanu cząstki nie znamy z całkowitą pewnością - znamy natomiast rozkład prawdopodobieństwa stanów, opisujemy go za pomocą wektora stanu. Jest to wektor z pewnej zespolonej przestrzeni liniowej (Hilberta) postaci:

$$p_1|s_1\rangle + p_2|s_2\rangle + \cdots + p_n|s_n\rangle,$$

o jednostkowej długości. $s_i$ są to możliwe stany układu, a $p_i^2$ prawdopodobieństwa ich zaobserwowania, a więc:

$$\sum_{i=0}^{n} |p_i|^2 = 1$$

- Stan układu składającego się z n kubitów definiujemy poprzez podanie wektora stanu w $2^n - 1$ wymiarowej przestrzeni.
- Wszystkie transformacje układu kwantowego muszą być odwracalne.

# Stan układu - Fizyka kwantowa

- Stanu cząstki nie znamy z całkowitą pewnością - znamy natomiast rozkład prawdopodobieństwa stanów, opisujemy go za pomocą wektora stanu. Jest to wektor z pewnej zespolonej przestrzeni liniowej (Hilberta) postaci:

$$p_1|s_1\rangle + p_2|s_2\rangle + \cdots + p_n|s_n\rangle,$$

o jednostkowej długości. $s_i$ są to możliwe stany układu, a $p_i^2$ prawdopodobieństwa ich zaobserwowania, a więc:

$$\sum_{i=0}^{n} |p_i|^2 = 1$$

- Stan układu składającego się z n kubitów definiujemy poprzez podanie wektora stanu w $2^n - 1$ wymiarowej przestrzeni.
- Wszystkie transformacje układu kwantowego muszą być odwracalne.
- Obserwacja układu powoduje jego 'uklasycznienie'.

# Transformacje układu

- Aby móc przeprowadzać obliczenia kwantowe, musimy mieć możliwość wpływania na stan układu.

# Transformacje układu

- Aby móc przeprowadzać obliczenia kwantowe, musimy mieć możliwość wpływania na stan układu.
- Prawa fizyki kwantowej pozwalają tylko na przekształcenia odwracalne. Wygodnym sposobem ich opisu jest macierz unitarna (jej sprzężenie jest równe jej transpozycji), która określa dla każdego stanu układu, prawdopodobieństwo znalezienia się w superpozycji innych stanów.

# Transformacje układu

- Aby móc przeprowadzać obliczenia kwantowe, musimy mieć możliwość wpływania na stan układu.
- Prawa fizyki kwantowej pozwalają tylko na przekształcenia odwracalne. Wygodnym sposobem ich opisu jest macierz unitarna (jej sprzężenie jest równe jej transpozycji), która określa dla każdego stanu układu, prawdopodobieństwo znalezienia się w superpozycji innych stanów.
- Przykład. Rozważmy transformacje:

$$|00\rangle \to |00\rangle \qquad |01\rangle \to |01\rangle$$
$$|10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) \qquad |11\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

Macierzą tego przekształcenia jest:

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{vmatrix}$$

# Transformacje układu cd.

- Przykład. Transformacja:
  $|00\rangle \to |00\rangle$ $\quad$ $|01\rangle \to |01\rangle$
  $|10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$ $\quad$ $|11\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$
- Jeśli teraz nasz układ jest w stanie:

$$\frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

i zadziałamy na niego powyższą transformacją

# Transformacje układu cd.

- Przykład. Transformacja:
  $|00\rangle \to |00\rangle$ $\quad$ $|01\rangle \to |01\rangle$
  $|10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$ $\quad$ $|11\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$
- Jeśli teraz nasz układ jest w stanie:

$$\frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

  i zadziałamy na niego powyższą transformacją
- To otrzymamy układ w stanie:

$$\frac{1}{2}(|10\rangle + |11\rangle) - \frac{1}{2}(|10\rangle - |11\rangle) = |11\rangle$$

# Transformacje układu cd.

- Przykład. Transformacja:
  $|00\rangle \to |00\rangle$ $\quad$ $|01\rangle \to |01\rangle$
  $|10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$ $\quad$ $|11\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$
- Jeśli teraz nasz układ jest w stanie:

$$\frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

  i zadziałamy na niego powyższą transformacją
- To otrzymamy układ w stanie:

$$\frac{1}{2}(|10\rangle + |11\rangle) - \frac{1}{2}(|10\rangle - |11\rangle) = |11\rangle$$

- Zauważmy, że zaszła tutaj interferencja prawdopodobieństw - jest to bardzo ważna cecha tych transformacji - to jest najbardziej istotne źródło mocy obliczeń kwantowych.

# Transformacje układu cd.

- Przykład. Transformacja:
  $|00\rangle \to |00\rangle$ $\quad$ $|01\rangle \to |01\rangle$
  $|10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$ $\quad$ $|11\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$
- Jeśli teraz nasz układ jest w stanie:

$$\frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

  i zadziałamy na niego powyższą transformacją
- To otrzymamy układ w stanie:

$$\frac{1}{2}(|10\rangle + |11\rangle) - \frac{1}{2}(|10\rangle - |11\rangle) = |11\rangle$$

- Zauważmy, że zaszła tutaj interferencja prawdopodobieństw - jest to bardzo ważna cecha tych transformacji - to jest najbardziej istotne źródło mocy obliczeń kwantowych.
- Transformacje można oczywiście składać - reprezentujemy je jako iloczyn tensorowy macierzy.

# Obwody kwantowe

- Jest to naturalne przeniesienie idei obwodów logicznych na grunt obliczeń kwantowych.

# Obwody kwantowe

- Jest to naturalne przeniesienie idei obwodów logicznych na grunt obliczeń kwantowych.
- Można na nich policzyć wszystko to co na obwodach logicznych - np. dzięki odwracalnemu odpowiednikowi bramki NAND (bramka Toffoli'ego), która działa na trzech bitach i zamienia ostatni bit jeśli pierwsze dwa są 1.

# Obwody kwantowe

- Jest to naturalne przeniesienie idei obwodów logicznych na grunt obliczeń kwantowych.
- Można na nich policzyć wszystko to co na obwodach logicznych - np. dzięki odwracalnemu odpowiednikowi bramki NAND (bramka Toffoli'ego), która działa na trzech bitach i zamienia ostatni bit jeśli pierwsze dwa są 1.
- Nadal jednak pozostają pewne niedogodności związane z koniecznością wypisywania wszystkich informacji potrzebnych do odwrócenia obliczeń.

# Obwody kwantowe

- Jest to naturalne przeniesienie idei obwodów logicznych na grunt obliczeń kwantowych.
- Można na nich policzyć wszystko to co na obwodach logicznych - np. dzięki odwracalnemu odpowiednikowi bramki NAND (bramka Toffoli'ego), która działa na trzech bitach i zamienia ostatni bit jeśli pierwsze dwa są 1.
- Nadal jednak pozostają pewne niedogodności związane z koniecznością wypisywania wszystkich informacji potrzebnych do odwrócenia obliczeń.
- Jedną z metod radzenia sobie z nimi jest metoda Bennett'a:

| | | | |
|---|---|---|---|
| INPUT | - | - | - |
| INPUT | OUTPUT | RECORD(F) | - |
| INPUT | OUTPUT | RECORD(F) | OUTPUT |
| INPUT | - | - | OUTPUT |
| INPUT | INPUT | RECORD($F^{-1}$) | OUTPUT |
| - | INPUT | RECORD($F^{-1}$) | OUTPUT |
| - | - | - | OUTPUT |

# Obwody kwantowe

- Jest to naturalne przeniesienie idei obwodów logicznych na grunt obliczeń kwantowych.
- Można na nich policzyć wszystko to co na obwodach logicznych - np. dzięki odwracalnemu odpowiednikowi bramki NAND (bramka Toffoli'ego), która działa na trzech bitach i zamienia ostatni bit jeśli pierwsze dwa są 1.
- Nadal jednak pozostają pewne niedogodności związane z koniecznością wypisywania wszystkich informacji potrzebnych do odwrócenia obliczeń.
- Jedną z metod radzenia sobie z nimi jest metoda Bennett'a:

| | | | |
|---|---|---|---|
| INPUT | - | - | - |
| INPUT | OUTPUT | RECORD(F) | - |
| INPUT | OUTPUT | RECORD(F) | OUTPUT |
| INPUT | - | - | OUTPUT |
| INPUT | INPUT | RECORD($F^{-1}$) | OUTPUT |
| - | INPUT | RECORD($F^{-1}$) | OUTPUT |
| - | - | - | OUTPUT |

# Podnoszenie do potęgi

- Dane $n$,$x$,$r$ - oblicz $x^r \pmod n$.

# Podnoszenie do potęgi

- Dane $n$,$x$,$r$ - oblicz $x^r \pmod n$.
- Idea algorytmu - znana wszystkim.

# Podnoszenie do potęgi

- Dane $n$,$x$,$r$ - oblicz $x^r \pmod n$.
- Idea algorytmu - znana wszystkim.
- Jednak pojawiają się problemy związane z odwracalnością.

# Podnoszenie do potęgi

- Dane $n$,$x$,$r$ - oblicz $x^r \ (mod\ n)$.
- Idea algorytmu - znana wszystkim.
- Jednak pojawiają się problemy związane z odwracalnością.
- Chcemy umieć przechodzić od $|b, 0\rangle$ do $|0, bc \ (mod\ n)\rangle$ gdzie $gcd(c, n) = 1$.

# Podnoszenie do potęgi

- Dane $n$,$x$,$r$ - oblicz $x^r \ (mod\ n)$.
- Idea algorytmu - znana wszystkim.
- Jednak pojawiają się problemy związane z odwracalnością.
- Chcemy umieć przechodzić od $|b, 0\rangle$ do $|0, bc \ (mod\ n)\rangle$ gdzie $gcd(c, n) = 1$.
- Możemy przejść odwracalnie $|b, 0\rangle \rightarrow |b, bc \ (mod\ n))$.

# Podnoszenie do potęgi

- Dane $n$,$x$,$r$ - oblicz $x^r \ (mod\ n)$.
- Idea algorytmu - znana wszystkim.
- Jednak pojawiają się problemy związane z odwracalnością.
- Chcemy umieć przechodzić od $|b, 0\rangle$ do $|0, bc \ (mod\ n)\rangle$ gdzie $gcd(c, n) = 1$.
- Możemy przejść odwracalnie $|b, 0\rangle \rightarrow |b, bc \ (mod\ n))$.
- A także $|0, bc \ (mod\ n)\rangle \rightarrow |bcc^{-1} \ (mod\ n), bc \ (mod\ n)) = |b \ (mod\ n), bc \ (mod\ n))$

# Podnoszenie do potęgi

- Dane $n$,$x$,$r$ - oblicz $x^r \ (mod\ n)$.
- Idea algorytmu - znana wszystkim.
- Jednak pojawiają się problemy związane z odwracalnością.
- Chcemy umieć przechodzić od $|b, 0\rangle$ do $|0, bc \ (mod\ n)\rangle$ gdzie $gcd(c, n) = 1$.
- Możemy przejść odwracalnie $|b, 0\rangle \rightarrow |b, bc \ (mod\ n))$.
- A także $|0, bc \ (mod\ n)\rangle \rightarrow |bcc^{-1} \ (mod\ n), bc \ (mod\ n)) = |b \ (mod\ n), bc \ (mod\ n))$
- A więc możemy najpierw wykonać pierwsze przejście, a potem odwrócone drugie i otrzymamy to o co nam chodzi.

# Podnoszenie do potęgi

- Dane $n$,$x$,$r$ - oblicz $x^r \ (mod\ n)$.
- Idea algorytmu - znana wszystkim.
- Jednak pojawiają się problemy związane z odwracalnością.
- Chcemy umieć przechodzić od $|b, 0\rangle$ do $|0, bc \ (mod\ n)\rangle$ gdzie $gcd(c, n) = 1$.
- Możemy przejść odwracalnie $|b, 0\rangle \rightarrow |b, bc \ (mod\ n))$.
- A także $|0, bc \ (mod\ n)\rangle \rightarrow |bcc^{-1} \ (mod\ n), bc \ (mod\ n)) = |b \ (mod\ n), bc \ (mod\ n))$
- A więc możemy najpierw wykonać pierwsze przejście, a potem odwrócone drugie i otrzymamy to o co nam chodzi.
- Jest jeszcze kwestia błedów w obliczeniach.

# Kwantowa transformata Fouriera

- Chcemy móc transformować w czasie wielomianowym:

$$|a\rangle \rightarrow \frac{1}{q^{\frac{1}{2}}} \sum_{c=0}^{q-1} |c(2\Pi iac/q)$$

$(0 \leqslant a \leqslant q)$
przyjmijmy, że $q = 2^l$ i liczbę $a$ reprezentujemy jako stan $|a_{l-1} \cdots a_0\rangle$.

- Rozbijemy cała transformację (której macierz ma wykładniczy rozmiar) na lokalne transformacje:
$R_j$ operująca na j- tym bicie: $\begin{vmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{vmatrix}$

# Kwantowa transformata Fouriera cd.

- oraz $S_{j,k}$, operujący na bitach $j < k$:

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & exp(i\ _{k-j}) \end{vmatrix} \text{ gdzie } \ _{k-j} = \frac{\Pi}{2^{k-j}}.$$

# Kwantowa transformata Fouriera cd.

- oraz $S_{j,k}$, operujący na bitach $j < k$:

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & exp(i\ _{k-j}) \end{vmatrix} \text{ gdzie } \ _{k-j} = \frac{\Pi}{2^{k-j}}.$$

- Aplikujemy je w porządku:
  $R_{l-1} S_{l-2,l-1} R_{l-2} S_{l-3,l-1} S_{l-3,l-2} R_{l-3} \cdots R_1 S_{0,l-1} S_{0,l-2} \cdots S_{0,2} S_{0,1} R_0$;

# Obliczanie rzędu elementu, a faktoryzacja

- Dane $n, x$, oblicz najmniejsze takie $r$, że $x^r = 1 \ (mod \ n)$.

# Obliczanie rzędu elementu, a faktoryzacja

- Dane $n, x$, oblicz najmniejsze takie $r$, że $x^r = 1 \ (mod \ n)$.
- Jeśli potrafimy znajdować szybko rząd elementu to (o ile $n$ nie jest potęgą liczby pierwszej) z dużym prawdopodobieństwem, $r$ będzie parzysty i: $(x^{r/2} - 1)(x^{r/2} + 1) = x^r - 1 = 0 \ (mod \ n)$ będzie rozkładało nietrywialnie $n$.

# Algorytm

- Dane $n, x$, znajdujemy takie $q = 2^l$, że $n^2 \leqslant q \leqslant 2n^2$. $n$,$x$ oraz $q$ zaszywamy w nasz obwód.

# Algorytm

- Dane $n, x$, znajdujemy takie $q = 2^l$, że $n^2 \leqslant q \leqslant 2n^2$. $n$,$x$ oraz $q$ zaszywamy w nasz obwód.
- Będziemy mieli jeden rejestr $(mod\ q)$ i drugi $(mod\ n)$ oraz jeden rejestr roboczy.

# Algorytm

- Dane $n, x$, znajdujemy takie $q = 2^l$, że $n^2 \leqslant q \leqslant 2n^2$. $n$,$x$ oraz $q$ zaszywamy w nasz obwód.
- Będziemy mieli jeden rejestr $(mod\ q)$ i drugi $(mod\ n)$ oraz jeden rejestr roboczy.
- Zaczynamy od jednostajnego rozkładu prawdopodobieństwa:

$$\frac{1}{q^{\frac{1}{2}}} \sum_{a=0}^{q-1} |a, 0\rangle$$

osiągamy to poprzez aplikowanie do każdego bitu transformacji $|a_i\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

# Algorytm

- Dane $n, x$, znajdujemy takie $q = 2^l$, że $n^2 \leqslant q \leqslant 2n^2$. $n$,$x$ oraz $q$ zaszywamy w nasz obwód.
- Będziemy mieli jeden rejestr $(mod\ q)$ i drugi $(mod\ n)$ oraz jeden rejestr roboczy.
- Zaczynamy od jednostajnego rozkładu prawdopodobieństwa:

$$\frac{1}{q^{\frac{1}{2}}} \sum_{a=0}^{q-1} |a, 0\rangle$$

osiągamy to poprzez aplikowanie do każdego bitu transformacji $|a_i\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

- podnosimy do potęgi

$$\frac{1}{q^{\frac{1}{2}}} \sum_{a=0}^{q-1} |a, x^a\ (mod\ n)\rangle$$

# Algorytm cd.

- stosujemy transformatę Fouriera

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1} exp(2\Pi iac/q)|c, x^a \ (mod\ n)\rangle$$

# Algorytm cd.

- stosujemy transformatę Fouriera

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1} exp(2\Pi iac/q)|c, x^a \ (mod\ n)\rangle$$

- i patrzymy na liczbę zapisaną w pierwszym rejestrze - z dużym prawdopodobieństwem będzie ona taka, że:

$$|\frac{c}{q} - \frac{d}{r}| \leqslant \frac{1}{2q}$$

.

# Algorytm cd.

- stosujemy transformatę Fouriera

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1} exp(2\Pi iac/q)|c, x^a \ (mod\ n)\rangle$$

- i patrzymy na liczbę zapisaną w pierwszym rejestrze - z dużym prawdopodobieństwem będzie ona taka, że:

$$|\frac{c}{q} - \frac{d}{r}| \leqslant \frac{1}{2q}$$

.

- szukamy teraz rozwinięcia $\frac{c}{q}$ do pierwszego takiego reduktu, którego mianownik jest mniejszy od $n$. Z dużym prawdopodobieństwem to jest $r$.

# Algorytm

- Dane $p, x, g$, znajdź takie $r$, że $g^r = x (mod\ p)$.

# Algorytm

- Dane $p, x, g$, znajdź takie $r$, że $g^r = x (mod\ p)$.
- Znajdujemy takie $q = 2^l$, że $p \leqslant q \leqslant 2p$. Będziemy mieli dwa rejestry $(mod\ p - 1)$ i jeden $(mod\ p)$.

# Algorytm

- Dane $p, x, g$, znajdź takie $r$, że $g^r = x (mod\ p)$.
- Znajdujemy takie $q = 2^l$, że $p \leqslant q \leqslant 2p$. Będziemy mieli dwa rejestry $(mod\ p - 1)$ i jeden $(mod\ p)$.
- Zaczynamy od jednostajnego rozkładu prawdopodobieństwa po wszystkich $a$ i $b$, a następnie obliczamy $g^a x^{-b} (mod\ p)$ w trzecim rejestrze:

$$\frac{1}{p-1} \sum_{a=0}^{p-2} \sum_{b=0}^{p-2} |a, b, g^a x^{-b} (mod\ p)\rangle$$

# Algorytm

- Dane $p, x, g$, znajdź takie $r$, że $g^r = x(mod\ p)$.
- Znajdujemy takie $q = 2^l$, że $p \leqslant q \leqslant 2p$. Będziemy mieli dwa rejestry $(mod\ p-1)$ i jeden $(mod\ p)$.
- Zaczynamy od jednostajnego rozkładu prawdopodobieństwa po wszystkich $a$ i $b$, a następnie obliczamy $g^a x^{-b}(mod\ p)$ w trzecim rejestrze:

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a, b, g^a x^{-b}(mod\ p)\rangle$$

- stosujemy transformatę Fouriera na pierwszy i drugi rejestr (osobno) otrzymując dla $|a, b\rangle$ stan:

$$\frac{1}{q}\sum_{c=0}^{q-1}\sum_{d=0}^{q-1} exp(2\Pi i/q(ac+bd))|c, d\rangle$$

# Algorytm cd.

- czyli całość jest w stanie:

$$\frac{1}{p-1}\sum_{a,b=0}^{p-2}\sum_{c,d=0}^{q-1} exp(2\Pi i/q(ac+bd))|c,d,g^a x^{-b}(mod\ p)\rangle$$

# Algorytm cd.

- czyli całość jest w stanie:

$$\frac{1}{p-1}\sum_{a,b=0}^{p-2}\sum_{c,d=0}^{q-1} exp(2\Pi i/q(ac+bd))|c,d,g^a x^{-b}(mod\ p)\rangle$$

- i patrzymy na liczby $|c,d,y\rangle$ w rejestrach i zaokrąglamy $\frac{d}{q}$ do najbliższej wielokrotności $\frac{1}{p-1}$ i dzielimy $(mod\ p-1)$ przez

$$c' = \frac{c(p-1) - c(p-1)_q}{q}$$

otrzymując z dużym prawdopodobieństwem $r$.

# Czemu nie mamy (jeszcze) komputerów kwantowych

- rozstrojenie układu kwantowego
- precyzja przekształceń
- zbudowanie układu n-poziomowego (na razie) wymaga wykładniczej ilości kubitów
- problemy NP-zupełne