Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 467 / Phys 767
C&O 481 / C&O 681

Lecture 9 (2005)

Richard Cleve
DC 3524
cleve@cs.uwaterloo.ca

Course web site at:
http://www.cs.uwaterloo.ca/~cleve/courses/cs467

Contents

- Loose ends in discrete log algorithm
- Universal sets of quantum gates

- Loose ends in discrete log algorithm
- Universal sets of quantum gates

Discrete log algorithm (I)

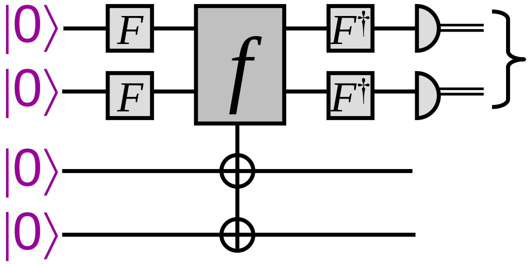
Input: p (n-bit prime), g (generator of $\mathbf{Z}^*_p$), $a \in \mathbf{Z}^*_p$

Output: $r \in \mathbf{Z}_{p-1}$ such that $g^r \bmod p = a$

Example: $p = 7$, $\mathbf{Z}^*_7 = \{1, 2, 3, 4, 5, 6\} = \{3^0, 3^2, 3^1, 3^4, 3^5, 3^3\}$
(hence 3 is a generator of $\mathbf{Z}^*_7$)

Define $f : \mathbf{Z}_{p-1} \times \mathbf{Z}_{p-1} \rightarrow \mathbf{Z}^*_p$ as $f(x, y) = g^x a^{-y} \bmod p$

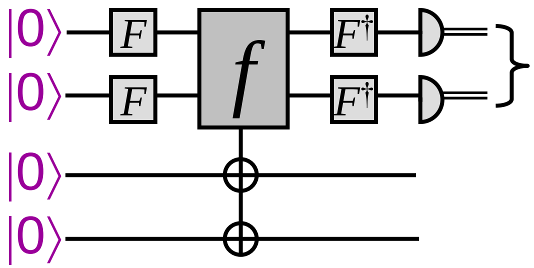
Then $f(x_1, y_1) = f(x_2, y_2)$ iff $(x_1, y_1) - (x_2, y_2) \equiv k(r, 1) \pmod{p-1}$
(for some k)



produces a random (s, t) such that
$(s, t) \cdot (r, 1) \equiv 0 \pmod{p-1}$

$\Leftrightarrow sr + t \equiv 0 \pmod{p-1}$

Discrete log algorithm (II)



produces a random (s, t) such that $sr + t \equiv 0 \pmod{p-1}$

If $\gcd(s, p-1) = 1$ then r can be computed as $r = -ts^{-1} \bmod p-1$

The probability that this occurs is $\phi(p-1)/(p-1)$, where ϕ is ***Euler's totient function***

It is known that $\phi(N) = \Omega(N/\log\log N)$, which implies that the above probability is at least $\Omega(1/\log\log p) = \Omega(1/\log n)$

Therefore, $O(\log n)$ repetitions are sufficient

… this is not bad—but things are actually better than that …

Discrete log algorithm (III)

We obtain a random (s, t) such that $sr + t \equiv 0 \pmod{p-1}$

Note that each $s \in \{0,\ldots, p-2\}$ occurs with equal probability

Therefore, if we run the algorithm ***twice***: we obtain two independent samples $s_1, s_2 \in \{0,\ldots,p-2\}$

If it happens that $\gcd(s_1, s_2) = 1$ then (by Euclid) there exist integers a and b such that $as_1 + bs_2 = 1$ ➔ $r = -(at_1 + bt_2)$

Question: what is the probability that $\gcd(s_1, s_2) = 1$?

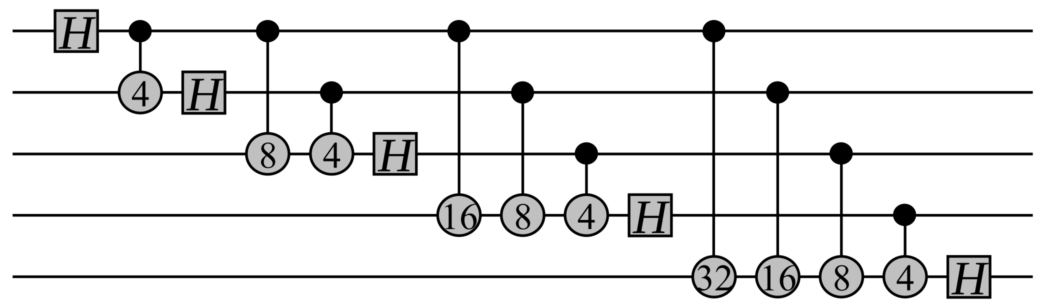
$$1 - \sum_{q \text{ prime}} \Pr[q \mid s_1] \Pr[q \mid s_2] > 1 - \sum_{q \text{ prime}} \frac{1}{q^2} > 0.54$$

Therefore, a ***constant*** number of repetitions suffices

Discrete log algorithm (IV)

***Another* loose end:** our algorithm uses QFTs modulo $p-1$, whereas we have only seen how to compute QFTs modulo 2^n

$$\frac{1}{\sqrt{N}}\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{bmatrix}$$



A variation of our QFT algorithm would work for moduli of the form 3^n, and, more generally, all ***smooth*** numbers (those that are products of “small” primes)

Discrete log algorithm (V)

In fact, for the case where $p-1$ is smooth, there already exist polynomial-time ***classical*** algorithms for discrete log!

It's only the case where $p-1$ is ***not*** smooth that is interesting

Shor just used a modulus ***close to*** $p-1$, and, using careful error-analysis, showed that this was good enough ...

There are also ways of attaining good approximations of QFTs for arbitrary moduli (which we won't consider now)

- Loose ends in discrete log algorithm
- Universal sets of quantum gates

A universal set of gates (I)

Main Theorem: any unitary operation U acting on k qubits can be decomposed into $O(4^k)$ CNOT and one-qubit gates

Proof sketch (for a slightly worse bound of $O(k^2 4^k)$) **:**

We first show how to simulate a controlled-U, for any one-qubit unitary U

Straightforward to show: every one-qubit unitary matrix can be expressed as a product of the form

$$\begin{bmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{bmatrix} \begin{bmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{bmatrix} \begin{bmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \begin{bmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{bmatrix}$$

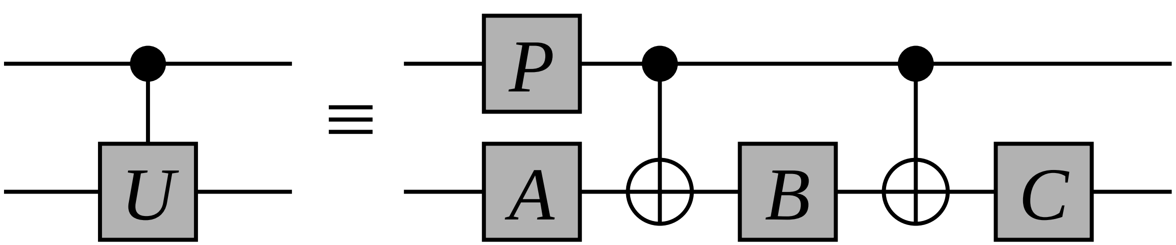
A universal set of gates (II)

This can be used to show that, for every one-qubit unitary U, there exist A, B, C, and λ, such that:

- $A\,B\,C = I$
- $e^{i\lambda} A\,X\,B\,X\,C = U$, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Exercise: show how this follows

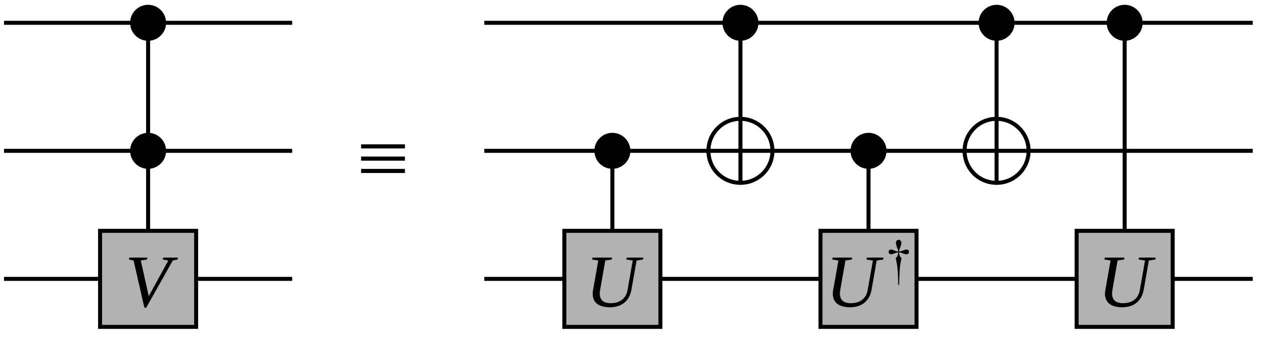
The fact implies that



where $P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix}$

A universal set of gates (III)

Controlled-U gates can also simulate <u>controlled-controlled</u>-V gates, for an arbitrary unitary one-qubit unitary V:

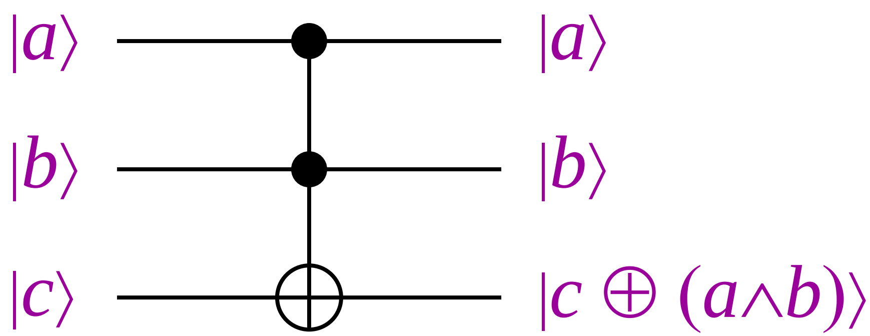


where $V = U^2$

A universal set of gates (IV)

Example: Toffoli gate

"controlled-controlled-NOT"

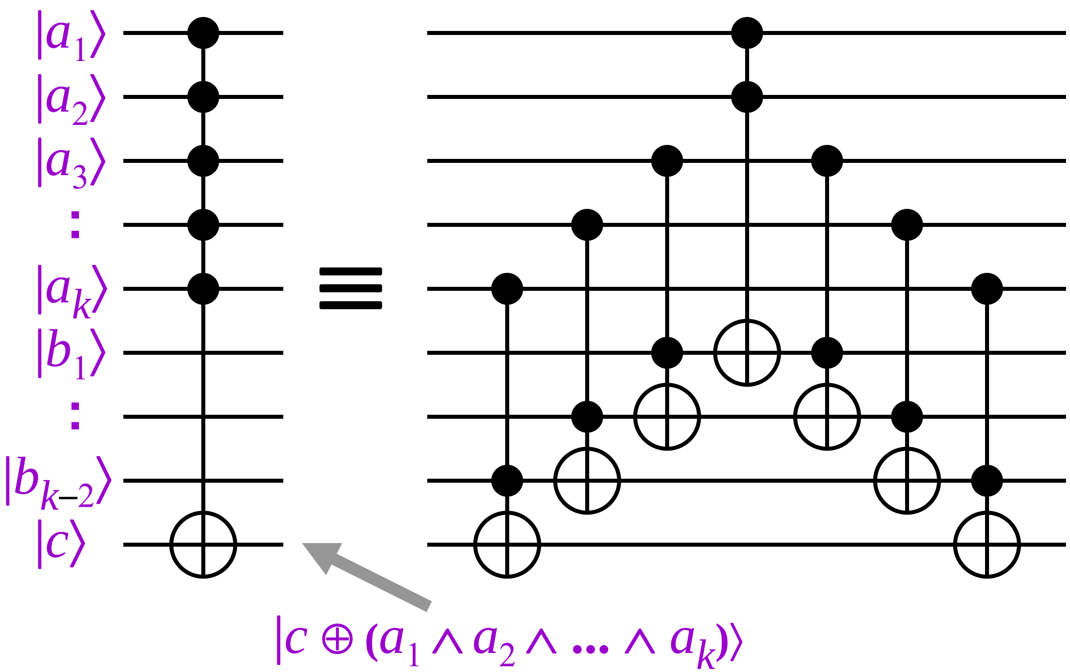


In this case, the one-qubit gates can be:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

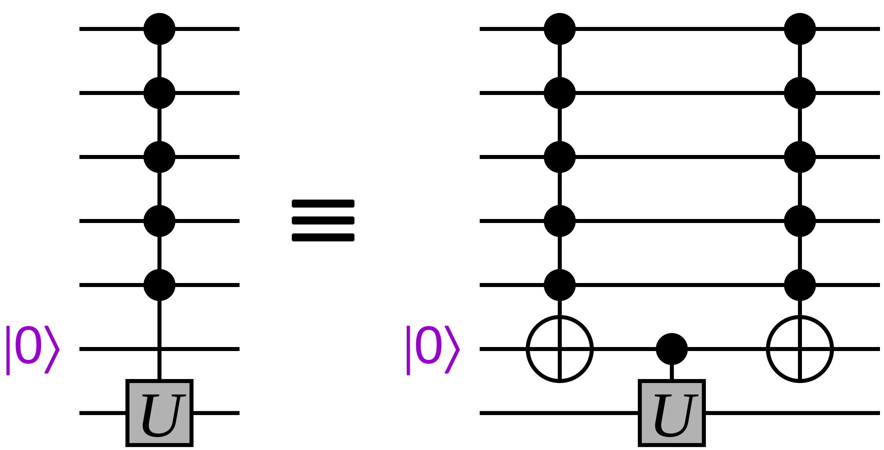
A universal set of gates (V)

From the Toffoli gate, ***generalized*** Toffoli gates (which are controlled-controlled- ... -NOT gates) can be constructed:



A universal set of gates (VI)

From generalized Toffoli gates, ***generalized controlled-U*** gates (controlled-controlled- ... -U) can be constructed:



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{10} & U_{11} \end{pmatrix}$$

A universal set of gates (VII)

The approach essentially enables any k-qubit operation of the simple form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_{00} & 0 & 0 & U_{01} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & U_{10} & 0 & 0 & U_{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

to be computed with $O(k^2)$ CNOT and one-qubit gates

In a spirit similar to Gaussian elimination, any $2^k \times 2^k$ unitary matrix can be decomposed into a product of $O(4^k)$ of these

A universal set of gates (VIII)

This completes the proof sketch*

Thus, the set of ***all*** one-qubit gates and the CNOT gate are ***universal*** in that they can simulate any other gate set

Question: is there a ***finite*** set of gates that is universal?

Answer 1: strictly speaking, ***no***, because this results in only countably many quantum circuits, whereas there are uncountably many unitary operations on k qubits (for any k)

$*$ Actually we proved a slightly worse bound of $O(k^2 4^k)$

Approximately **universal gate sets**

Answer 2: yes, for universality in an ***approximate*** sense ...

To be continued ...

THE END