

Introduction to quantum computing

Miklos Santha

CNRS-LRI Orsay

- Basic facts about quantum computing
- Grover's search
- The hidden subgroup problem
 - Simon's problem
 - Abelian groups
 - Shor's factorization
- Perspectives

- Church – Turing thesis (1936), quantitative version
- Manin (80) – Feynman (82): Simulation of quantum systems
- Benioff (82) – Deutsch (85): QTM
- Bennett – Brassard (84): Q key distribution
- Deutsch (89) – Yao (93): Q circuits
- Bennett et al. (93): Q teleportation
- Bernstein – Vazirani (93): Q complexity
- Lloyd (93): Q cellular automata
- Shor (94): Factorization and discrete logarithm
- Grover (96): Q search
- Hallgren (02): Pell's equation

Classical bit: $b \in \{0, 1\}$

Probabilistic bit

Probability distribution $d \in \mathbb{R}_+^{\{0,1\}}$ such that $\|d\|_1 = 1$.

$\implies d = (p, 1 - p)$ with $p \in [0, 1]$.

Quantum bit

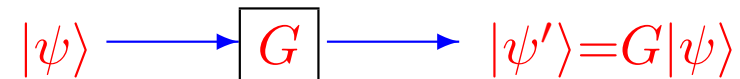
Superposition $|\psi\rangle \in \mathbb{C}^{\{0,1\}}$ such that $\| |\psi\rangle \|_2 = 1$.

$\implies |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Unitary transformation

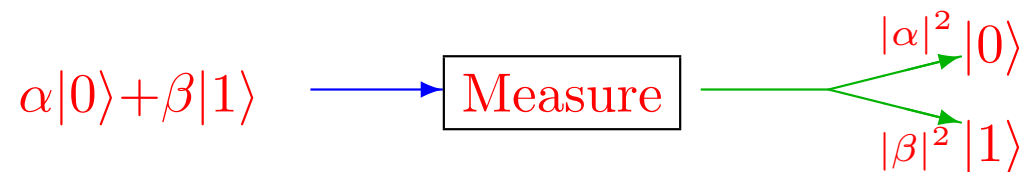
$|\psi\rangle \mapsto G|\psi\rangle$, with $G \in \mathbb{C}^{2 \times 2}$ such that $G^\dagger G = Id$.



Unitary \implies Reversible:



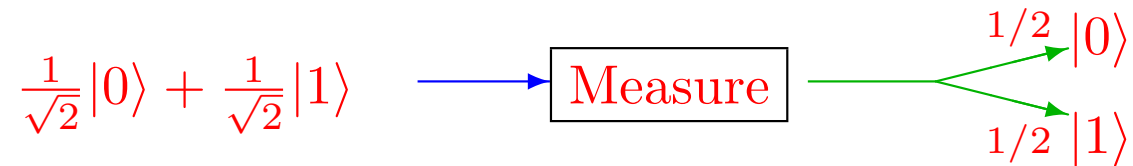
Measure: Reads and modifies.



\implies Superposition \rightarrow Probability distribution.

Superposition: $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

Measure

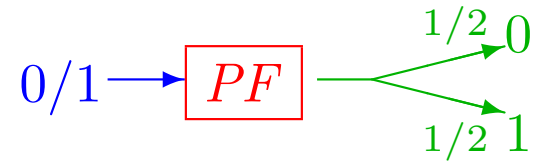


Unitary transformations

$$|\psi\rangle \longrightarrow \boxed{G} \longrightarrow |\psi'\rangle = G|\psi\rangle$$

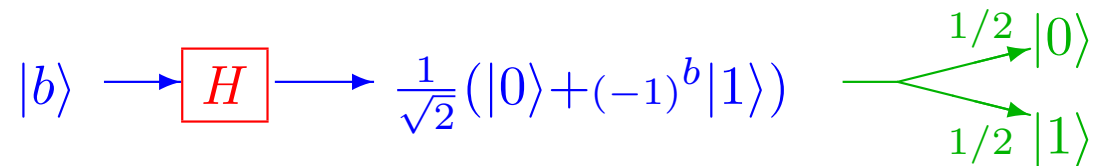
- NOT, $|0\rangle \leftrightarrow |1\rangle$: $G = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Probabilistic flip



Remark: $PF \circ PF = PF$.

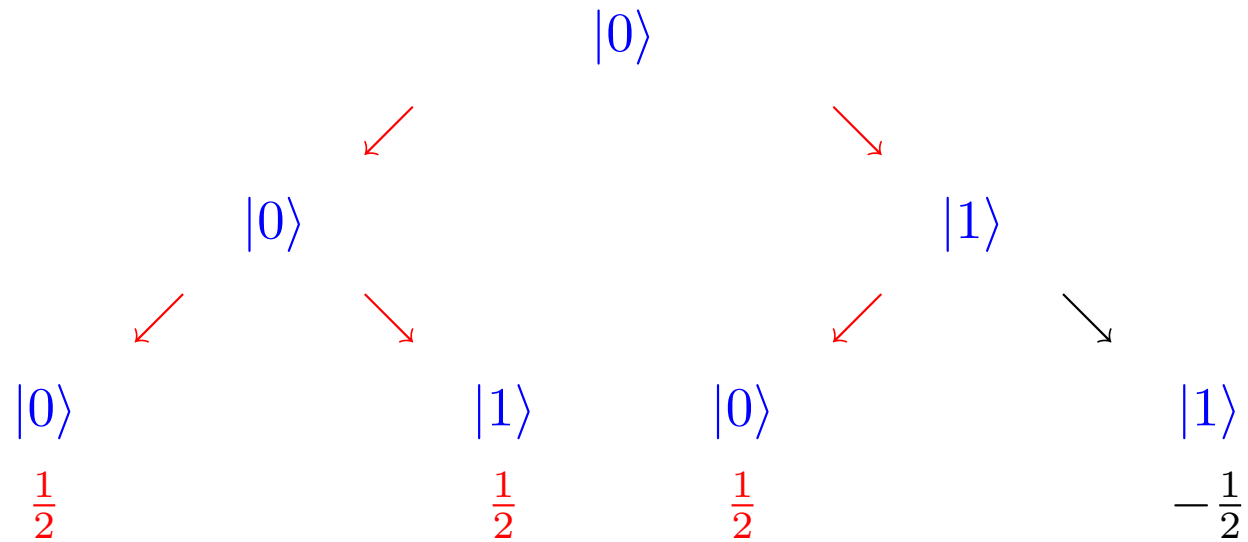
Quantum flip



Conclusion : $PF = \text{Measure} \circ H$.

Question : $H \circ H = ?$

$$\rightarrow : +\frac{1}{\sqrt{2}}, \quad \leftarrow : -\frac{1}{\sqrt{2}}.$$



$$H \circ H|b\rangle = |b\rangle \quad \implies \quad H \circ H = Id.$$

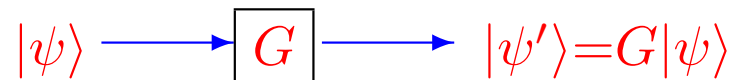
Conclusion : Measures change the computation

Definition: n -qubit \leftrightarrow tensor product of n qubits.

$|\psi\rangle \in \mathbb{C}^{\{0,1\}^n}$ such that $\| |\psi\rangle \|_2 = 1$.

$$\implies |\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \text{ with } \sum_x |\alpha_x|^2 = 1.$$

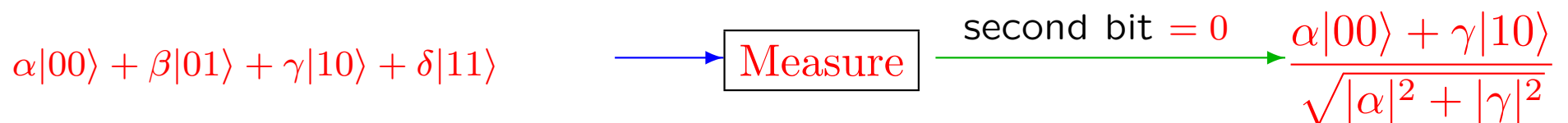
Unitary transformation: $|\psi\rangle \mapsto G|\psi\rangle$, with $G \in U(2^n)$.



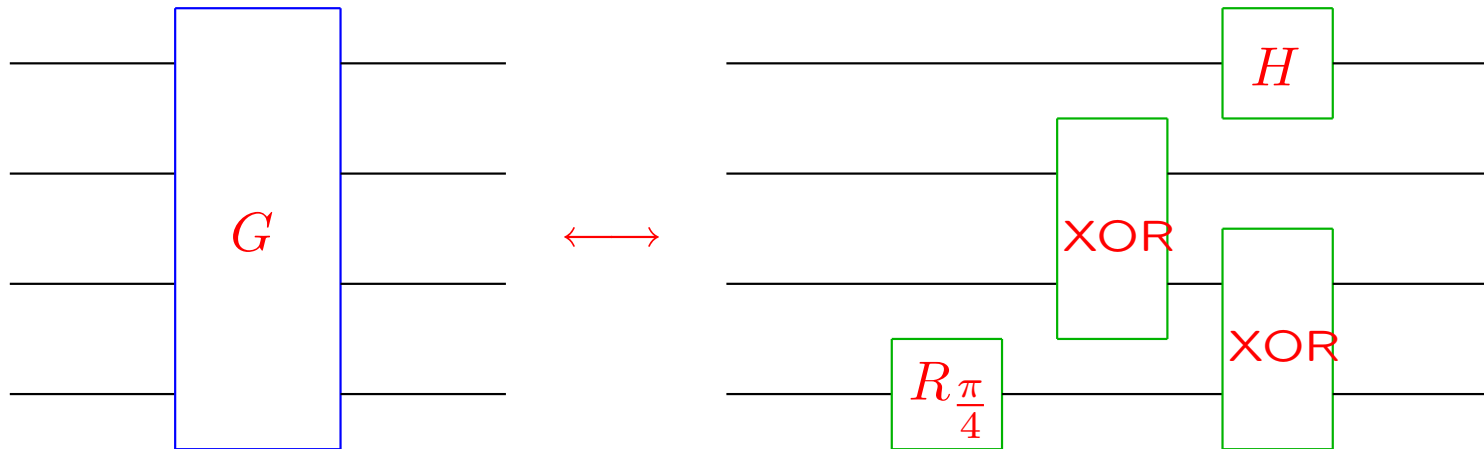
Measure



Partial measure



Quantum circuit: ($G \in U(16)$)

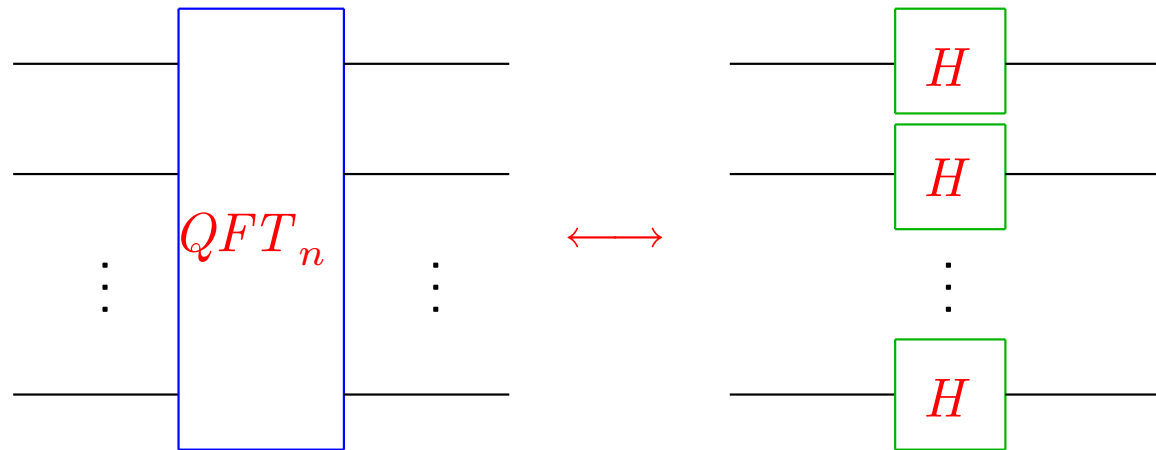


Theorem [DiV95,BMPRV99]:

Every transformation on n -qubit decomposes into transformations on 1-qubit and 2-qubit.

\implies Universal family.

Circuit



Definition

$$QFT_n |x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$$

where $x \cdot y = \sum_i x_i y_i \pmod{2}$

$$\begin{aligned} \text{Let } f : \{0, 1\}^n &\rightarrow \{0, 1\}^m \\ x &\mapsto f(x) \end{aligned}$$

Reversible

$$\begin{aligned} R_f : \{0, 1\}^{n+m} &\rightarrow \{0, 1\}^{n+m} \\ (x, y) &\mapsto (x, y \oplus f(x)) \end{aligned}$$

Quantum

$$\begin{aligned} U_f \in U(2^{n+m}) : \mathbb{C}^{2^{n+m}} &\rightarrow \mathbb{C}^{2^{n+m}} \\ |x\rangle|y\rangle &\mapsto |x\rangle|y \oplus f(x)\rangle \end{aligned}$$

QUANTUM SEARCH

INPUT: $f : \{0, \dots, N - 1\} \rightarrow \{0, 1\}$, $N = 2^n$

$f(i) = 1$ for some $0 \leq i \leq N - 1$

$f(j) = 0 \quad \forall j \neq i$

OUTPUT: i

Complexity : Number of queries to f

Deterministic: N

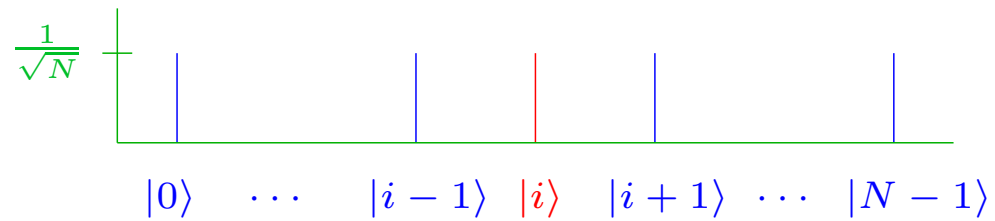
Probabilistic: $N/2$

Quantum:

Theorem (GROVER): $O(\sqrt{N})$

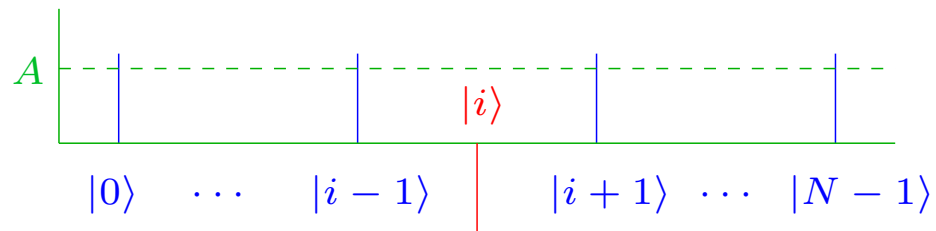
GROVER'S ALGORITHM

- Initialization

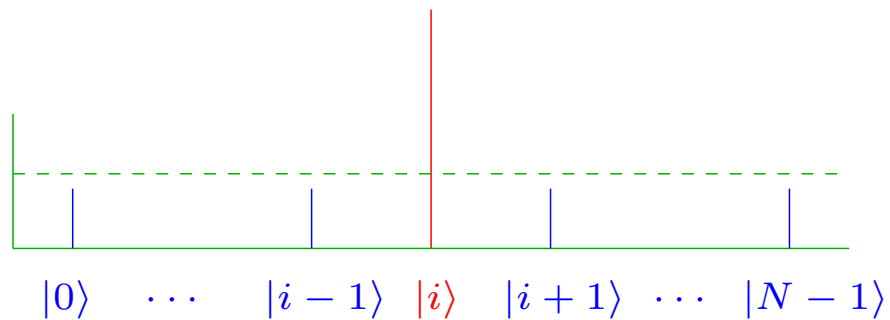


- Repeat $O(\sqrt{N})$ times

- Phase shift for $|i\rangle$



- Inversion about the average



Amplitude of $|i\rangle$ increases by $O(\frac{1}{\sqrt{N}})$.

After $O(\sqrt{N})$ repetitions it becomes $O(1)$.

INVERSION ABOUT THE AVERAGE

The dispersion matrix:

$$\begin{aligned} D &= \begin{pmatrix} -1 + \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & -1 + \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & & \ddots & \\ \frac{2}{N} & & & -1 + \frac{2}{N} \end{pmatrix} \\ &= - \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \\ 0 & & 1 \end{pmatrix} + 2 \begin{pmatrix} \frac{1}{N} & \cdots & \frac{1}{N} \\ \vdots & \ddots & \\ \frac{1}{N} & & \frac{1}{N} \end{pmatrix} \\ &= -I + 2P \end{aligned}$$

Unitarity:

$$P^2 = P \Rightarrow D^2 = I$$

Inversion:

$$(P \cdot v)_k = A, \quad A = \text{average of } v$$

$$(D \cdot v)_k = -v_k + 2A = A + (A - v_k)$$

IMPLEMENTATION

- Initialization:

$$QFT_n |0^n\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$$

- Phase flip for $|i\rangle$:

Apply U_f with an ancilla

$$\begin{aligned} |x\rangle (|0\rangle - |1\rangle) &\rightarrow |x\rangle (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle) \end{aligned}$$

- Dispersion:

$$D = QFT_n \circ R \circ QFT_n$$

where

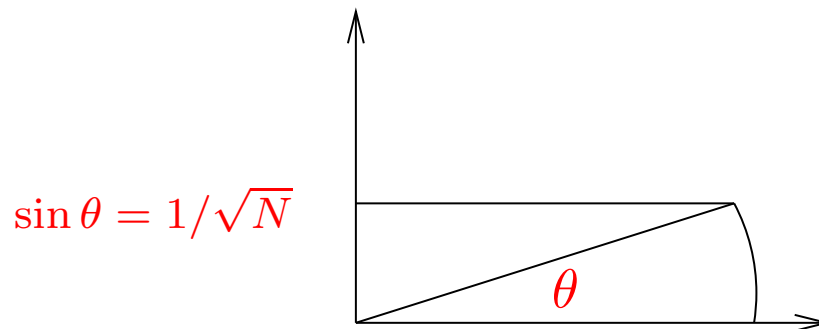
$$R = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & & \ddots & \\ 0 & & & -1 \end{pmatrix}$$

ANALYSIS

Recursion for the amplitudes:

$$\left. \begin{aligned} r_0 &= 1/\sqrt{N} \\ b_0 &= 1/\sqrt{N} \end{aligned} \right\}$$
$$\left. \begin{aligned} r_{k+1} &= \frac{N-2}{N}r_k + \frac{2(N-1)}{N}b_k \\ b_{k+1} &= \frac{N-2}{N}b_k - \frac{2(N-1)}{N}r_k \end{aligned} \right\}$$

Explicit solution:



$$\left. \begin{aligned} r_k &= \sin(2k + 1)\theta \\ b_k &= \frac{1}{\sqrt{N-1}} \cos(2k + 1)\theta \end{aligned} \right\}$$

Optimum number of iterations:

$$r_k = 1 \Leftrightarrow k = \frac{\pi - 2\theta}{4\theta} \approx \frac{\pi}{4} \cdot \sqrt{N}$$

The problem

Input: $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ such that

$$\exists s \neq 0^n, \quad f(x) = f(y) \iff (x = y \quad \text{or} \quad x = y \oplus s)$$

Output: s

Constraint: f is a black box.

Complexity: Number of evaluations of f and computing time.

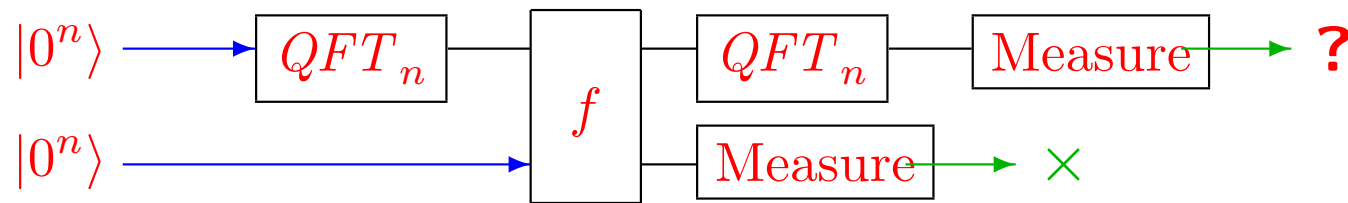
Deterministically: $2^{n-1} + 1$ evaluations.

Probabiliste : $\Omega(2^{n/2})$ evaluations.

Quantum algorithm [Simon'94]: $O(n)$ evaluations and $O(n^3)$ time.

Idea: Use QFT_n to find the period s .

Circuit



Analysis

- Initialization : $|0^n\rangle|0^n\rangle$
- Fourier on 1st register: $\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |0^n\rangle$
- Evaluation of f : $\frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle$
- Measure of 2nd register: $\frac{1}{\sqrt{2}} (|x\rangle + |x \oplus s\rangle) |f(x)\rangle$
- Fourier on 1st register: $\frac{1}{2^{n/2}\sqrt{2}} \sum_y ((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}) |y\rangle$
 $= \frac{1}{2^{n/2}\sqrt{2}} \sum_y (-1)^{x \cdot y} (1 + (-1)^{s \cdot y}) |y\rangle$
- Measure of 1st register: uniform $|y\rangle$ such that $s \cdot y = 0$

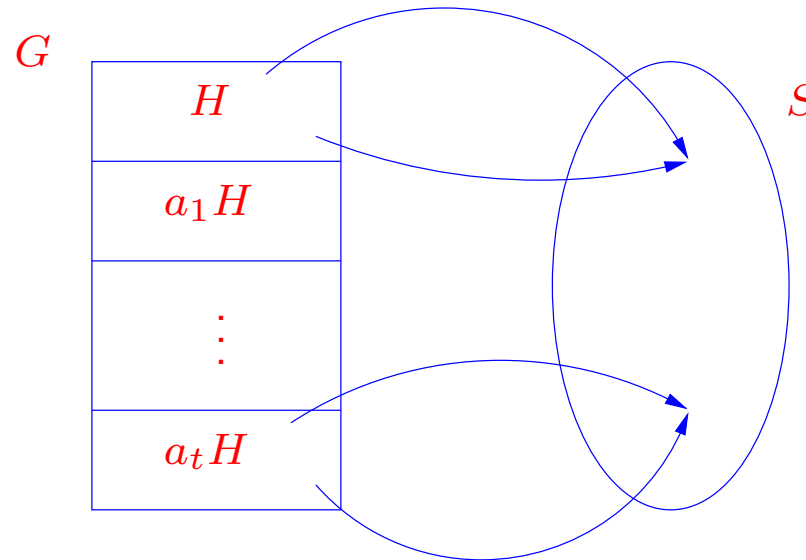
Conclusion

After $O(n)$ iterations, system of rank $n-1 \implies 2$ solutions : $\{0^n, s\}$.

The problem

Input: Finite group G and $f : G \rightarrow S$ which hides $H \leq G$: constant and distinct on the left cosets of H .

Output: Generators for H .



Theorem: If G is Abelian then there is a quantum algorithm

- which finds H with probability $\geq 1 - 1/|G|$,
- in polynomial time in $\log|G|$.

G : Abelian group.

Definition

A character $\chi : G \rightarrow \mathbb{C}^*$ is a group homomorphism.

$\widehat{G} = \{\text{characters of } G\}$.

Remark: $\chi(x)$ is a $|G|^{\text{th}}$ root of the unity.

Theorem: G and \widehat{G} are isomorphic $\leadsto \widehat{G} = \{\chi_y : y \in G\}$.

Examples : $G = \mathbb{Z}_d \leadsto \chi_y(x) = \omega_d^{x \cdot y}$.

$G = G_1 \times G_2 \leadsto \chi_y(x) = \chi_{y_1}(x_1)\chi_{y_2}(x_2)$.

Orthogonality

$H \leq G \mapsto H^\perp = \{y \in G : \forall h \in H, \chi_y(h) = 1\}$.

Lemma. Let $H \leq G$.

There is a deterministic algorithms which finds H from a set of generators for H^\perp in time $O(\log^3 |G|)$.

G : Abelian group.

Bases

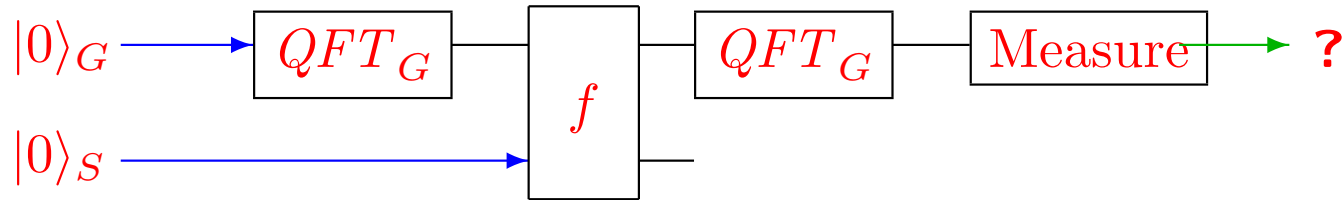
- Dirac: $(\delta_x)_{x \in G} \rightsquigarrow |\delta_x\rangle = |x\rangle$.
- Characters: $(\chi_y)_{y \in G} \rightsquigarrow |\chi_y\rangle = \sum_x \chi_y(x) |x\rangle$.

Definition: $QFT_G : |y\rangle \mapsto \frac{1}{\sqrt{|G|}} |\chi_y\rangle$.

Principal property. $H \leq G, x \in G$.

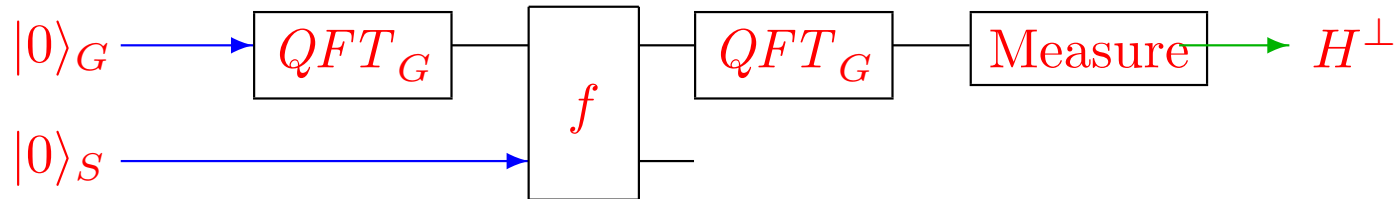
$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + h\rangle = |x + H\rangle \xrightarrow{QFT_G} |H^\perp(x)\rangle = \frac{1}{\sqrt{|H^\perp|}} \sum_{y \in H^\perp} \chi_y(x) |y\rangle.$$

Theorem: Efficient implementation of QFT_G .

Circuit : Fourier sampling^f (G)**Analysis**

- Initialization : $|0\rangle_G |0\rangle_S$
- Fourier on 1st register : $\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |0\rangle$
- Query of f : $\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle = |f\rangle$
- Fourier on 1st register : $\frac{1}{|G|} \sum_{x, y \in G} \chi_y(x) |y\rangle |f(x)\rangle$
 $= \frac{1}{\sqrt{|G|}} \sum_{x \in G} |\{0\}^\perp(x)\rangle |f(x)\rangle$
- Measure of 1st register : ...

Circuit : Fourier sampling ^{f} (G)



Analysis

- Initialization : $|0\rangle_G |0\rangle_S$
- Fourier on 1st register : $\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |0\rangle$
- Query of f : $|f\rangle = \frac{1}{\sqrt{|G/H|}} \sum_{x \in G/H} |x + H\rangle |f(x)\rangle$
- Fourier on 1st register : $\frac{1}{\sqrt{|G/H|}} \sum_{x \in G/H} |H^\perp(x)\rangle |f(x)\rangle$
- Measure of 1st register : $|y\rangle$ uniform in H^\perp .

$$G = \{0, 1\}^n$$

$$H = \{0^n, s\} \quad \text{for some } 0^n \neq s \in \{0, 1\}^n$$

$$f(x) = f(y) \quad \text{iff } x = y \quad \text{or } x \oplus y = s$$

The characters

$$\begin{aligned} \chi_y : \{0, 1\}^n &\rightarrow \mathbb{C} && \text{for } y \in \{0, 1\}^n \\ x &\mapsto (-1)^{x \cdot y} \end{aligned}$$

$$\text{where } x \cdot y = \sum_{i=1}^n x_i y_i \pmod{2}$$

Conclusion

$$H^\perp = \{y : s \cdot y = 0\}$$

$n-1$ independent elements of H^\perp determine H .

Factorization

Input: a composite number $n \in \mathbb{N}$.

Output: a non trivial divisor of n .

Order finding

Input: $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^*$.

Output: the period r of $x \rightarrow a^x \pmod n$.

Lemma: Factorization \leq_R Order finding.

Let $a \in \mathbb{Z}_n$ random.

- Verify that $\gcd(a, n) = 1$.
- Compute the period r of $x \rightarrow a^x \pmod n$.
- Restart if r is odd or $a^{r/2} = -1 \pmod n$.
(otherwise $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \pmod n$.)
- Output $\gcd(a^{r/2} \pm 1, n)$.

Input: q, n and $a \in \mathbb{Z}_n^*$ such that $r = \text{order}(a) \bmod n$ divides q

Output : r

$G = \mathbb{Z}_q$, $H = \{0, r, 2r, \dots\}$, H is a subgroup.

The hiding function:

$$f : \mathbb{Z}_q \rightarrow \mathbb{Z}_n$$

$$x \mapsto a^x \bmod n$$

Characters:

$$\chi_k : \mathbb{Z}_q \rightarrow \mathbb{C} \quad \text{for } k \in \mathbb{Z}_q$$

$$x \rightarrow e^{2\pi i \frac{kx}{q}}$$

$\chi_k(r) = 1$ iff q/r divides k , $H^\perp = \{k : q/r \text{ divides } k\}$

Output of Fourier sampling:

Random element of H^\perp : tq/r where $t \in_R \{0, 1, \dots, r-1\}$

If $\gcd(t, r) = 1$ then $\gcd(tq/r, q) = q/r$

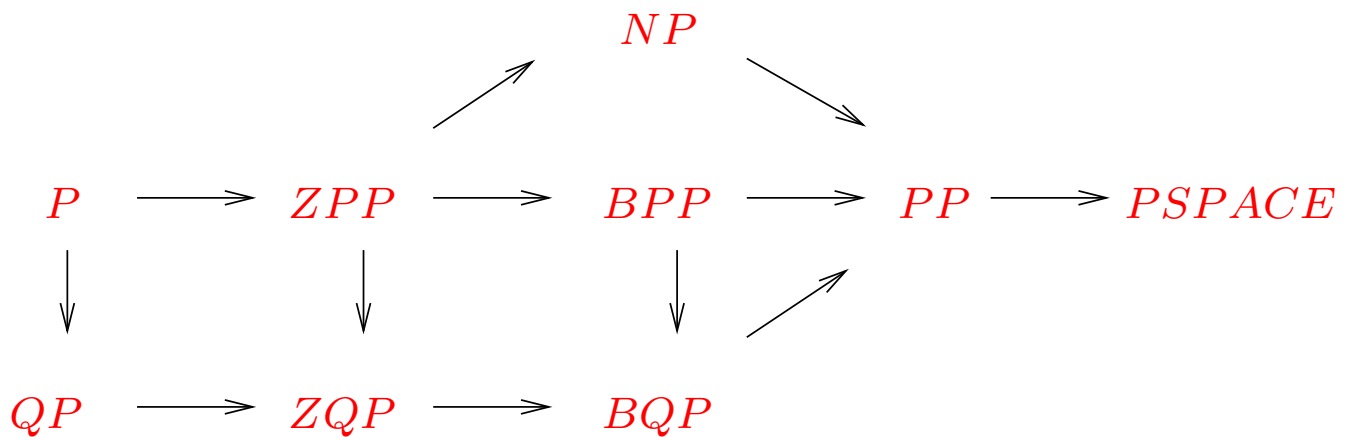
Theorem (Shor): The algorithm can be extended to $G = \mathbb{Z}$

QUANTUM COMPLEXITY CLASSES

QP : — polynomial time
— no error

ZQP : — expected polynomial time
— no error

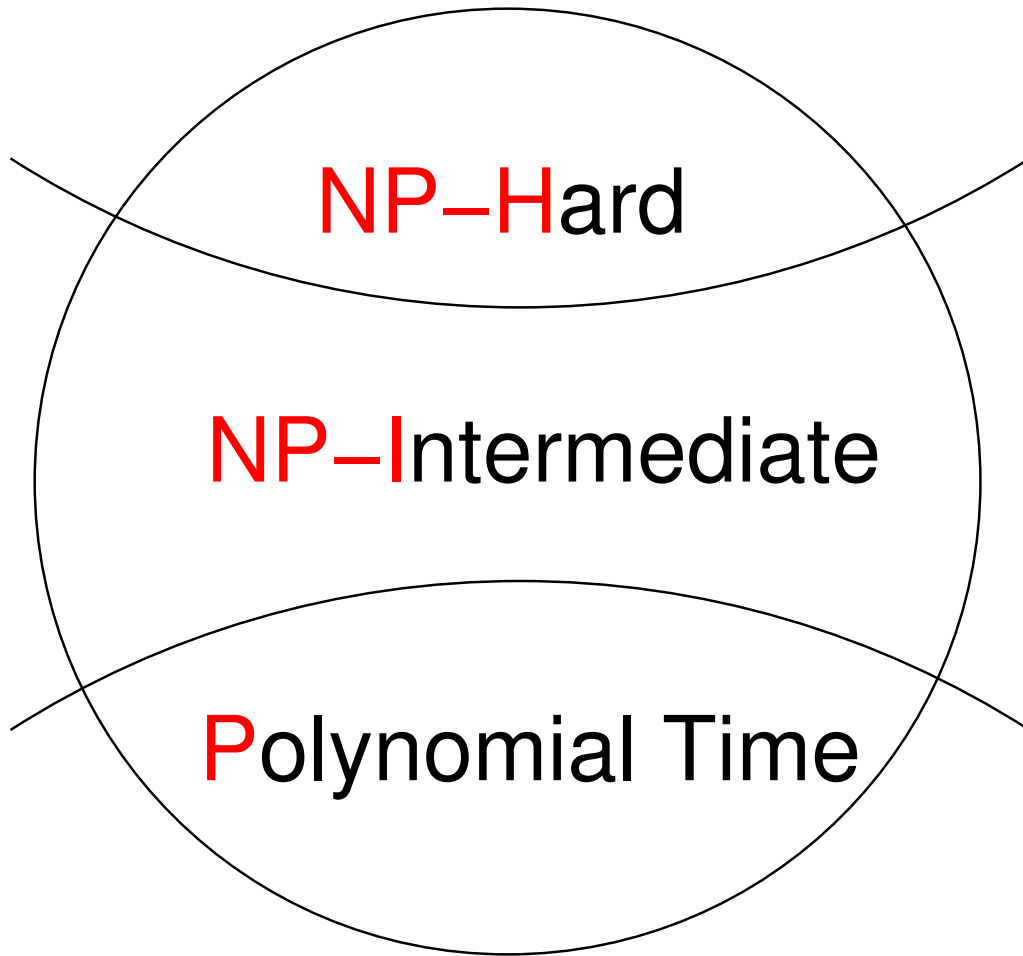
BQP : — polynomial time
— error $\leq \frac{1}{3}$



$\mathcal{L} = \{(x, y) : x \text{ has a prime divisor } < y\} \in ZQP$

Conjecture: $\mathcal{L} \notin BPP$

CLASSICAL COMPLEXITY CLASSES



- *P*: Efficient classical algorithms
- *NP-I*: Maybe efficient quantum algorithms
- *NP-H*: Probably no efficient quantum algorithms

NP- INTERMEDIATE PROBLEMS

1. GRAPH ISOMORPHISM

INPUT: $G_1 = (V, E_1), G_2 = (V, E_2)$

QUESTION : Is there $f : V \rightarrow V$ such that
 $\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$?

2. HIDDEN SUBGROUP

INPUT: G finite group

$\gamma : G \rightarrow X$

γ is constant and distinct on the
cosets of a subgroup H of G .

OUTPUT : Generating set for H

3. SHORTEST VECTOR

INPUT: A basis v_1, \dots, v_n for a lattice

$L \subseteq \mathbb{Z}^n$ and $w > 0$

QUESTION : Is there $0^n \neq x \in L$ such that
 $\|x\|^2 \leq w$?

NP- INTERMEDIATE PROBLEMES

4. PIGEONHOLE SUBSET SUM

INPUT: $s_1, \dots, s_n \in \mathbb{N}$ such that

$$\sum_{i=1}^n s_i < 2^n$$

OUTPUT: $I_1 \neq I_2 \subseteq \{1, \dots, n\}$ such that

$$\sum_{i \in I_1} s_i = \sum_{i \in I_2} s_i$$

5. IDENTICAL PRODUCT

INPUT: $s_1, \dots, s_n \in \mathbb{N}$, $s_i < p < 2^n$

OUTPUT: $I_1 \neq I_2 \subseteq \{1, \dots, n\}$ such that

$$\prod_{i \in I_1} s_i = \prod_{i \in I_2} s_i \pmod{p}$$

6. HAPPYNET

INPUT: $G_1 = (V, E_1)$ and $w : E \rightarrow \mathbb{Z}$

OUTPUT : $S : V \rightarrow \{-1, 1\}$ such that $\forall i \in V$

$$S(i) \sum_{\{i,j\} \in E} S(j)w(i,j) \geq 0$$