IQI 04, Seminar 10/11

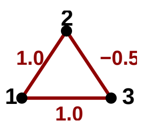
Produced with pdflatex and xfig

- Search problems.
- Unstructured search.
- Grover's algorithm.
- Quantum counting.

E. "Manny" Knill: knill@boulder.nist.gov

Examples of Search Problems

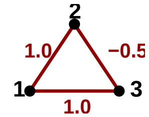
- BITSEARCH.
  Input: Bitstring $\mathbf{b}$.
  Problem: Find the position of a 1 in b if there is a 1 in b.
  Example: $\mathbf{b} = 0010100$. Solution: 3 or 5.
  Input complexity: $|\mathbf{b}| = \text{bitlength}(\mathbf{b})$.
- MINISING.
  Input: Coupling network $\{J_{i,j}\}$ for n two-level systems.
  Problem: Find a configuration $\mathbf{b} = b_1 b_2 \ldots b_n$ that minimizes the energy $\sum_{i,j} J_{i,j}(-1)^{b_i}(-1)^{b_j}$
  Example: $n = 3$, $J_{1,2} = J_{1,3} = 1$, $J_{2,3} = -0.5$. Solution: 100 or 011.
  Input complexity: $\sum_{i,j} \text{bitlength}(J_{i,j})$.



- OPTREVNET.
  Input: n-gate $\mathbf{c^2not}$ network $\mathcal{N}$ on k bits.
  Problem: Find the smallest $\mathbf{c^2not}$ network that implements the same function as $\mathcal{N}$.
  Input complexity: $\text{bitlength}(\mathcal{N})$.
- CHECKERSMOVE.
  Input: A "checkers" position on an $n \times n$ gameboard.
  Problem: Find a winning move for "black", if such a move exists.
  Input complexity: n^2.

Examples of Decision Problems

- EXISTSBIT.
  Input: Bitstring $\mathbf{b}$.
  Problem: Does b have a 1?.
  Example: $\mathbf{b} = 0010100$. Answer: "yes".
- BELOWISING.
  Input: Coupling network $\{J_{i,j}\}$ for n two-level systems, energy E.
  Problem: Is there a configuration $\mathbf{b} = b_1 b_2 \ldots b_n$ with energy $\sum_{i,j} J_{i,j}(-1)^{b_i}(-1)^{b_j} < E$?
  Example: $n = 3$, $J_{1,2} = J_{1,3} = 1$, $J_{2,3} = -0.5$, $E = -3$. Answer: No.



- BETTERREVNET.
  Input: n-gate $\mathbf{c^2not}$ network $\mathcal{N}$ on k bits.
  Problem: Is there a smaller network implementing the same function as $\mathcal{N}$?
- WINCHECKERS.
  Input: A "checkers" position on an $n \times n$ gameboard.
  Problem: Does "black" have a winning strategy?

Decision Problems in P, NP

- A *Decision problem* or *language* is a relation $R(x, y, \ldots)$ of one or more strings.
  Examples:
  - EXISTSBIT$(x) = [x$ has a $1]$.
  - BELOWISING$(x, y) =$ $[x$ encodes $\{J_{i,j}\}, E$. y encodes a configuration with energy $\leq E.]$
- $R(x, y, \ldots)$ is *polynomial time* (is in **P**) if for some k there exists a deterministic classical algorithm that computes $R(x, y, \ldots)$ in time $\leq \text{bitlength}(x, y, \ldots)^k$.
  Examples: EXISTSBIT(x) and BELOWISING(x, y) are in **P**.
- $R(x)$ is *non-deterministic polynomial time* (is in **NP**) if for some k and $Q(x, y)$ in **P**, $R(x) = \exists y\big(|y| \leq |x|^k$ and $Q(x, y)\big)$.
  Examples:
  - BELOWISING$(x) = \exists y$BELOWISING(x, y).
  - NONPRIME$(x) = \exists y[1 < y < x$ and $x = z * y]$.

NP Completeness and Hardness

- S is **NP** *hard* if for every Q in **NP**, Q is in $\mathbf{P}^S$.
  Def.: $\mathbf{P}^S$ means "polynomial time given an oracle for S".
- S is **NP** *easy* if for some Q in **NP**, S is in $\mathbf{P}^Q$.
  - Note: [R is **NP** complete] $\overset{\Rightarrow}{\not\Leftarrow}$ [R is **NP** hard and **NP** easy].
- MinIsing and BelowIsing are **NP** hard and **NP** easy.
  ... BelowIsing is **NP** complete.
- BetterRevNet may not be **NP** easy.
- WinCheckers is "**PSPACE** complete", hence not expected to be **NP** easy.

Unstructured Search

- BBSearch. $x \in \{s \mid |s| \leq m\}$
  Given: "Black Box" function $\text{BB}(x) \in \{0, 1\}$.
  Problem: Find an x such that $\text{BB}(x) = 1$ if such an x exists.
- Examples:
  - To solve BelowIsing using an algorithm $\mathcal{A}(m, \text{BB})$ for BBSearch, let $\text{BB}_{\{J_{i,j}\},E}(C) = 1$ if and only if C is a configuration with energy below E. Use $\mathcal{A}(n, \text{BB}_{\{J_{i,j}\},E})$.
  - Any problem $\exists y \left(|y| \leq |x|^k \text{ and } R(x, y)\right)$ in **NP** can be solved for a given x by using $\mathcal{A}$ with $m = |x|^k$, $\text{BB}_x(y) = R(x, y)$.

  Unstructured: Does not use prior knowledge about the internals of BB.
- qBBSearch.
  Given: "Black Box" operator $q\text{BB}|x\rangle|a\rangle = |x\rangle|a + \text{BB}(x)\rangle$.
  Problem: Find an x such that $\text{BB}(x) = 1$ if such an x exists.
  ... x and a are restricted to $x \in \{0, \ldots, N\}$, $a \in \{0, 1\}$.

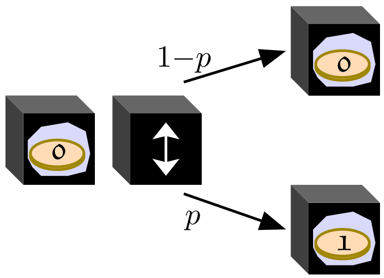
Classical Algorithms for Unstructured Search

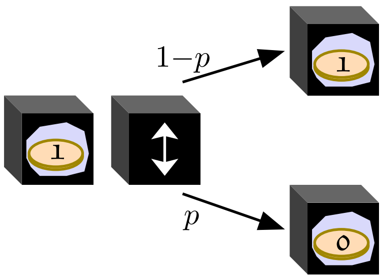
- Deterministic search.
  detSearch(BB)
  Input: BB : $\{0, \ldots, 2^n - 1\} \rightarrow \{0, 1\}$
  Output: x such that $\text{BB}(x) = 1$ or "no" if no such x exists.
  for $x = 0$ **to** $x = 2^n - 1$
  if $\text{BB}(x) = 1$ **then return** x
  end
  return "no"
  - Worst-case number of queries is 2^n.
- Probabilistic search.
  probSearch(BB)
  Input: BB : $\{0, \ldots, 2^n - 1\} \rightarrow \{0, 1\}$
  Output: x such that $\text{BB}(x) = 1$ or "no" if no such x exists.
  repeat
  $x \leftarrow \text{Rand}([2^n] \setminus X)$; $X \leftarrow X \cup \{x\}$
  until $\text{BB}(x) = 1$ or $X = [2^n]$
  if $\text{BB}(x) = 1$ **then return** x **else return** "no"
  - If a solution exists, expected number of queries $\leq (2^n + 1)/2$.

egin

Probabilities versus Quantum Amplitudes

- Given: Box with bit.
  A shake flips the bit with probability $p = 0$ or $p = \epsilon$.
  Problem: Determine p.

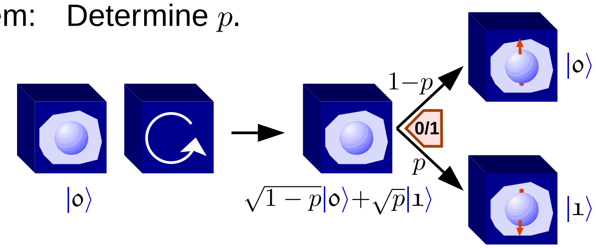




- Shake n times: Prob. of ≥ 1 flip is $1 - (1-p)^n \simeq np$ for $n \ll 1/p$.

Probabilities versus Quantum Amplitudes

- Given: Box with bit.
  A shake flips the bit with probability $p = 0$ or $p = \epsilon$.
  Problem: Determine p.
- Shake n times: Prob. of ≥ 1 flip is $1-(1-p)^n \simeq np$ for $n \ll 1/p$.
- Given: Box with qubit.
  A turn applies $\mathbf{Y}_{2\arcsin(\sqrt{p})}$, $p = 0$ or $p = \epsilon$
  Problem: Determine p.



- Turn n times: $|0\rangle \to \cos(n\arcsin(\sqrt{p}))|0\rangle + \sin(n\arcsin(\sqrt{p}))|1\rangle$.
  Prob. of detecting $|1\rangle$ is $\simeq n^2p$ for $n^2 \ll 1/p$.

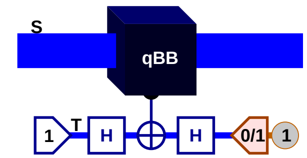
Probabilities versus Quantum Amplitudes

- Given: Box with bit.
  A shake flips the bit with probability $p = 0$ or $p = \epsilon$.
  Problem: Determine p.
- Shake n times: Prob. of ≥ 1 flip is $1-(1-p)^n \simeq np$ for $n \ll 1/p$.
- Given: Box with qubit.
  A turn applies $\mathbf{Y}_{2\arcsin(\sqrt{p})}$, $p = 0$ or $p = \epsilon$
  Problem: Determine p.
- Turn n times: $|0\rangle \to \cos(n\arcsin(\sqrt{p}))|0\rangle + \sin(n\arcsin(\sqrt{p}))|1\rangle$.
  Prob. of detecting $|1\rangle$ is $\simeq n^2p$ for $n^2 \ll 1/p$.
- Complexity. Probabilistically: $\Omega(1/p)$.
  Quantumly: $\Omega(1/\sqrt{p})$.

Grover's Algorithm: States

$x \in \{1,\ldots,N\}, b \in \{0,1\}$

- Given: qBB such that
  qBB$|x\rangle_S|b\rangle_T = |x\rangle_S|b+[x=u]\rangle_T$ with u unknown.
  Problem: Determine u.



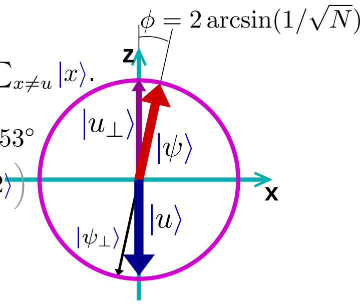
- Use phase-kickback to construct
  zBB$|x\rangle_S = (-1)^{[x=u]}|x\rangle_S$.
- Idea:
  Apply zBB in quantum parallel, amplify the amplitude of $|u\rangle_S$.
- How can one "rotate" from $\frac{1}{\sqrt{N}}\sum_x|x\rangle$ to $|u\rangle$?

Grover's Algorithm: Rotations

- Rotate from $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x|x\rangle$ to $|u\rangle$.

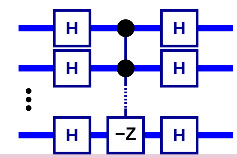
  Consider the 2-d subspace Q spanned by $|\psi\rangle$ and $|u\rangle$.
  - Overlap: $\langle u|\psi\rangle = \frac{1}{\sqrt{N}}$.
  - Bloch sphere picture:

$|u_\perp\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\neq u}|x\rangle$.



Example: $N = 3$, $|u\rangle = |2\rangle$.
$|\psi\rangle = \frac{1}{\sqrt{3}}\big(|0\rangle+|1\rangle+|2\rangle\big)$, $\langle u|\psi\rangle = \frac{1}{\sqrt{3}}$, $\phi = 70.53°$
$|u_\perp\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)$, $|\psi_\perp\rangle = \frac{1}{\sqrt{6}}\big(|0\rangle+|1\rangle-2|2\rangle\big)$

- Operators that leave Q invariant:
  - zBB. Acts as $\mathbf{Z}_{180°}$.
  - $180°$ rotation about $|\psi\rangle$:
    $\mathbf{HZH}|\psi\rangle \to -|\psi\rangle$
    $\mathbf{HZH}|\psi_\perp\rangle \to |\psi_\perp\rangle$ if $\langle\psi|\psi_\perp\rangle = 0$.
    Qubit implementation of $\mathbf{HZH}$:



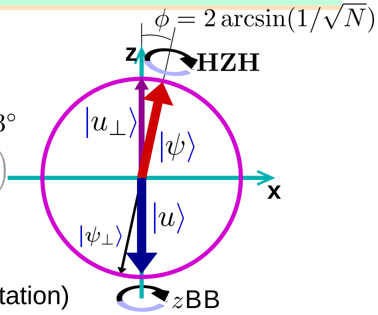
Grover's Algorithm

- Bloch sphere picture.

  Example: $N=3$, $|u\rangle = |2\rangle$.

  $|\psi\rangle = \frac{1}{\sqrt{3}}\big(|0\rangle+|1\rangle+|2\rangle\big)$, $\langle u|\psi\rangle = \frac{1}{\sqrt{3}}$, $\phi = 70.53°$

  $|u_\perp\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)$, $|\psi_\perp\rangle = \frac{1}{\sqrt{6}}\big(|0\rangle+|1\rangle-2|2\rangle\big)$



  Effect of zBB.**HZH** in Bloch sphere:

  $\hat{y} \xrightarrow{z\text{BB}} -\hat{y} \xrightarrow{\mathbf{HZH}} \hat{y}$ (it is a y-rotation)

  $\hat{z} \xrightarrow{z\text{BB}} \hat{z} \xrightarrow{\mathbf{HZH}} \begin{cases} \cos(4\arcsin(1/\sqrt{N}))\hat{z} \\ +\sin(4\arcsin(1/\sqrt{N}))\hat{x} \end{cases}$ (... by $4\arcsin(1/\sqrt{N})$)

- Grover's algorithm:
  1. Prepare $|\psi\rangle$.
  2. $\big(z\text{BB}.\mathbf{HZH}\big)^{(\pi-2\arcsin(1/\sqrt{N}))/(4\arcsin(1/\sqrt{N}))}$
  3. Measure logical basis. ...repeat, if necessary.
- Complexity: $\approx \pi\sqrt{N}/4$.

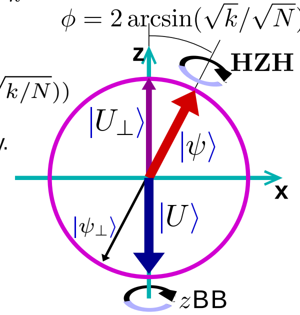
Quantum Database Search?

- An N-entry unstructured database is ...
  N items $D(i)$ stored at classical memory locations $1,\ldots,N$.
- A generic query: "Return an index i such that $Q(D(i)) = 1$.
  $Q(.)$ is a subroutine provided with the query.
- Classical complexity for unique answers. (...sequential)
  Complexity of $Q(.)$: q. Item access complexity: a.
  - On average, half the items must be *accessed*.
  - The query function is executed for each item accessed.
  - Total complexity: $O(N(a+q)/2)$.
- Quantum complexity with Grover's algorithm. (...sequential)
  Complexity of reversible $Q(.)$: $\tilde{q}$. Q. access complexity: $\tilde{a}$.
  - All items are accessed twice for each use of reversible Q.
  - Q may have to be reversibly computed twice in each iteration.
  - Total complexity: $\Omega(\sqrt{N}(2N\tilde{a}+\tilde{q}))$.

  Grover can beat classical only if $q \gg N^{1/2}\tilde{a}$.

Unstructured Quantum Search

- Given: BB such that $\text{BB}|x\rangle_{\mathsf{S}}|b\rangle_{\mathsf{T}} = |x\rangle_{\mathsf{S}}|b+[x\in U]\rangle_{\mathsf{T}}$, $|U| = k$.
  Problem: Find an element of U.
- Algorithm.
  1. Construct zBB : $|x\rangle \mapsto (-1)^{[x\in U]}|x\rangle$ by phase kickback.
     - zBB and **HZH** preserve $\text{span}\big(|U\rangle = \frac{1}{\sqrt{k}}\sum_{x\in U}|x\rangle, |\psi\rangle\big)$.
  2. Prepare $|\psi\rangle$
  3. $(z\text{BB}.\mathbf{HZH})^{(\pi-2\arcsin(\sqrt{k/N}))/(4\arcsin(\sqrt{k/N}))}$
  4. Measure logical basis. ...repeat, if necessary.

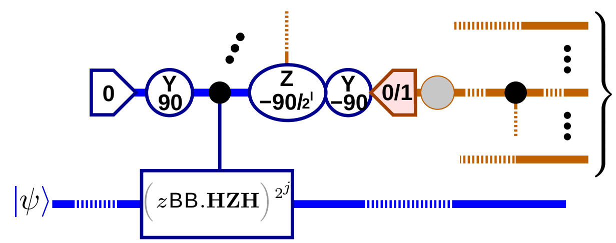


- Complexity: $\approx \pi\sqrt{N/k}/4$.
- If k is unknown: Binary search on k.
  Try $k{=}N/2, k{=}N/4, k{=}N/8, \ldots$.
  Check solutions.

Quantum Counting

"implementable as a quantum controlled operation"

- Given: (c-)BB such that $\text{BB}|x\rangle_{\mathsf{S}}|b\rangle_{\mathsf{T}} = |x\rangle_{\mathsf{S}}|b+[x\in U]\rangle_{\mathsf{T}}$.
  Problem: Determine $|U|/N$ to within ϵ. ...let $k = |U|$.
- A Grover iterate zBB.**HZH** is a Bloch-sphere rotation by $4\arcsin(\sqrt{k/N})$ in the 2-d space containing $|\psi\rangle$ and $|U\rangle$.
  - Idea: Measure an eigenvalue of zBB.**HZH**.
    The eigenvalues are
    $$-e^{\pm 2\arcsin(\sqrt{k/N})i} = -\big(\sqrt{(N-k)/N} \pm i\sqrt{k/N}\big)^2.$$



$\big(\pm\arcsin(\sqrt{k/N})/\pi\big) \pm \epsilon$
using zBB.**HZH**
$O(1/\epsilon)$ times.

Quantum versus Classical Counting

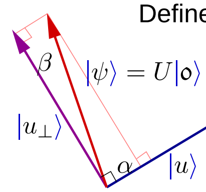
Let $u = |U|/N$.

- Quantum: Given: (c-)BB such that BB$|x\rangle_S|b\rangle_T = |x\rangle_S|b+[x \in U]\rangle_T$.
  Problem: Determine u to within ϵ.
  1. $\frac{d}{dt}\arcsin(\sqrt{t}) = \frac{1}{2\sqrt{t(1-t)}} \geq 1$.
  2. Determine $\arcsin(\sqrt{u})$ within $\delta = \epsilon/(2\sqrt{(u+\epsilon)(1-u+\epsilon)})$.
  3. Effort required: $O(\sqrt{(u+\epsilon)(1-u+\epsilon)}/\epsilon)$ uses of zBB.$\mathbf{HZH}$.
- Classical: Given: BB such that BB$(x) = [x \in U]$.
  Problem: Determine u to within ϵ.
  1. Randomly choose l distinct elements. r is the fraction in U.
  2. $\langle r\rangle = u$. std$(r) = \sqrt{u(1-u)(1-\frac{l-1}{n-1})/l}$.
  3. So set $l > u(1-u)(1-\frac{l-1}{n-1})/\epsilon^2 \approx u(1-u)/\epsilon^2$ for $l \ll n$.
  4. Effort required: $l = O(u(1-u)/\epsilon^2)$ for $l \ll n, u > 0$.
- With these methods: Quantum counting is quadratically more efficient then classical probabilistic counting.

Algorithms for Amplitude

- Given: zBB with eigenvalues in $\{-1, +1\}$ and U such that $U|o\rangle$ is not in the $+1$ eigenspace of zBB.
  Problem: Prepare a state in the -1 eigenspace of zBB.
- Write $U|o\rangle = \alpha|u\rangle + \beta|u_\perp\rangle$,
  with zBB$|u\rangle = -|u\rangle$, zBB$|u_\perp\rangle = |u_\perp\rangle$, α, β non-negative real.

Hilbert space picture:

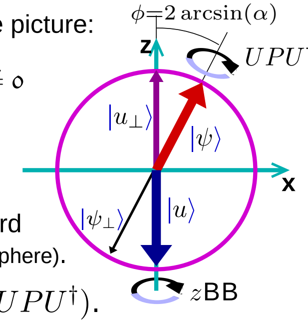


Define $P|o\rangle = -|o\rangle$, $P|b\rangle = |b\rangle$ for $b \neq o$

$$UPU^\dagger|\psi\rangle = -|\psi\rangle$$
$$UPU^\dagger|\psi_\perp\rangle = |\psi_\perp\rangle$$

zBB.$(UPU^\dagger)$ rotates $|\psi\rangle$ toward $|u\rangle$ by $4\arcsin(\alpha)$ (in the Bloch sphere).

Bloch sphere picture:

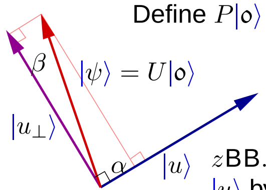


- "Amplify" overlap of $|\psi\rangle$ with $|u\rangle$ by zBB.$(UPU^\dagger)$.
  $(z\text{BB}.(UPU^\dagger))^{\pi/(4\arcsin(\alpha))-1/2}|\psi\rangle$ to come closest to $|u\rangle$.

Algorithms for Amplitude

- Given: zBB with eigenvalues in $\{-1, +1\}$ and U such that $U|o\rangle$ is not in the $+1$ eigenspace of zBB.
  Problem: Prepare a state in the -1 eigenspace of zBB.
- Write $U|o\rangle = \alpha|u\rangle + \beta|u_\perp\rangle$,
  with zBB$|u\rangle = -|u\rangle$, zBB$|u_\perp\rangle = |u_\perp\rangle$, α, β non-negative real.

Hilbert space picture:

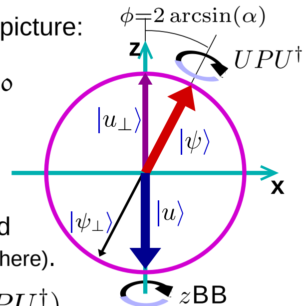


Define $P|o\rangle = -|o\rangle$, $P|b\rangle = |b\rangle$ for $b \neq o$

$$UPU^\dagger|\psi\rangle = -|\psi\rangle$$
$$UPU^\dagger|\psi_\perp\rangle = |\psi_\perp\rangle$$

zBB.$(UPU^\dagger)$ rotates $|\psi\rangle$ toward $|u\rangle$ by $4\arcsin(\alpha)$ (in the Bloch sphere).

Bloch sphere picture:



- "Estimate" overlap of $|\psi\rangle$ with $|u\rangle$ by zBB.$(UPU^\dagger)$.
  Measure an eigenv. of zBB.$(UPU^\dagger)$ on $|\psi\rangle$, get $\arcsin(\alpha) \pm \epsilon$.

Quantum Summing

- Given: Alg. for $f : \{0, \ldots, N{=}2^{n-1}\} \to \{0, \ldots, M{=}2^{m-1}\}$
  Problem: Determine $\langle f\rangle = \frac{1}{N}\sum_x f(x)$ with error less than e.
- Classical probabilistic algorithm.
  1. Choose k random, distinct inputs $x_1, \ldots, x_k$.
  2. Compute $E_k = \frac{1}{k}\sum_j f(x_j)$.

  Properties: $\langle E_k\rangle = \langle f\rangle$
  std$(E_k) \leq \sqrt{\langle f^2\rangle - \langle f\rangle^2}/\sqrt{k}$
- Applications.
  - Numerical integration in many dimensions.
  - Monte Carlo path integration.
- Goal. Double the number of digits of precision for similar effort.

Quantum Summing

- Given: Alg. for $f:\{0,\ldots,N{=}2^{n-1}\}\rightarrow\{0,\ldots,M{=}2^{m-1}\}$
  Problem: Determine $\langle f\rangle = \frac{1}{N}\sum_x f(x)$ with error less than e.
- Classical probabilistic algorithm. std$(E_k)\leq\sqrt{\langle f^2\rangle-\langle f\rangle^2}/\sqrt{k}$
- Quantum algorithm: Direct amplitude estimation.
  $z\mathsf{BB}|x\rangle|b\rangle = (-1)^b|x\rangle|b\rangle$
  $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x|x\rangle\left(\sqrt{f(x)/M}|\mathsf{1}\rangle+\sqrt{1-f(x)/M}|\mathsf{0}\rangle\right) = U_f|0\rangle|\mathsf{0}\rangle$
  $|u\rangle = \frac{1}{\sqrt{N}}\sum_x|x\rangle\sqrt{f(x)/M}|\mathsf{1}\rangle,\;\; |u_\perp\rangle = \frac{1}{\sqrt{N}}\sum_x|x\rangle\sqrt{1-f(x)/M}|\mathsf{0}\rangle$
  $\alpha = \langle u|U_f|0\rangle|\mathsf{0}\rangle = \frac{1}{N}\sum_x f(x)/M$
  Use amplitude estimation to obtain $M\alpha = \langle f\rangle$ with error e.
  Error with k uses of cond. $z\mathsf{BB}.(U_fPU_f^\dagger)$: $O(M\sqrt{1-(\alpha+\epsilon)^2}/k)$.
  - Better than classical if $\sqrt{\langle f^2\rangle-\langle f\rangle^2}\gg M/\sqrt{k}$.

Contents

References

[1] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219, New York, New York, 1996. ACM press.

[2] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, 1997.

[3] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In Jr. S. J. Lomonaco, editor, *Quantum Computation and Quantum Information: A Millennium Volume*, page (To appear). AMS Contemporary Mathematics Series, Am. Math. Soc. USA, 2000.

[4] G. Brassard, P. Høyer, and A. Tapp. Quantum counting. In K. G. Larsen, S. Skyum, and G. Winskel, editors, *Automata, Languages and Programming, Proceedings of ICALP'98*, volume 1443 of *Lecture Notes in Computer Science*, pages 820–831, Berline, Germany, 1998. Springer Verlag.