ESF
EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA

IEGULDĪJUMS TAVĀ NĀKOTNĒ

Variable time amplitude amplification and quantum algorithms for linear algebra

Andris Ambainis
University of Latvia

European Social Fund project “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

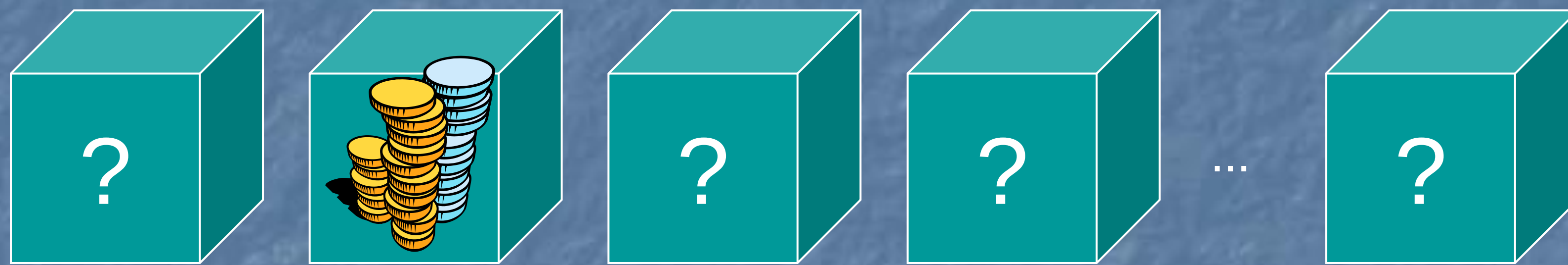
Part 1

Variable time amplitude amplification

Amplitude amplification [Brassard, Hoyer, Mosca, Tapp, 00]

- Algorithm A that succeeds with probability $\varepsilon>0$.
- Success is verifiable.
- k repetitions $\rightarrow$ success probability $\approx k\varepsilon$.
- Success probability of 3/4:
  - $O(1/\varepsilon)$ classical repetitions.
  - Quantumly: $O(1/\sqrt{\varepsilon})$ repetitions.

Search [Grover, 96]



- Find an object with a certain property.

Check a random object:
success probability $\varepsilon = 1/N$.

Success probability 3/4:
$O(1/\sqrt{\varepsilon}) = O(\sqrt{N})$ repetitions.

Variable-time algorithm

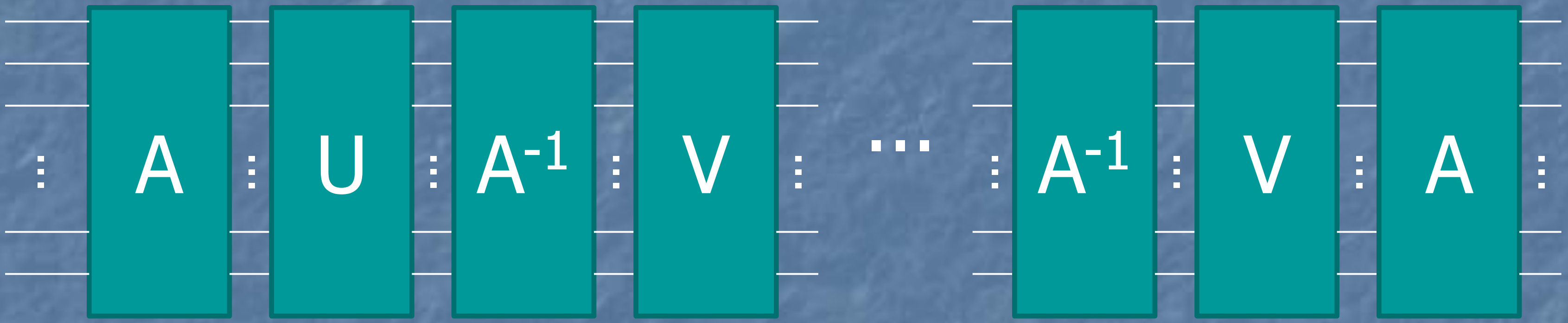
- Success probability: small $\varepsilon>0$.
- Maximum running time: T_{max}.
- Average running time $T_{avg} \ll T_{max}$.
- Time to obtain success probability ¾?

Classically: $T_{avg} \bullet O(1/\varepsilon)$

Quantumly: $T_{max} \bullet O(1/\sqrt{\varepsilon})$

Why T_{max}?

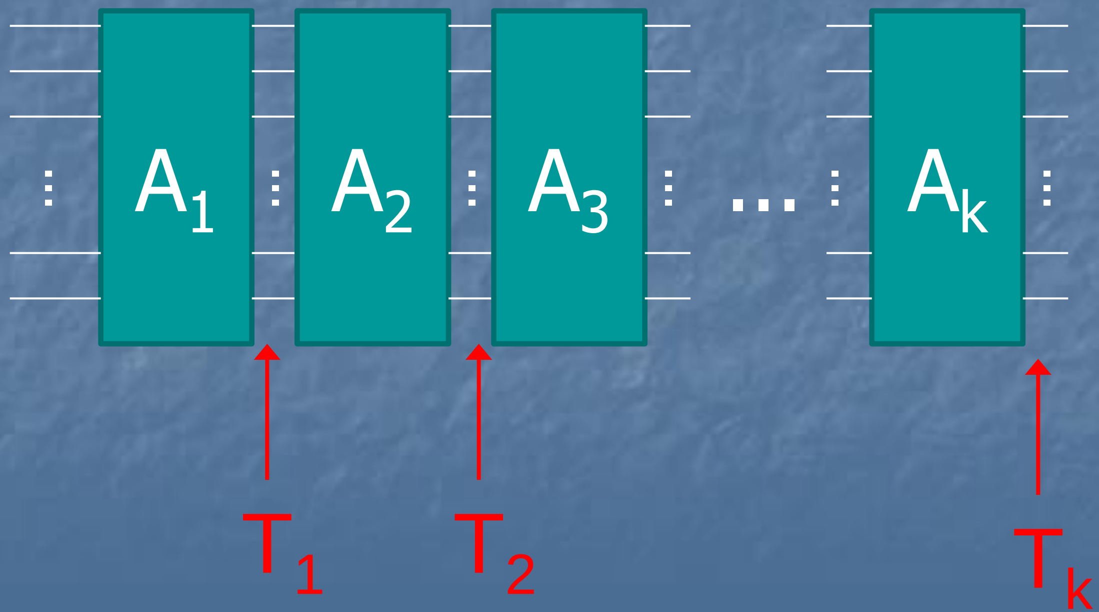
- Standard amplitude amplification regards A as one "quantum black box".



Running time: $O\left(\frac{1}{\sqrt{\varepsilon}}\right)\cdot T_{\max}$

Variable time quantum algorithms

- Algorithm that stops at one of several times $T_1, \ldots, T_k$, with probabilities $p_1, \ldots, p_k$.

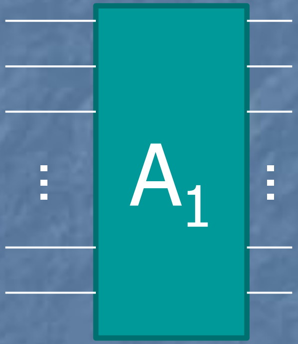


Our result

- Let $$T_{av} = \sqrt{\sum_{i=1}^{k} p_i T_i^2}$$
- Quantum algorithm with success probability ε and average running time T_{av} $\rightarrow$ quantum algorithm with success probability 2/3 and running time

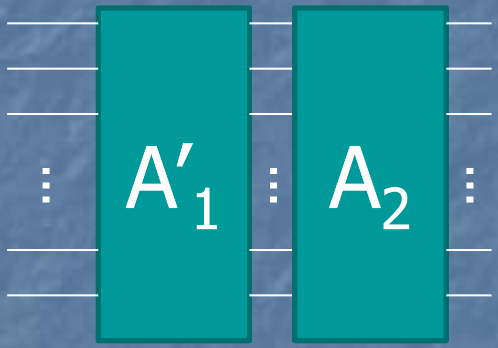
$$\tilde{O}\left(\frac{T_{av}}{\sqrt{\varepsilon}}\right)$$

Basic idea



- 3 outcomes: "success", "failure", "did not stop"
- Amplify "success" and "did not stop".
- Amplified version A'_1.

Basic idea (2)



- 3 outcomes: "success", "failure", "did not stop"
- Amplify "success" and "did not stop".
- Amplified version A'_2.

Difficulties

- Amplitude amplification repeated k times;
- If one amplification loses a factor of c, then k amplifications lose a factor of c^k.
- We need a very precise analysis of amplitude amplification.

Part 2

Testing if a matrix is singular

Singularity testing

- Matrix A;
- Promise A is singular or all singular values of A are at least λ_{min}.
- Task: distinguish between the two cases.

Our result

- Let $\lambda_1, \lambda_2, \ldots, \lambda_N$ - singular values of B.
- <u>Theorem</u> There is a quantum algorithm for singularity with running time $\tilde{O}\left(\frac{\sqrt{N}}{\lambda_{av}}\right)$ where

$$\lambda_{av} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\max\left(\left|\lambda_i\right|^2, \left|\lambda_{\min}\right|^2\right)}$$

Component 1: eigenvalue estimation [Cleve et al., 1998]

- Input: state $|\psi\rangle$: $B|\psi\rangle=\lambda|\psi\rangle$.
- Output: estimate for λ.
- To obtain estimate λ' with $|\lambda'-\lambda|\leq\varepsilon$, it suffices to apply B to $|\psi\rangle$ for time $O(1/\varepsilon)$.
- Can be used to check if $\lambda>0$, in time $O(1/\lambda_{min})$.

Component 2: quantum search

- We can search among N eigenvalues in time $O(\sqrt{N})$.
- Straightforward combination with eigenvalue estimation: $O(\sqrt{N}/\lambda_{min})$.
- Variable time amplitude amplification: $O(\sqrt{N}/\lambda_{avg})$.

Part 3

Solving systems of linear equations

The problem

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1N}x_N = b_1$$
$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2N}x_N = b_2$$
$$\ldots$$
$$a_{N1}x_1 + a_{N2}x_2 + \ldots + a_{NN}x_N = b_N$$

- Given a_{ij} and b_i, find x_i.
- Best classical algorithm: $O(N^{2.37\ldots})$.

Quantum algorithm?

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1N}x_N = b_1$$
$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2N}x_N = b_2$$
$$\ldots$$
$$a_{N1}x_1 + a_{N2}x_2 + \ldots + a_{NN}x_N = b_N$$

Obstacle: takes time O(N) to output all x_i.

Harrow, Hassidim, Lloyd, 2008

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1N}x_N = b_1$$
$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2N}x_N = b_2$$
$$\ldots$$
$$a_{N1}x_1 + a_{N2}x_2 + \ldots + a_{NN}x_N = b_N$$

Output = $\sum_{i=1}^{N} x_i |i\rangle$

- Measurement $\rightarrow$ i with probability x_i^2.
- Enables estimating $c_1x_1+c_2x_2+\ldots+c_Nx_N$.

Seems to be difficult classically.

Harrow, Hassidim, Lloyd, 2008

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1N}x_N &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2N}x_N &= b_2 \\
&\ldots \\
a_{N1}x_1 + a_{N2}x_2 + \ldots + a_{NN}x_N &= b_N
\end{aligned}
$$

- Running time for producing $\sum_{i=1}^{N} x_i |i\rangle$: $O(\log^c N)$, but with dependence on two other parameters.

Condition number

$$k = \frac{\mu_{\max}}{\mu_{\min}}$$

μ_{max} and μ_{min} – biggest and smallest singular values of A

$$Running\ time - O\left(\kappa^2 \log^c N\right)$$

Our result

- Theorem There is a quantum algorithm for generating $\sum_{i=1}^{N} x_i |i\rangle$ in time $O(k^{1+o(1)} \log^c N)$.

- [HHL, 2008]: $\Omega(k^{1-o(1)})$ time required, unless BQP=PSPACE.

Open problem

- What problems can we reduce to systems of linear equations (with $\sum_i x_i |i\rangle$ as the answer)?
  - Examples:
    - Search;
    - Perfect matchings in a graph;
    - Graph bipartiteness.

Biggest issue: condition number.