Efficient Quantum Algorithm for Computing the Circumference of Infrastructures

Pradeep Sarvepalli

School of Chemistry and Biochemistry
Georgia Institute of Technology, Atlanta

Joint work with Pawel Wocjan

July 18, 2012.
Department of Computer Science and Engineering, IIT Hyderabad.

Outline

Infrastructures

Quantum Information

Quantum Algorithm
- Preprocessing
- Quantum part of the algorithm
- Classical part of the algorithm

Infrastructures

An infrastructure of circumference R is a pair (X, d) where

- $X = \{x_0, x_1, \ldots, x_{m-1}\}$
- $d : X \hookrightarrow \mathbb{R}$
  $d(x_0) = 0 < d(x_1) < \cdots < d(x_{m-1}) < R$

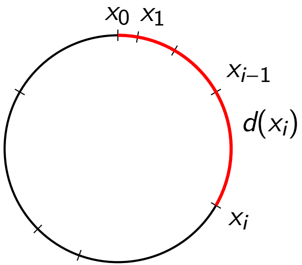


Figure: Visualizing an infrastructure

Functions on Infrastructures

Baby-step : $\mathrm{bs} : X \to X$

$$\mathrm{bs}(x_i) = \begin{cases} x_{i+1} & 0 \leq i < m-1 \\ x_0 & i = m-1 \end{cases} \quad (1)$$

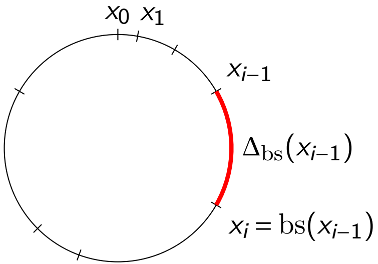


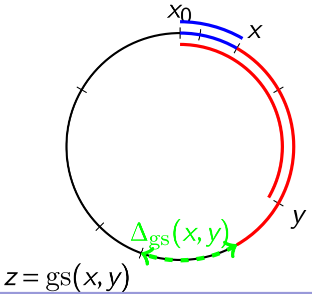
Figure: Baby-step

Functions on Infrastructures

Giant-step : $\mathrm{gs}: X \times X \to X$

Operational interpretation of $\mathrm{gs}(x, y)$

- From x move a distance of $d(y)$ along the circle.
- Find the element $z \in X$ that is immediately "after" $d(x) + d(y)$.
- $\Delta_{\mathrm{gs}}(x, y) = d(z) - d(x) - d(y) \bmod R$.



Computational Problems

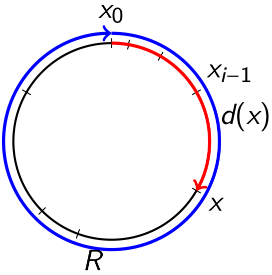


Figure: Computational problems of an infrastructure

- Compute an m-bit approximation of the circumference R.
- Given an element x, compute an m-bit approximation of $d(x)$.

Example

A cyclic group $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$. Distance function

$$d(g^i) = i$$

Example

A cyclic group $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$. Distance function

$$d(g^i) = i$$

Baby-step: Multiplication by g.

$$\begin{aligned} \mathrm{bs}(g^j) &= g^{j+1} \\ \Delta_{\mathrm{bs}}(g^j) &= 1 \end{aligned}$$

Example

A cyclic group $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$. Distance function

$$d(g^i) = i$$

Baby-step: Multiplication by g.

$$\begin{aligned} \mathrm{bs}(g^i) &= g^{i+1} \\ \Delta_{\mathrm{bs}}(g^i) &= 1 \end{aligned}$$

Giant-step: Group multiplication in G.

$$\begin{aligned} \mathrm{gs}(g^i, g^j) &= g^{i+j} \\ \Delta_{\mathrm{gs}}(g^i, g^j) &= 0 \end{aligned}$$

Example

A cyclic group $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$. Distance function

$$d(g^i) = i$$

Baby-step: Multiplication by g.

$$\begin{aligned} \mathrm{bs}(g^i) &= g^{i+1} \\ \Delta_{\mathrm{bs}}(g^i) &= 1 \end{aligned}$$

Giant-step: Group multiplication in G.

$$\begin{aligned} \mathrm{gs}(g^i, g^j) &= g^{i+j} \\ \Delta_{\mathrm{gs}}(g^i, g^j) &= 0 \end{aligned}$$

Circumference is simply the order of the group.

Example

A cyclic group $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$. Distance function

$$d(g^i) = i$$

Baby-step: Multiplication by g.

$$\begin{aligned} \mathrm{bs}(g^i) &= g^{i+1} \\ \Delta_{\mathrm{bs}}(g^i) &= 1 \end{aligned}$$

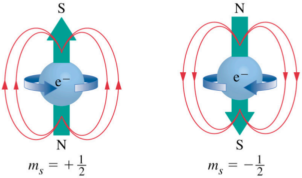
Giant-step: Group multiplication in G.

$$\begin{aligned} \mathrm{gs}(g^i, g^j) &= g^{i+j} \\ \Delta_{\mathrm{gs}}(g^i, g^j) &= 0 \end{aligned}$$

Circumference is simply the order of the group.
Discrete logarithm problem: Given g^i, compute i.

Qubits i.e. Quantum Bits

Qubits are 2-state quantum systems

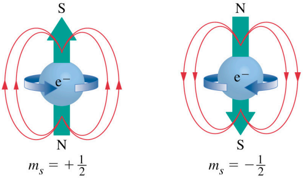


Source: General Chemistry, Principles and Modern Applications

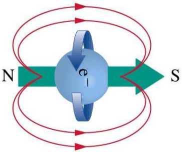
$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Qubits i.e. Quantum Bits

Qubits are 2-state quantum systems



Source: General Chemistry, Principles and Modern Applications



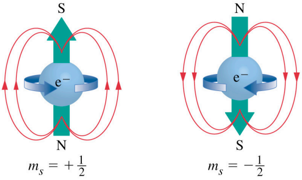
$$|\psi\rangle = a|0\rangle + b|1\rangle$$

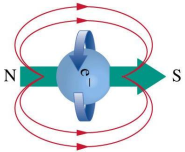
State space of a qubit is $\mathbb{C}^2$.

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Qubits i.e. Quantum Bits

Qubits are 2-state quantum systems





$$\left|\psi\right\rangle = a|0\rangle + b|1\rangle$$

State space of a qubit is $\mathbb{C}^2$.

Source: General Chemistry, Principles and Modern Applications

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

The state of n qubits is a unit vector in $\mathbb{C}^{2^n} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n}$.

$$\left|\psi\right\rangle = \sum_{x_i \in \mathbb{F}_2} \alpha_{x_1,\ldots,x_n} |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle; \qquad \sum_{x_i \in \mathbb{F}_2} |\alpha_{x_1,\ldots,x_n}|^2 = 1.$$

Qubits—Measurement

In general observing (measuring) a quantum state changes the state.

$$\alpha|0\rangle + \beta|1\rangle \overset{\text{Observe}}{\longmapsto} \begin{cases} |0\rangle & Pr(|0\rangle) = |\alpha|^2 \\ |1\rangle & Pr(|1\rangle) = |\beta|^2 \end{cases}$$

Qubits—Measurement

In general observing (measuring) a quantum state changes the state.

$$\alpha|0\rangle + \beta|1\rangle \overset{\text{Observe}}{\longmapsto} \begin{cases} |0\rangle & Pr(|0\rangle) = |\alpha|^2 \\ |1\rangle & Pr(|1\rangle) = |\beta|^2 \end{cases}$$

More generally if we observe some qubits of a state, it "collapses" the state.

$$\sum_i \sum_j a_{i,j} |i\rangle_A |j\rangle_B \rightarrow \sum_i a_i |i\rangle |j_B\rangle_B$$

No cloning and entanglement

No Cloning Theorem

We cannot make copies of an unknown quantum state.

No cloning and entanglement

No Cloning Theorem

We cannot make copies of an unknown quantum state.

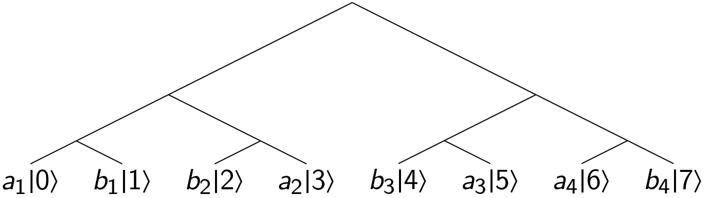
Entanglement: Consider the state

$$\left|\psi\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$$

Entangled states exhibit non-local correlations.

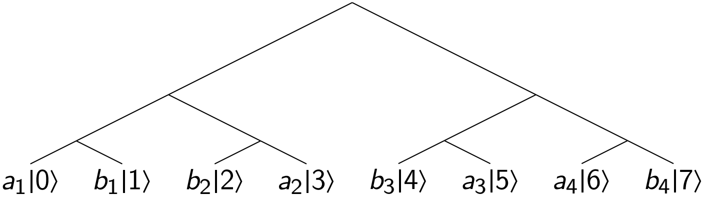
Quantum Parallelism and Interference

A quantum computer takes many computational paths simultaneously.



Quantum Parallelism and Interference

A quantum computer takes many computational paths simultaneously.



Quantum computer interferes different computational paths so that only the desirable final states survive with high probabilities.

The Road Ahead—Some Obstacles and the Strategy

Some obstacles

- We must be able to compute efficiently within the infrastructure, i.e., compute $\mathrm{bs}(x)$, $\mathrm{gs}(x,y)$, $\Delta_{\mathrm{bs}}(x)$ and $\Delta_{\mathrm{gs}}(x,y)$ (without the knowledge of R).
- The distances could be transcendental, but we assume only finite precision arithmetic.

Imposing a group structure

In order to be able to compute efficiently within an infrastructure, we embed into a circle group.

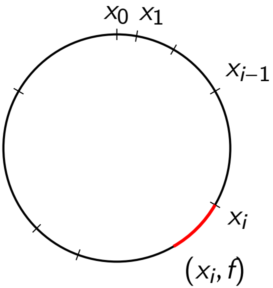


Figure: Embedding into the circle group $\mathbb{R}/R\mathbb{Z}$

Imposing a group structure

In order to be able to compute efficiently within an infrastructure, we embed into a circle group.

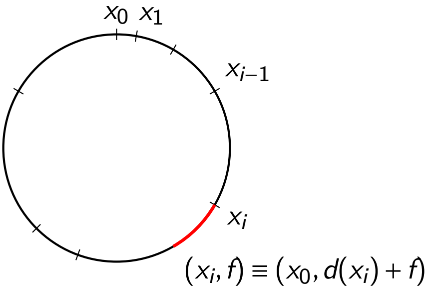


Figure: Embedding into the circle group $\mathbb{R}/R\mathbb{Z}$

The Road Ahead—Some Obstacles and the Strategy

Structure of the Algorithm

— Setup a function h over $\mathbb{R}$ that is periodic with R.

The Road Ahead—Some Obstacles and the Strategy

Structure of the Algorithm

- Setup a function h over $\mathbb{R}$ that is periodic with R.
- Evaluate an approximate version of h (due to finite precision).

  The goal here is to loosely preserve the periodicity of h in the approximate version as well.

The Road Ahead—Some Obstacles and the Strategy

Structure of the Algorithm

— Setup a function h over $\mathbb{R}$ that is periodic with R.

— Evaluate an approximate version of h (due to finite precision).

The goal here is to loosely preserve the periodicity of h in the approximate version as well.

— Discretize the approximate version of h still preserving "approximate periodicity".

The Road Ahead—Some Obstacles and the Strategy

Structure of the Algorithm

- Setup a function h over $\mathbb{R}$ that is periodic with R.
- Evaluate an approximate version of h (due to finite precision).

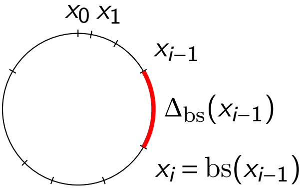
  The goal here is to loosely preserve the periodicity of h in the approximate version as well.
- Discretize the approximate version of h still preserving "approximate periodicity".
- Use quantum Fourier transform to estimate the period R by finding an integer close to R.

The Road Ahead—Some Obstacles and the Strategy

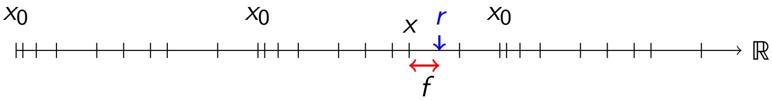
Structure of the Algorithm

- Setup a function h over $\mathbb{R}$ that is periodic with R.
- Evaluate an approximate version of h (due to finite precision).
  The goal here is to loosely preserve the periodicity of h in the approximate version as well.
- Discretize the approximate version of h still preserving "approximate periodicity".
- Use quantum Fourier transform to estimate the period R by finding an integer close to R.
- Refine the approximation to the desired degree of precision using classical post processing.

Setting Up a Periodic Function, $h : \mathbb{R} \to \mathbb{R}/R\mathbb{Z}$



Unwrap the circle and place it on $0 \cup \mathbb{R}^+$ as shown below.



$h(r) = (x, f)$, where x is the nearest element of X to the left of r and $f = r - d(x) \bmod R$.

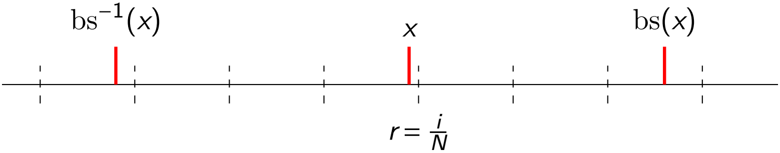
Preserving Periodicity with Approximate h

If r is too "close" to an element of X, then h may be evaluated incorrectly. We can overcome this problem as follows:

Preserving Periodicity with Approximate h

If r is too "close" to an element of X, then h may be evaluated incorrectly. We can overcome this problem as follows:

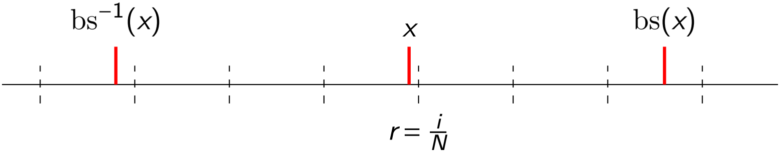
- Discretize h, and evaluate h for only a finite set of points. This discrete version h_N has period RN, where $1/N$ is sampling period.



Preserving Periodicity with Approximate h

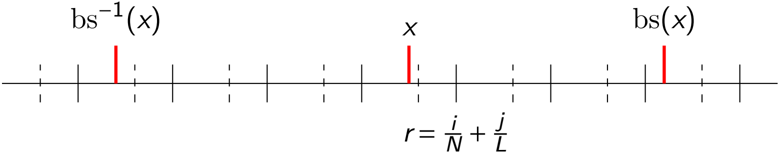
If r is too "close" to an element of X, then h may be evaluated incorrectly. We can overcome this problem as follows:

- Discretize h, and evaluate h for only a finite set of points. This discrete version h_N has period RN, where $1/N$ is sampling period.



- Shift the evaluation points so that they are not too close to the elements of X.

Preserving Periodicity with Approximate h



Setting a Pseudo-Periodic State

We choose a sufficiently large integer $q \geq 2R^2N^2$.

— Prepare two quantum registers in the following state

$$|\psi\rangle \mapsto \sum_{j=0}^{q-1} |j\rangle_1 |0\rangle_2 \quad (2)$$

Setting a Pseudo-Periodic State

We choose a sufficiently large integer $q \geq 2R^2N^2$.

- Prepare two quantum registers in the following state

$$|\psi\rangle \mapsto \sum_{j=0}^{q-1} |j\rangle_1 |0\rangle_2 \tag{2}$$

- We then transform this state to

$$|\psi\rangle \mapsto \sum_{j=0}^{q-1} |j\rangle_1 |h_N(j)\rangle_2 \tag{3}$$

Setting a Pseudo-Periodic State

We choose a sufficiently large integer $q \geq 2R^2N^2$.

- Prepare two quantum registers in the following state

$$|\psi\rangle \mapsto \sum_{j=0}^{q-1} |j\rangle_1 |0\rangle_2 \tag{2}$$

- We then transform this state to

$$|\psi\rangle \mapsto \sum_{j=0}^{q-1} |j\rangle_1 |h_N(j)\rangle_2 \tag{3}$$

- Measure the second register.

$$|\psi\rangle \mapsto \sum_{j\in\mathscr{J}} |o + \lfloor jRN \rceil\rangle_1 |h_N(o))\rangle_2, \quad \mathscr{J} \subseteq \{0, 1, \ldots, \lfloor q/NR \rfloor - 1\} \tag{4}$$

We call these states pseudo-periodic states.

Quantum Fourier Transform

Graphically, the first register is in the following state.

Quantum Fourier Transform

Graphically, the first register is in the following state.

Quantum Fourier transform (QFT) can be be used to extract the periodicity of the function from this approximately periodic state.

Quantum Fourier Transform

Graphically, the first register is in the following state.

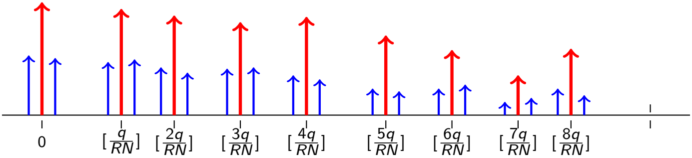
Quantum Fourier transform (QFT) can be be used to extract the periodicity of the function from this approximately periodic state.

$$|k\rangle \overset{QFT}{\mapsto} \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} e^{i2\pi kj/q} |j\rangle \quad (5)$$

$$|\psi\rangle \overset{QFT}{\mapsto} \frac{1}{\sqrt{q|\mathscr{J}|}} \sum_{\ell=0}^{q-1} \sum_{j\in\mathscr{J}} e^{i2\pi\ell\lfloor jRN\rceil/q} |\ell\rangle \quad (6)$$

Extracting Periodicity via Quantum Fourier Transform

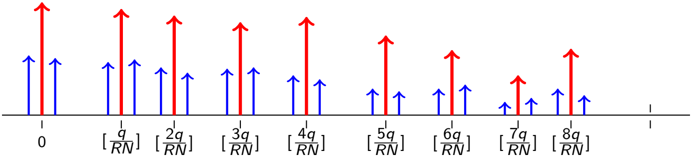
A q-point QFT of the first register gives the following state[1].



[1] Respresentative only, not exact.

Extracting Periodicity via Quantum Fourier Transform

A q-point QFT of the first register gives the following state[1].

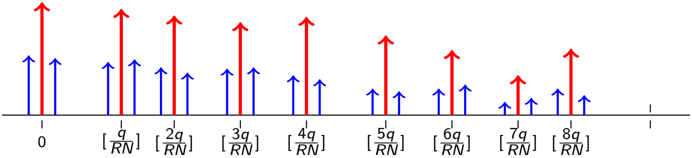


— Measure the first register.

[1] Respresentative only, not exact.

Extracting Periodicity via Quantum Fourier Transform

A q-point QFT of the first register gives the following state[1].

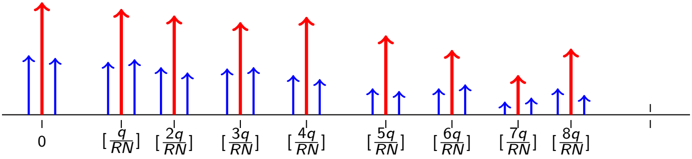


- Measure the first register.
- In order to extract the period we need to measure a term $\ell = [mq/NR]$.

[1] Respresentative only, not exact.

Extracting Periodicity via Quantum Fourier Transform

A q-point QFT of the first register gives the following state[1].

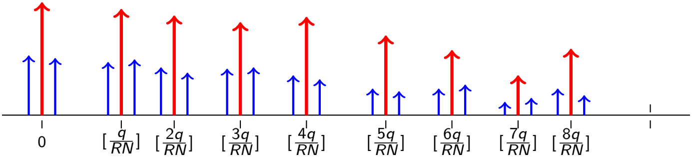


- Measure the first register.
- In order to extract the period we need to measure a term $\ell = [mq/NR]$.
- Such a state occurs with high probability provided the state was "sufficiently" periodic and q is large.

[1] Respresentative only, not exact.

Extracting Periodicity via Quantum Fourier Transform

A q-point QFT of the first register gives the following state[1].



- Measure the first register.
- In order to extract the period we need to measure a term $\ell = [mq/NR]$.
- Such a state occurs with high probability provided the state was "sufficiently" periodic and q is large.
- Two such measurements can be used to approximate an integer that is close to RN using continued fractions.

[1] Respresentative only, not exact.

Classical Postprocessing

— Observe that $\ell = [\frac{mq}{NR}]$ that there are two unknowns, m and R. So one measurement is not sufficient.

Classical Postprocessing

- Observe that $\ell = [\frac{mq}{NR}]$ that there are two unknowns, m and R. So one measurement is not sufficient.
- With two measurements $c = [\frac{kq}{NR}]$ and $d = [\frac{lq}{NR}]$, k/l occurs as a convergent of c/d where the denominator of the convergent is less than $q/32$.

Classical Postprocessing

- Observe that $\ell = [\frac{mq}{NR}]$ that there are two unknowns, m and R. So one measurement is not sufficient.
- With two measurements $c = [\frac{kq}{NR}]$ and $d = [\frac{lq}{NR}]$, k/l occurs as a convergent of c/d where the denominator of the convergent is less than $q/32$.
- We can now obtain a finite list of candidates one of which $\overline{NR}$ is guaranteed to be close to NR.

Classical Postprocessing

- Observe that $\ell = [\frac{mq}{NR}]$ that there are two unknowns, m and R. So one measurement is not sufficient.
- With two measurements $c = [\frac{kq}{NR}]$ and $d = [\frac{lq}{NR}]$, k/l occurs as a convergent of c/d where the denominator of the convergent is less than $q/32$.
- We can now obtain a finite list of candidates one of which $\overline{NR}$ is guaranteed to be close to NR.
- Compute $h(\overline{NR}/N)$ and if this is in the neighbourhood of x_0, then $\overline{NR}/N$ is within a unit of R or its multiples.

Classical Postprocessing

- Observe that $\ell = [\frac{mq}{NR}]$ that there are two unknowns, m and R. So one measurement is not sufficient.
- With two measurements $c = [\frac{kq}{NR}]$ and $d = [\frac{lq}{NR}]$, k/l occurs as a convergent of c/d where the denominator of the convergent is less than $q/32$.
- We can now obtain a finite list of candidates one of which $\overline{NR}$ is guaranteed to be close to NR.
- Compute $h(\overline{NR}/N)$ and if this is in the neighbourhood of x_0, then $\overline{NR}/N$ is within a unit of R or its multiples.
- Successively improve the estimate of R using a binary search procedure with the baby-step.

Improvements

Proposed algorithm

- Generalizes Hallgren's algorithm for number fields, and can be used to solve Pell's equation $x^2 - dy^2 = 1$.
- Uses a tighter analysis and presents a technical result of larger applicability.
- Has lower complexity, polynomial speedup over Hallgren's algorithm for Pell's equation.
- Success probability $= \Omega(1)$, in contrast Hallgren's algorithm which can only guarantee a success probability $\Omega(1/\log N^4 R^4)$.

Summary

- Polynomial time quantum algorithms for infrastructures. PS, Wocjan arXiv:1106.5347
  - Computing the circumference of the infrastructures.
  - Computing the generalized discrete logarithms.
- When specialized to cases such as the quadratic number fields, the proposed algorithms have
  - Lower complexity.
  - Higher success probability.

Questions?

Questions?

Thank you!