# Fine-grained 量子スプレマシー

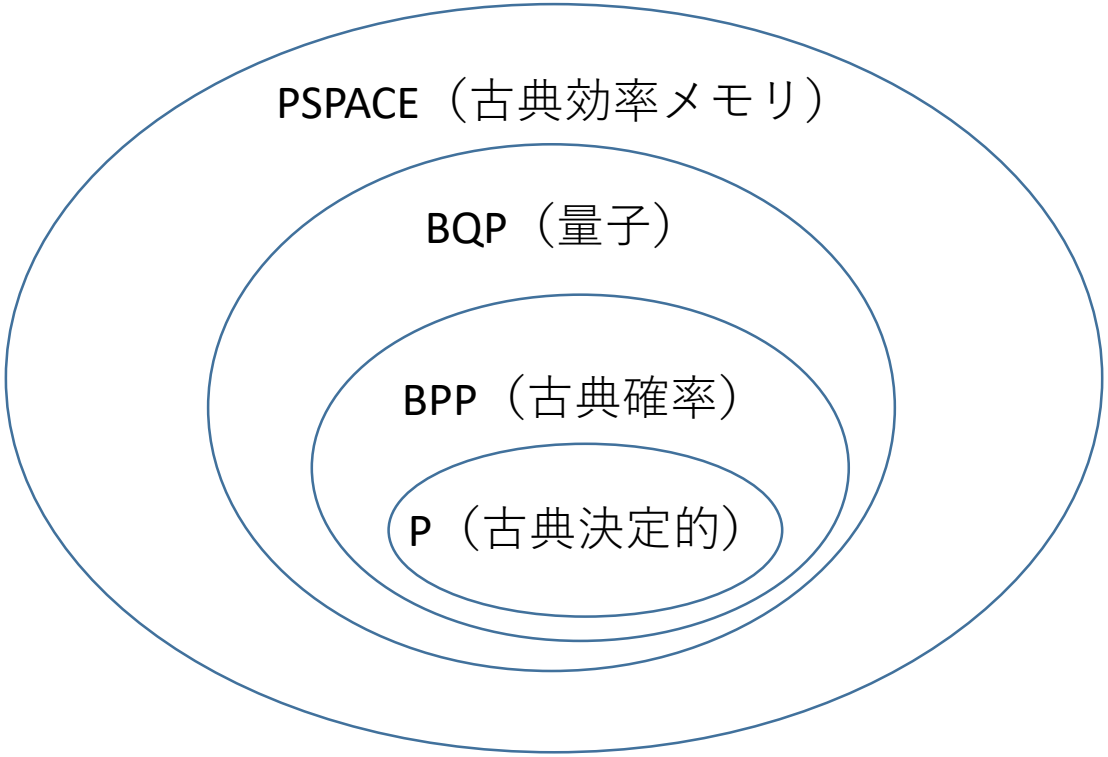
森前智行
(京都大学基礎物理学研究所)

QIT40@九州大学　15分

Joint work with 玉置卓 (兵庫県立大学)

TM and Tamaki, arXiv:1901.01637, 1902.08382


# 量子計算は古典計算より速いのか？




BQP≠BPP→P≠PSPACE

BQP≠BPPを示すのは難しい！

そうはいっても皆量子のほうが古典より速いと信じている
これまでのアプローチ：
古典のベストよりも速いことを示す（例：Shor）
Query complexityでの優位性を示す（例：Simon、Grover）

# サイモン、グローバー等

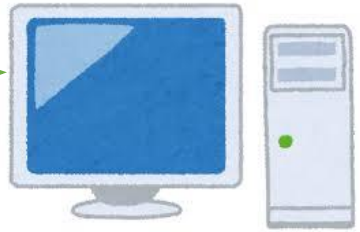
私の勝ち


量子計算機

回数少ない

サブルーチン

くやしい



古典計算機

回数多い

サブルーチン

サブルーチンを呼ぶ回数だけ見ている。
→計算量理論におけるスタンダードなアプローチ（query complexity）
→限界の証明がしやすい。（多くの結果が得られている。）
→実時間では見ていない。

# ショアー、量子シミレーション等

こちらは実時間を見る(time complexity)

古典のベストより高速であることを示す

素因数分解：古典では遅いが量子では速い

→古典では遅いという数学的証明があるわけではない

将来古典の高速アルゴリズムが見つかるかも！


Quantum memeing

例：recommendation system
客の購買データーからおすすめ商品を見つける量子機械学習アルゴリズム

→米国の１８歳の学部生が高速古典アルゴリズムを見つけてしまった！

古典のベストと比較して速い、というのは危険！

# サンプリング

サンプリング問題を考えると、量子の優位性が強力な計算量的基盤で証明できる。


$z \in \{0,1\}^n$

古典計算機

$z \in \{0,1\}^n$

量子計算機

$$|p_z - q_z| \leq \epsilon p_z$$

量子計算機がzを出す確率

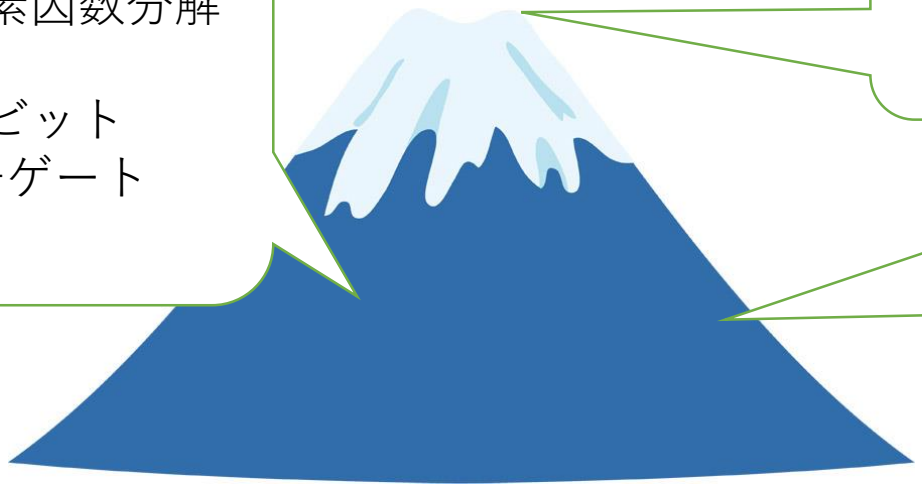
古典計算機がzを出す確率

多項式階層が崩壊しない限り、量子計算は多項式時間で古典サンプル不可能

多項式階層が崩壊しない：P≠NPのようなもの（すごい大雑把…）

# 弱い量子マシンでもOK

サンプリングにおける量子優位性は弱いマシンでもでる！



1024ビットの素因数分解

2000個の量子ビット
10^11個の量子ゲート
が必要

究極のゴール:
量子ビット使い放題
ユニバーサル
Fault-tolerant

Near-term goal
弱いマシンで量子の
優位性をデモンスト
レート

量子スプレマシー：弱いマシンで量子優位性を強い基盤で示す研究

# 量子スプレマシーのでる弱いモデルの例

Depth-4 circuit
Terhal and DiVincenzo, QIC 2004

Boson Sampling
Aaronson and Arkhipov, STOC 2011

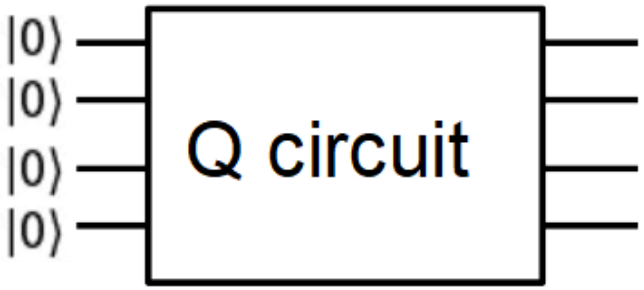
Commuting gates(IQP)
Bremner, Jozsa, and Shepherd, Proc. Roy. Soc. A 2010

One-clean qubit model
TM, Fujii, and Fitzsimons, PRL 2014

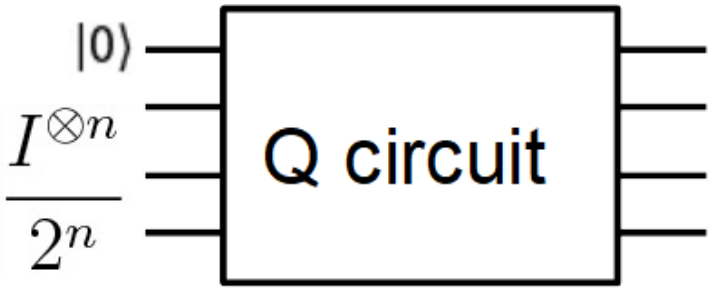
HC1Q model
TM, Nishimura, and Takeuchi, Quantum 2018

Random gates
Fefferman et al. Nature Phys. 2018

# One-clean qubit モデル




通常の量子計算




One clean qubit model

[Knill and Laflamme, PRL 1998]

古典よりはちょっと強いだろう

例：Jones多項式の計算
[Shor and Jordan 2007]

ここじゃない
[Ambainis 2000]

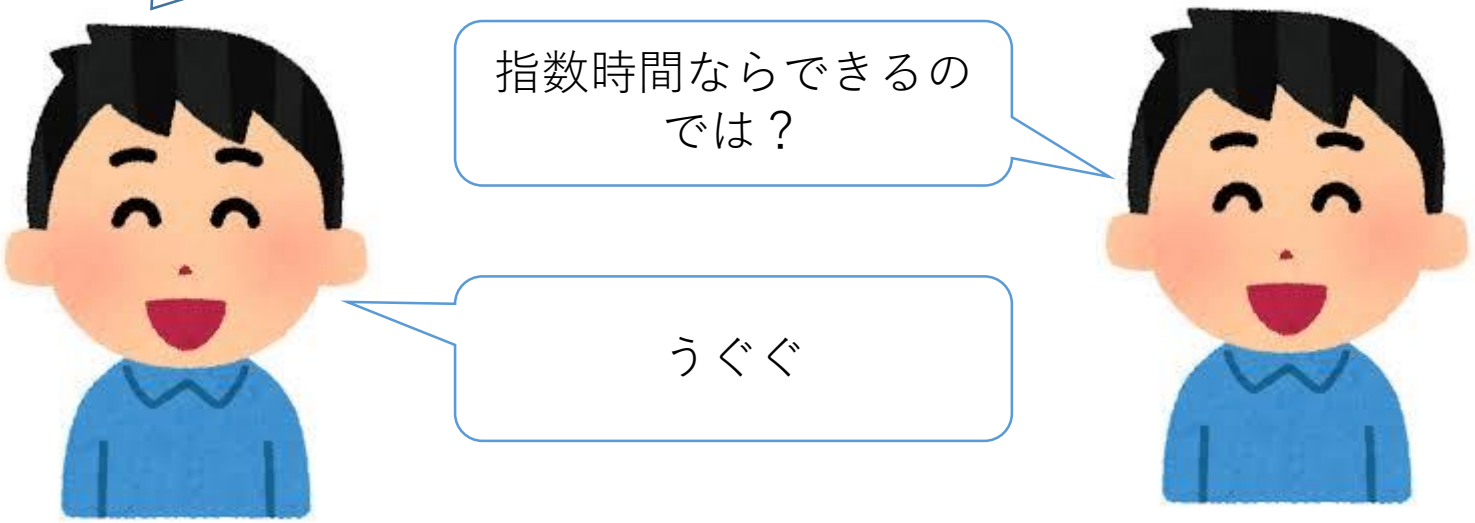
古典 → ユニバーサル量子

多項式階層が崩壊しない限りone-clean qubitモデルは古典サンプル不可。
[TM, Fujii, Fitzsimons, PRL 2014]

# Fine-grained 量子スプレマシー

これまでの量子スプレマシー

「多項式階層が崩壊しない限り、私の量子マシンは古典で多項式時間ではサンプルできない」



# Fine-grained量子スプレマシー

示したいこと：

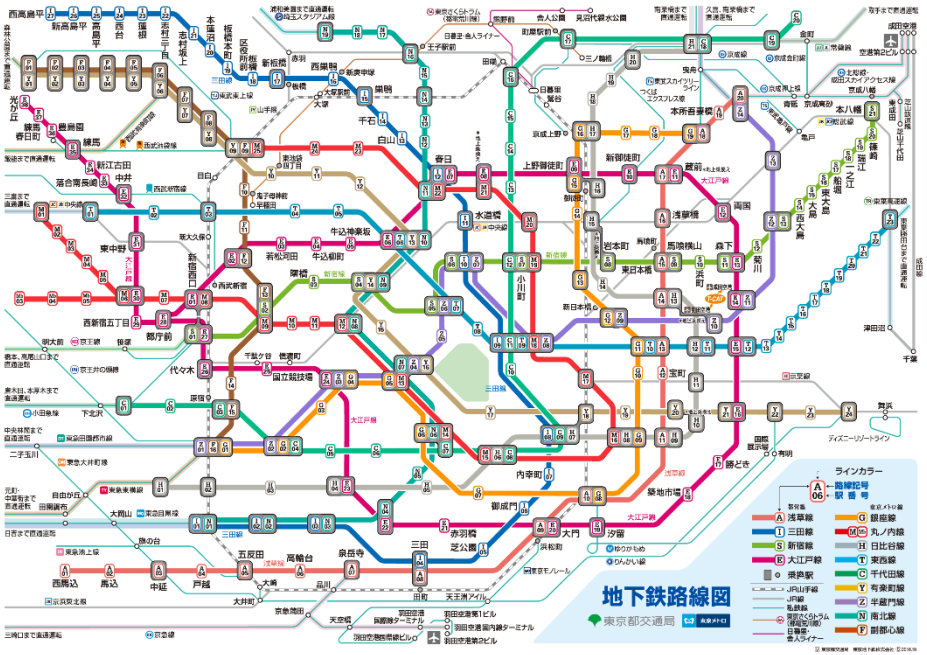
〇〇が正しい限り、私の量子マシンは指数時間でも古典サンプルできない

P≠NPみたいな、何か「正しそうな」
計算量理論的仮定

PやNP、多項式階層等の「伝統的」計算量理論は使えなさそう。

→Fine-grained complexity！！　（ETH, SETH, OV, 3SUM, APSP）

# Exponential time hypothesis




2^n個の組み合わせの中から、解を見つけろ

poly(n)時間ではできません　→　P≠NP仮説

o(2^n)時間ではできません　→　Exponential time hypothesis

いろんな変種がある：SETH、NSETH、NCSETH、＃ETH、Parity-SETH。。。

# SETH-like conjecture

SETH:

任意の a>0に対し、ある k が存在して、n 変数のk-CNF-SAT は $2^{(1-a)n}$ 時間では解けない。

SETH を以下のように変更する：

(1) k-CNF ⇒ log-depth Boolean circuit f　（強力になる）

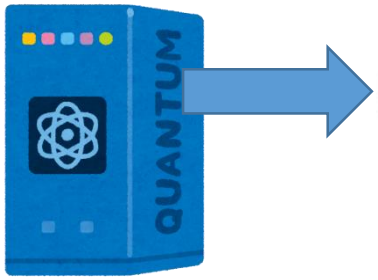
(2) SAT ⇒ gap(f)≠0 or=0　（たぶん強力になりそう）

(3) Deterministic time ⇒ non-deterministic time　（弱くなるかも）

$$gap(f) = \sum_{x \in \{0,1\}^n} (-1)^{f(x)}$$

# 結果

もしSETH-like conjectureが正しいなら、




$$z \in \{0,1\}^n$$

$$z \in \{0,1\}^n$$

古典計算機

N-qubit
one-clean qubit model

$$|p_z - q_z| \leq \epsilon p_z$$

量子計算機がzを出す確率

古典計算機がzを出す確率

任意のa>0 に対し

$$2^{(1-a)(N-3)}$$

時間必要

# Orthogonal vectors

Conjecture:

Given d-dim vectors, $u_1, \ldots, u_n, v_1, \ldots, v_n \in \{0,1\}^d$ with d=clog(n).
For any δ>0 there is a c>0 such that deciding gap≠0 or gap=0 cannot be done in non-deterministic time n^{2 − δ}.

$$gap = |\{(i,j) \mid u_i \cdot v_j = 0\}| - |\{(i,j) \mid u_i \cdot v_j \neq 0\}|$$

Result:

Assume that Conjecture is true. Then, for any δ>0 there is a c>0 such that there exists an N-qubit quantum computing that cannot be classically sampled within multiplicative error ε<1 in time $2^{\frac{(2-\delta)(N-4)}{3c}}$

# 3-SUM

Conjecture:

Given the set $S \subset \{-n^{3+\eta}, \ldots, n^{3+\eta}\}$ of size n, deciding

gap≠0 or =0 cannot be done in non-deterministic n^{2-δ} time for any η,δ>0.

$$gap = |\{(a,b,c) \mid a+b+c=0\}| - |\{(a,b,c) \mid a+b+c \neq 0\}|$$

Result:

Assume the conjecture is true. Then, for any η,δ>0, there exists an N-qubit quantum computing that cannot be classically sampled within a multiplicative error ε<1 in time $2^{\frac{(2-\delta)(N-15)}{3(3+\eta)}}$

# 応用

スパコンの量子計算のシミレーションにも応用！

現在、スパコンで量子計算をシミレートする研究が盛ん。

量子スプレマシーを破壊する研究：
米国：「７０量子ビットでスプレマシーでるよ」
中国：「うちのスパコンでシミレートできました」
米国：「うぐぐ」

量子計算を古典計算でシミレートするアルゴリズムの研究がさかん

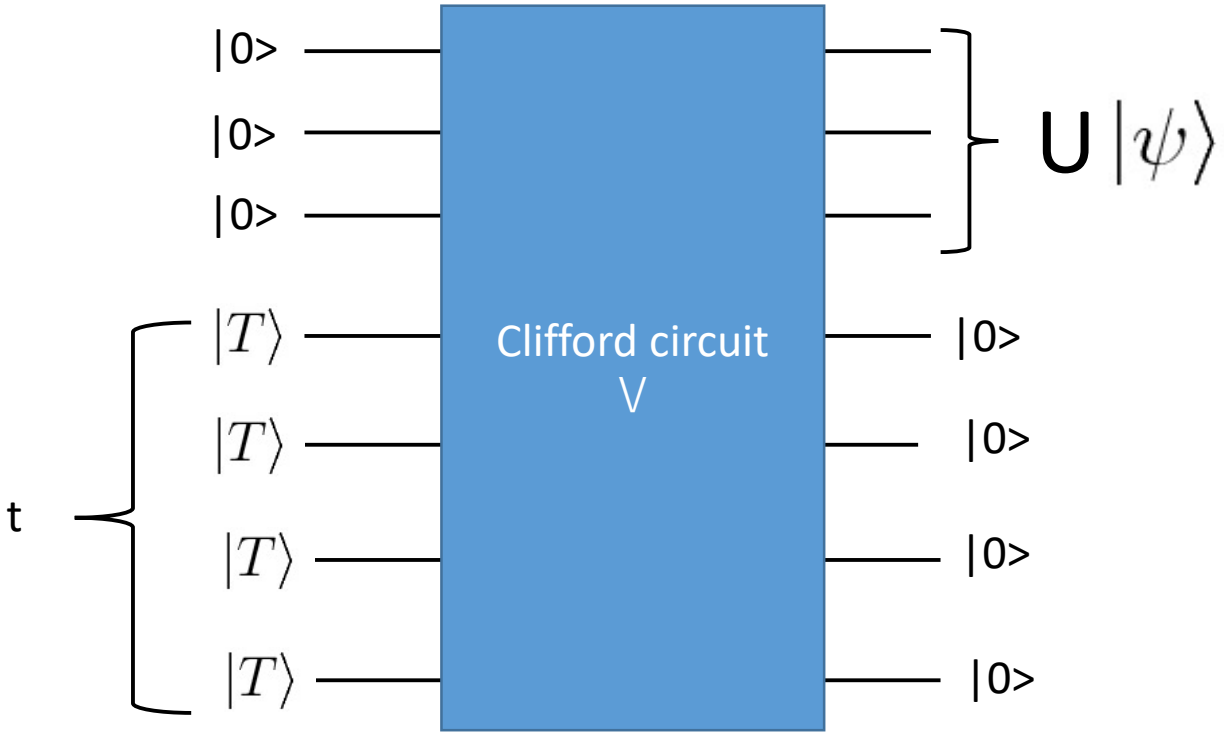
最も有名なもの：Bravy-Gosset アルゴリズム

Clifford+Tゲートでユニバーサル量子計算が可能。

Cliffordのみだと古典シミレート可能（Gottesman-Knill）
Tが量子スピードアップの「リソース」だ＝古典シミレートの複雑さはTに依存

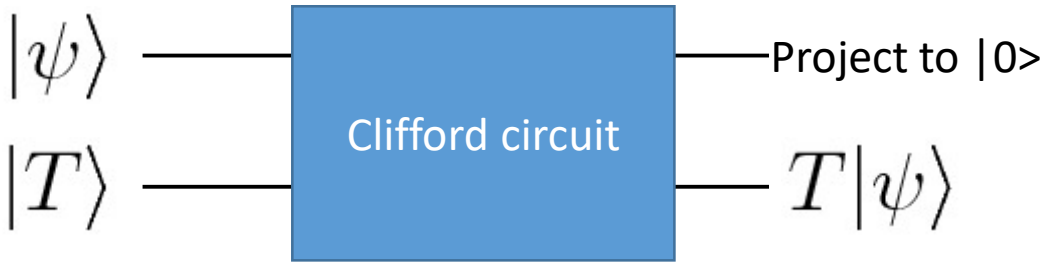
Ｔの個数をｔとする。2^{0.48t}時間でシミレート可能（Bravyi-Gosset）

U：クリフォードと t 個の T ゲートからなる量子回路




$$|T\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$$

Magic state gadget



# Bravyi-Gosset アルゴリズム

Clifford circuit

Stabilizer state

$$\langle 0^n|U|0^n\rangle = \langle 0^n|V(|0^m\rangle \otimes |T\rangle^{\otimes t})$$
$$= \sum_{j=1}^{\chi} c_j \langle 0^n|V(|0^m\rangle \otimes |\phi_j\rangle^{\otimes t})$$

χ<2^{0.48t}であることを証明→量子計算は2^{0.48t}時間でシミレートできる。

2^t時間で古典シミレート可能（Brute force）

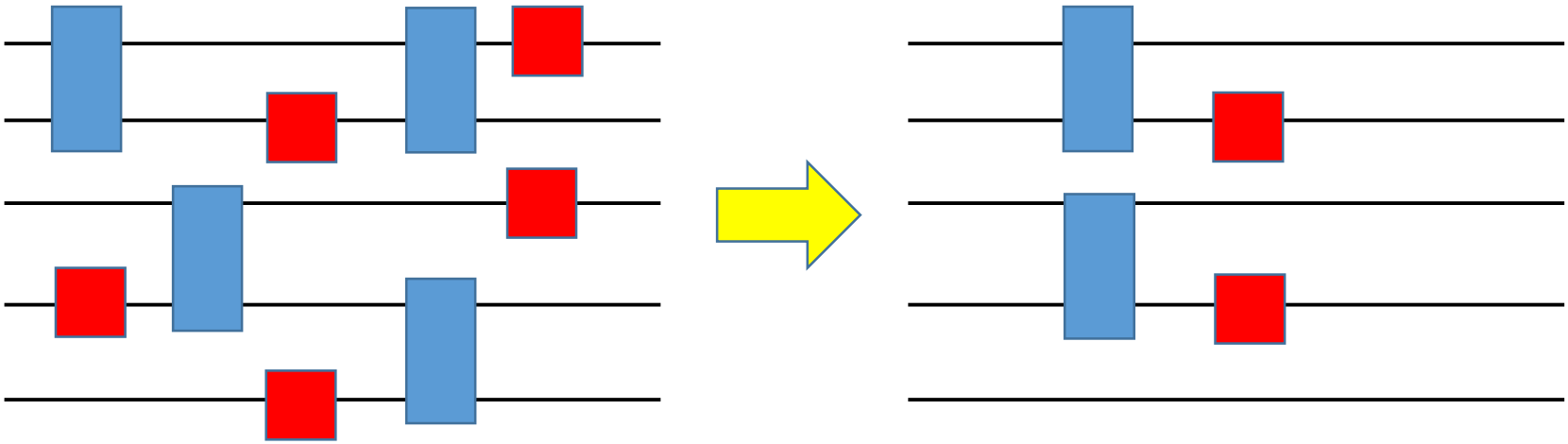
2^{0.48t}で古典シミレート可能（Bravyi-Gosset）

2^{o(t)}では古典シミレート不可（TM and Tamaki）

ETHが正しいなら

Quantum circuit optimization: 量子回路を最適化して、簡単にしたい！

特に、Tの個数を減らしたい！（Tは誤り訂正しにくい）



いろいろなアルゴリズムが提案されている[Zhang, arXiv:1903.12456]

→ o(T)個までは減らせない！（TM and Tamaki）

ETHが正しいなら

# ＡＣＴ－Ｘ

ＪＳＴ戦略的創造研究推進事業
ＣＲＥＳＴ、さきがけ、ＡＣＴ－Ｘ

数理・情報に関するテーマ
量子情報も対象！！！

若手対象：博士取得後８年以内もしくは大学院生

若手の方是非応募お願いします！若手の方への宣伝お願いします！

締め切り：５月２８日