古典検証者によるセキュアクラウド量子コンピューティング

～安心安全な量子クラウドの実現に向けて～

森前智行（京都大学基礎物理学研究所）

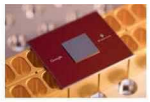
クラウド量子計算

1．プライバシーは保てるか
2．計算結果を検証できるか

２００９年に１が、２０１２年に２が可能であることが理論的に証明される。
（シンガポール、英国、カナダ、日本の研究者ら）

光量子コンピューターを用いた実験も（ウィーン大学）

量子スプレマシー



Google,IBM等が小さなサイズの量子コンピューターを実現

「弱い」量子コンピューターでも古典より本当に「強い」のか？

例：素因数分解。将来高速な古典アルゴリズムが見つかるかも→確固とした証拠ではない。

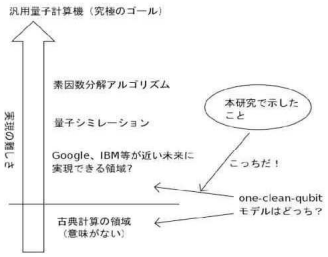
成果１

ポストフォック検証

量子クラウドの正しさを事後的にチェックできる新しいプロトコルの提案

成果２

１量子ビットモデルの量子スプレマシー



弱い量子コンピューターでも古典より強かった

詳細

Fitzsimons, Hajdusek, and TM, Physical Review Letters 120, 040501 (2018)

BQP decision problem
の結果１ビット送る

QMAのwitness送る
１量子ビット測定する

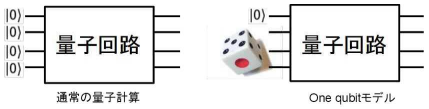
1. BQP is in QMA with trivial witness
2. QMA verification can be done with only single-qubit measurements [TM, Nagaj, and Schuch, PRA2016]
3. BQP is closed under complement

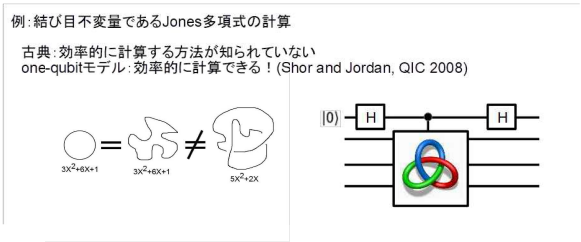
Local Hamiltonian problem:
Yes: ground energy of H is less than a
No: ground energy of H is larger than b

$$\frac{1}{\sqrt{T+1}}\sum_{t=0}^{T} U_t ... U_0 |0^n\rangle|t\rangle \qquad H=\sum_{i,j}[X_iX_j+Z_iZ_j+X_i+Z_i]$$

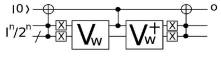
詳細

Fujii, Kobayashi, TM, Nishimura, Tamate, and Tani, to appear in Physical Review Letters 2018; ICALP2017





多項式階層が第二レベルで崩壊しない限り、one-clean qubit modelの出力確率分布は古典計算機で効率的にサンプルできない



$$P \subset NP \subset NP^{NP} \subset NP^{NP^{NP}} \subset \ldots$$