

オンライン教材：量子計算理論

量子回路

0. [基礎](#)
1. [Gottesman-Knill](#)
2. [Gottesman-Knill 2](#)
3. [マジック状態、T ガジェット](#)
4. [スタビライザーランク](#)
5. [スタビライザーランク予想、続き](#)
6. 論文を読んでみよう

Aaronson and Gottesman, quant-ph/0406196

Van den Nest, arXiv:0811.0898

Bravyi and Gosset, arXiv:1601.07601

Bravyi, Smith, and Smolin, arXiv:1506.01396

Morimae and Tamaki, arXiv: 1901.01637

測定型量子計算

1. [グラフ状態](#)
2. [グラフ状態の性質](#)
3. [1量子ビットユニバーサル量子計算、続き](#)
4. [ユニバーサル量子計算](#)
5. [Matrix product states、続き](#)
6. [テンソルネットワーク](#)

量子計算量理論

1. P、BPP、BQP
2. $BQP \subseteq PSPACE$
3. NP
4. QMA、QCMA
5. Local Hamiltonian problem

量子スプレマシー

1. [Strong simulation](#)
2. [Weak simulation、サンプリング](#)
3. Strong simulation と weak simulation の関係
4. IQP モデル、古典イジング分配関数
5. DQC1 モデル
6. Multiplicative error サンプリング不可能性
7. Additive error サンプリング不可能性

量子暗号プロトコル

1. [Quantum one-time pad](#)
2. [Pauli twirling](#)
3. Quantum authentication
4. Quantum digital signature
5. [ブラインド量子計算 1 : BFK プロトコル](#)
6. [ブラインド量子計算 2 : MF プロトコル](#)
7. [量子計算の検証 1 : ポストフォックプロトコル](#)
8. 量子計算の検証 2 : マハデフ
9. Interactive proof of quantumness
10. [量子ゼロ知識 1 : GMW GI プロトコルの量子攻撃に対するゼロ知識性](#)
11. [量子ゼロ知識 2 : GMW 3C プロトコルの量子攻撃に対するゼロ知識性、続き](#)
12. 量子ゼロ知識 2 : QMA に対するゼロ知識

参考書等：

量子情報全般：Nielsen-Chuang

古典計算量理論：Arora-Barak

量子対話型証明：Vidick-Watrous (<https://arxiv.org/abs/1610.01664>)

量子計算全般：量子計算理論、森前

測定型量子計算：観測に基づく量子計算、小柴・藤井・森前

Dorit Aharonov による Local Hamiltonian complexity の講義 [1](#)、[2](#)、[3](#)

(3の16：45あたりからポストフォックプロトコルについても簡単に説明されている。)

Thomas Vidick による量子計算量理論、量子計算の検証、量子 authentication の講義 [1](#)、[2](#)、[3](#)

Joe Fitzsimons によるブラインド量子計算、量子計算の検証の[講義](#)