

### 量子コンピュータIBMQを用いた量子非局所性の検証 Verification of quantum nonlocality using cloud quantum computer

総合政策学部2年 西尾 真

本研究では、量子もつれにおける非局所性や隠れた変数理論を判定する**CHSH不等式**を、IBMの**クラウド量子コンピュータ**によって量子もつれを生成し複数の基底で観測することで検証した。

1935年にアインシュタイン、ポドルスキー、ローゼン(頭文字からEPR)は、局所実在論的立場から、量子力学における量子もつれが相対性理論と矛盾する可能性を指摘した(**EPRパラドックス**)。[1] EPRの主張を検証するため、**CHSH不等式**などの不等式が考案された。[2] これは、複数の量子の状態の相関を導出するものである。

CHSH不等式  $|\langle AB \rangle - \langle aB \rangle + \langle Ab \rangle + \langle ab \rangle| \leq 2$   
CHSH不等式の値(n)は、 $n < 2$ (不等式成立)で**古典的相関**、 $2 < n < 2\sqrt{2}$ で**量子非局所的相関**、 $2\sqrt{2} < n$ で物理的に不可能な相関(**実験失敗**)となる。

およそ半世紀後、光学系を用いてアラン・アスペらが実験を行い不等式を検証した。

しかし、この実験は再現が難しい上実験装置は非常に高額である。[3] よって、本研究ではより手軽に追実験を行えるように、IBMQ(図1)[4]を用いてBell pair(図2)を観測する。

観測基底は、 $Z, X, \frac{Z+X}{\sqrt{2}}, \frac{Z-X}{\sqrt{2}}$ 測定を採用し、それぞれ**A, a, B, b**と呼称する。(図3)



図1 IBM Q [5]

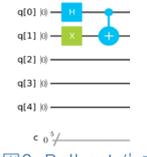


図2 Bell pair生成

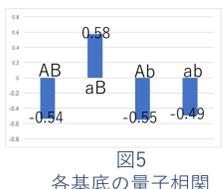
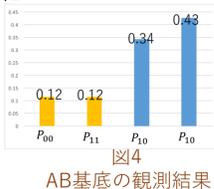
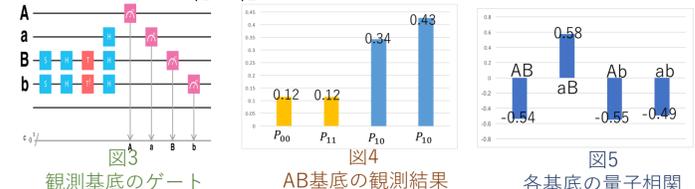


図6 全測定データ

測定基底	量子状態の観測確率				相関 <MN>
	$P_{00}$	$P_{11}$	$P_{01}$	$P_{10}$	
AB	0.12	0.12	0.34	0.43	-0.54
aB	0.35	0.43	0.11	0.1	0.58
Ab	0.18	0.05	0.41	0.36	-0.55
ab	0.17	0.09	0.43	0.32	-0.49

#### 結果

相関は、それぞれの観測基底(例: 図4)に対し、 $\langle MN \rangle = P_{00} + P_{11} - P_{01} - P_{10}$ として導出できる。(図5)[6] 全ての結果をまとめると(図6)のようになる。CHSH不等式の値は**2.156**となり、2以上 $2\sqrt{2}$ 以下なので、不成立となる。(図7)



よって、局所実在論は誤りで、**量子非局所性が存在することが示された**。

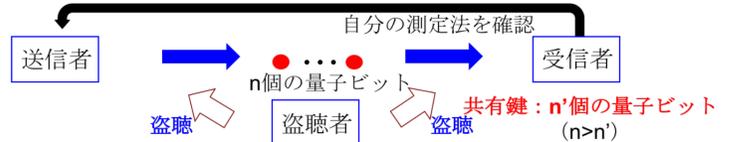
- [1] milena, 2013"L'Intrication quantique persiste entre deux photons si l'un disparaît"
- [2] 筒井泉, 高エネルギー加速器研究機構・素粒子原子核研究所 "物性研究 Vol.3, No.1, 031209(2013年11月・2014年2月合併号); 量子力学の基礎に関する最近の話題"
- [3] Chanou 2017"Cosmic Bell Test: Measurement Settings From Milky Way Stars"
- [4] IBM, 2017"Learn about IBM Q and quantum computing"
- [5] IBM Research, 2017 "IBM 50Q system"
- [6] 中山茂, 2016"クラウド量子計算入門 IBMの量子シミュレーションと量子コンピュータ"

### BB84シミュレータを用いた通信ノイズの定量的評価 Quantitative evaluation of noise using BB84 simulator

環境情報学部3年 尾澤慎之介

量子力学の性質を用いて盗聴の影響なしに鍵を共有する**量子鍵配送(QKD)**のシミュレータを実装し、実際のネットワーク上で存在する**ノイズ・盗聴の影響**を再現した上で量子鍵配送のシミュレートを行なった。

量子力学によると、**量子ビット(qubit)**は状態を測定するとその状態が変化してしまう。これを応用した鍵の共有方法が**量子鍵配送(Quantum Key Distribution)**のプロトコル**BB84**[1]である。共有鍵を生成するためのランダムな量子ビット列のいずれかが盗聴(測定)されると盗聴された量子ビットの状態は変化する。ここで変化した量子ビットを省いて残った量子ビット列を暗号化された通信の復号化を行う鍵とする。



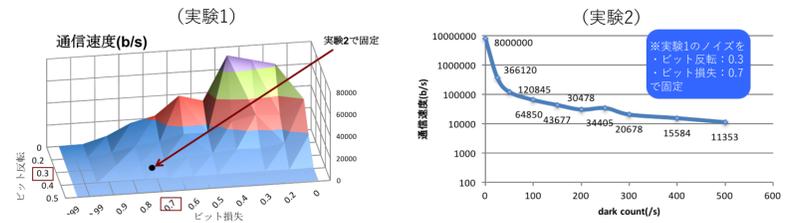
量子鍵配送プロトコルのうちBB84[1]は様々な量子暗号装置が市販されており[2]、またQKDを要素技術としたセキュアネットワークが実現している[3]ように、最も実用化に近いプロトコルである。現段階の問題として、

- 通信速度遅い(数10kbps~1Mbps)
- ノイズが一定条件を超えるとノイズ・盗聴どちらの影響で通信が失敗したかが判定不可能となるなどの点があるが、[4]や[5]のようにこれに対して様々な対処法が考えられている。

今回はC言語により量子鍵配送プロトコルBB84のシミュレータを実装し、2017年6月にNICTの行なった量子通信実験[6]の値を参考にシミュレーションを行なった。

実験1: 通信路のノイズ(量子ビットの損失、反転)の影響を測定  
実験2: 実験1にてノイズを固定し、dark count(量子ビットの誤受信)の影響を測定

**結論: 通信を実現するためには膨大な数の量子ビットを送信する必要があり、通信後のエラー訂正やプライバシー増幅を考慮すると通信速度を改善する必要がある。**



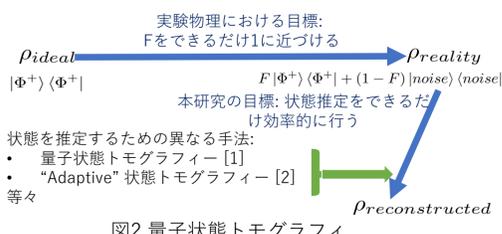
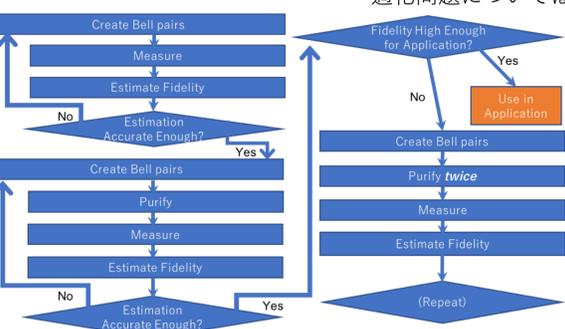
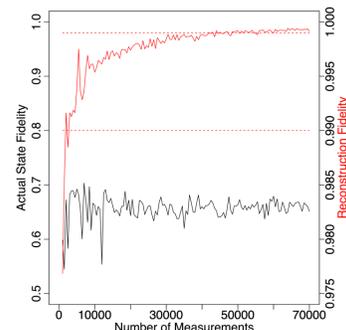
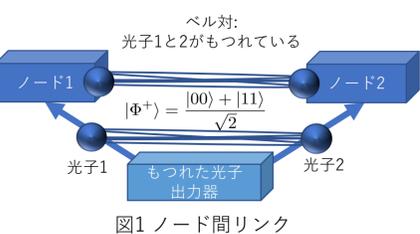
- [1] C.H.Bennett and G.Brassard "Quantum Kye Cryptograpy: Public Kye distribution and Coin Tossing"
- [2] 量子暗号の基礎とその実用化に向けて <http://ibisml.org/ibis2010/session/ibis2010tsurumaru.pdf>
- [3] 谷澤佳道, 高橋莉奈, 香 量子鍵配送技術に基づくセキュアネットワーク 2014
- [4] Andrew J. Shields, Zhiliang Yan High-Bit-Rate Unconditionally Secure Quantum Key Distribution 2009
- [5] NICT "量子鍵配送に関する新理論を確立" <https://www.nict.go.jp/press/2014/10/24-2.html>
- [6] NICT "超小型衛星による量子通信の実証実験に世界で初めて成功" <https://www.nict.go.jp/press/2017/07/11-1.html>

### 量子ネットワークにおけるノード間リンク生成のための最適な純粋化方法の提案

Optimal Fidelity Estimation in Purification for the Fastest Bootstrap of a Quantum Link

環境情報学部4年 岡 尚史

量子ネットワークの実現に向けて、量子中継器やリンクなどの構成装置の状態確認を行う手法が必要となる。本研究では、量子ネットワークにおける**量子トモグラフィ**の運用(図1,2,4)を想定し、具体的な**プロトコルの提案**と、**リソース消費の定量的評価**を行った。



量子中継器ネットワークでは、通信資源として量子もつれ状態にある量子ビット対を用いる。量子ビットは、測定により古典ビット(0/1)に確率的に収束し、直接的に、しかし、多数の試行を繰り返すことにより、これらの古典ビットの情報を集めれば、元の量子ビット対を推定することができる。この手続きを、量子トモグラフィと呼ぶ。試行の回数が多ければ多いほど、量子ビットを正確に推定することができる。しかし、現在提案されているトモグラフィの手法は、量子ネットワークにおける利用は想定されていない。離れた2地点におけるノード間リンクの生成を想定した、トモグラフィ運用のプロトコル、および、既存の量子状態トモグラフィでの状態推定精度(fidelity)と、必要な試行回数との関係(図3)は[3]にて研究されている。前述の最適化問題については、現在研究中である。

- [1] Altepeter, J. B., Jeffrey, E. R., & Kwiat, P. G. (2005). Photonic State Tomography. *Advances In Atomic, Molecular, and Optical Physics*, 52, 105-159. [http://doi.org/10.1016/S1049-250X\(05\)52003-2](http://doi.org/10.1016/S1049-250X(05)52003-2)
- [2] Blume-Kohout, R. J., Mahler, D. H., Rozema, L. A., Darabi, A., Ferrie, C. S., & Steinberg, A. M. (2012). Adaptive Quantum State Tomography Improves Accuracy Quadratically. *Proposed for Publication in Arxiv.org*. Retrieved from <https://www.osti.gov/scitech/biblio/1062365>
- [3] Oka, T., Satoh, T., & Van Meter, R. (2016). A Classical Network Protocol to Support Distributed Quantum State Tomography. In *2016 IEEE Globecom Workshops (GC Wkshps)* (pp. 1-6). IEEE. doi:10.1109/GLOCOMW.2016.7848802

### 量子中継器ネットワークのための測定型量子ネットワークコーディング

Measurement-based Quantum Network Coding for Repeater Networks

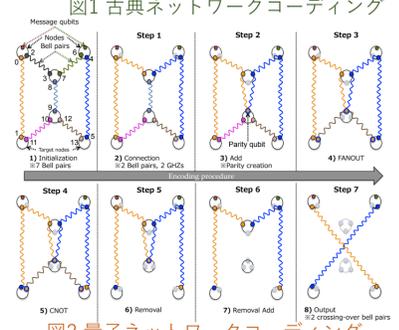
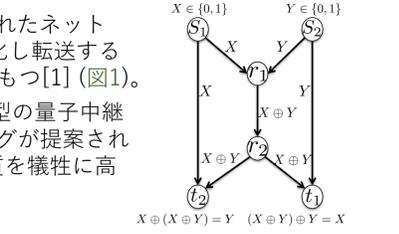
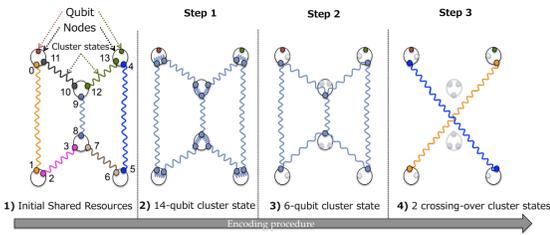
政策・メディア研究科 修士1年 松尾賢明

本研究は、**バタフライ型の量子中継器ネットワーク**で発生する**ボトルネック問題**を、より簡単に解決するための**測定型量子ネットワークコーディング**プロトコルの考案とノイズ下における性能評価をモンテ・カルロシミュレーションによって行った。

2000年にAhlsweide, Cai, LiとYeungによって提案されたネットワークコーディングは、中継器内で複数の情報を符号化し転送する事で、単純な経路選択手法よりも高い情報伝達能力をもつ[1](図1)。

2012年には, Satoh, Le Gall, Imaiによってバタフライ型の量子中継器ネットワークのための量子ネットワークコーディングが提案され[2](図2), 2016年に経路選択手法と比較して、通信品質を犠牲に高いスループットを有する相対的な優位性を示した[3]。

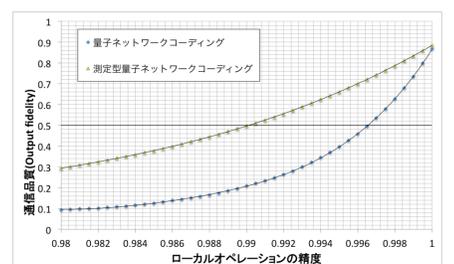
本研究では、量子ネットワークコーディングの高いスループットを維持したまま、高い通信品質を実現するために、並列処理を行える測定型量子計算を応用した新しいプロトコルを考案した(図3)。



評価を行うにあたって、以下のエラーソースをモンテ・カルロシミュレーションに採用した。

1. 中継機間の初期リソースエラー
2. ローカルオペレーションエラー
  - a) 単一-qubit/制御ゲートエラー
  - b) 測定エラー
  - c) メモリエラー

モンテ・カルロシミュレーションによって、考案されたプロトコルは既存のもの比べて、**同等のスループットを保持しながら、約2倍の通信品質を確保できることが示された(図4)**。



- [1] Rudolf Ahlsweide, Ning Cai, Shuoyen Robert Li and Raymond W. Yeung Network information flow IEEE Transactions on Information Theory 2000 Vol. 46, no. 4, pp. 1204-1216
- [2] T. Satoh, F. Le Gall, and H. Imai, Phys. Rev. A 86, 032331 (2012)
- [3] T. Satoh, K. Ishizaki, S. Nagayama, and R. Van Meter, Phys. Rev. A 93, 032302 (2016).