Vol.2020-QS-1 No.9
2020/10/16

量子サンプリングの検証

廣岡　大河[1,a)]　竹内　勇貴[2,b)]　森前　智行[1,c)]

概要：
量子計算が正しく動作しているかを古典計算機のみで検証できるかという問題は基礎的、応用的に重要であり近年盛んに研究がなされている。例えば、クライアントが量子ビットを生成できる場合は、Fitzsimons-Kashefi(FK) プロトコルと呼ばれる方法で、量子計算の検証をすることが可能である。しかしながら、FK プロトコルや他の既存の方法では量子計算のサンプリング問題を計算内容に依存しない最初の量子通信 (オフライン量子通信) を用いて検証することはできない。量子計算の出力確率分布をサンプリングする問題は古典計算機では効率的にできないことが（計算量的仮定のもとで）証明されている（量子超越性)。したがって、これを検証するプロトコルを構築することは重要である。本講演では量子サーバーが正しく状態を測定していることを検証するプロトコルを提案する。このプロトコルと FK プロトコルを組み合わせることにより、オフライン量子通信を用いて量子サンプリング問題を検証することができる。

1. はじめに

量子計算機が実用化されても、各個人がすぐに量子計算機を持つことは技術的、経済的に困難である。そこで、量子計算機を持っていない人が量子計算を行いたい時には、量子計算機を所有している企業に量子計算を委託する必要がある。量子計算機を所有している企業（以降証明者と呼ぶ）は必ずしも正しく計算を行わず、量子計算を委託する人（以降検証者と呼ぶ）は証明者が正しく計算を行っているかを検証する必要がある。このように、量子計算は検証可能かどうかという問は応用的に大変関心がもたれており、近年活発に研究が行われている。また、基礎的には理論計算機科学における重要な一つの分野である量子対話型証明 [1] とも密接な関連があり、基礎的応用的ともに重要な研究である。

検証者が量子ビットを生成できる場合は情報理論的な健全性のもとに量子計算が正しく行われていることを検証できることが知られており様々なプロトコルが提案されている [2–6]。しかしながら、これらのプロトコルでは計算内容に依存しない量子通信は初めのみに行い、その後の計算内容に依存する通信はすべて古典通信のみで行うこと（オフライン量子通信）で量子計算のサンプリング問題を検証することができない。量子計算のサンプリング問題は古典計算機では（計算量的仮定のもとで）効率的に行うことができない（量子超越性）[7–9] ので、これを検証するプロトコルの開発は重要である。

本研究では証明者に測定を委託し、証明者が正しく状態を測定していることを検証するプロトコル（プロトコル 1）を提案することでこの問題を解決する。以下では我々が提案するプロトコルを概説する。

検証者は m 個の n-qubit レジスターを用意し、ランダムに 1 つ計算用のレジスターを選び、残りの $m-1$ 個についてはテスト用のレジスターとする。テスト用のレジスターでは検証者はそれぞれのレジスターごとに $a^i \equiv (a^i_1, ..., a^i_n) \in \{0,1\}^n$ をランダムに選び (i = 1,2...,$m-1$)、n-qubit 状態 $X^{a^i}|0^n\rangle$ を生成する。ここで、$X^{a^i} \equiv \bigotimes_{j=1}^{n} X^{a^i_j}$ である。計算用のレジスターでも、$(\alpha, \beta) \in \{0,1\}^n \times \{0,1\}^n$ をランダムに選ぶ。その後、行いたい計算に対応する n-qubit 状態 $|\Psi\rangle$ を生成し、$X^\alpha Z^\beta$ を $|\Psi\rangle$ に対して作用させ、$X^\alpha Z^\beta|\Psi\rangle$ を作る。

次に検証者は用意したレジスターを順番に証明者に送る。証明者はもらったレジスターの各量子ビットを計算基底で測定し、測定結果を検証者に伝える。すべてのテスト用のレジスターについて、検証者は伝えられた古典メッセージが a^i の時に受理する。このとき証明者は計算用のレジスターについても高い確率で正しく計算基底で測定していることが証明できる。

上記の手法がうまくいく直感的な理由は以下のとおりである。送られてくるレジスターにはランダムに XZ がかけられているので、証明者にとって検証者から送られてくる

[1] Yukawa Institute for Theoretical Physics, Kyoto University
[2] NTT communication science laboratories
[a)] taiga.hiroka@yukawa.kyoto-u.ac.jp
[b)] yuki.takeuchi.yt@hco.ntt.co.jp
[c)] tomoyuki.morimae@yukawa.kyoto-u.ac.jp

状態は完全混合状態であり（量子ワンタイムパッド）、計算用のレジスターとテスト用のレジスターを区別できない。したがって、計算用のレジスターには計算基底以外の測定を行いテスト用のレジスターには正しく計算基底測定を行うということができないのである。

我々が提案するプロトコルでは検証者が状態の準備と量子操作が行え測定のみが行えない時に、測定を証明者に委託し証明者が正しく測定を行っていることを検証する。我々が提案するプロトコルと FK プロトコルを併せて用いることで行いたい計算に対応する状態の準備と量子操作を証明者に委託できる。そのようにして作られたプロトコルにおいては、計算内容に依存しない量子通信は初めのみで、その後の通信はすべて古典通信のみで（オフライン量子通信）で、量子計算のサンプリング問題を検証することが可能である。

本論文の構成は以下の通りである。第 2 章で記法や本結果の説明に必要な準備を導入する。第 3 章では正しい測定を定式化し、測定を検証するプロトコル 1 を導入する。第 4 章では主な結果である定理 5 の証明を行う。第 5 章では、我々が提案するプロトコルと FK プロトコルを組み合わせることでサンプリング問題の検証ができることをみる。

2. 記法や準備

2.1 量子ワンタイムパッド

量子ワンタイムパッドは量子状態を暗号化する手法であり任意の n-qubit 状態 ρ を以下のように変形する。

$$\frac{1}{4^n}\sum_{a,b\in\{0,1\}^n} X^a Z^b \rho Z^b X^a = \frac{I^{\otimes n}}{2^n} \qquad (1)$$

ここで $(a,b)\equiv(a_1\dots a_n, b_1\dots b_n)\in\{0,1\}^n\times\{0,1\}^n$ は古典ビットで暗号化の鍵となっている。また、$X^aZ^b\equiv\bigotimes_{i=1}^n X^{a_i}Z^{b_i}$ であり、後についても断り無くこの記法を用いる。 この暗号化の方法は攻撃者が鍵の知識が無い場合において情報理論的安全性を満たしている。ρ の状態をあらかじめ知っているときに関しては暗号化する際には Z など必要が無い場合もある。(e.g., ρ=$|0\rangle\langle 0|$ の場合には Z は不必要である。)

2.2 量子超越性

IQP モデルは n-qubit 状態 $|0^n\rangle$ に $H^{\otimes n}$ を作用させ、その後、Z 基底で見たとき対角行列であるゲートから構成される回路を作用させ、最後に $H^{\otimes n}$ を作用させ計算基底で測定を行うような量子計算モデルである。IQP モデルはユニバーサルな量子計算を行うことはできない。しかし、IQP モデルは統計物理や測定型量子計算 [10] とも関連があり、広く研究されている。また、IQP 回路の出力確率分布をある定数の l_1-norm エラーで古典多項式時間でサンプルすることは計算量的仮定のもとで不可能であることが知られている（量子超越性)。ここで出力確率分布 $\{p(x)\}$ を l_1-norm エラー ϵ でサンプルするとは以下を満たす出力確率分布 $\{q(x)\}$ で x のサンプリングを行うことである。

$$\sum_{x\in\{0,1\}^n}|p(x)-q(x)|\le\epsilon$$

より正確に上の量子超越性の主張を定式化すると以下の通りである。

定理 1. [7] 以下の仮定 2 が成立するとする。このときもし任意の IQP 回路の出力を古典多項式時間で l_1-norm エラー $1/192$ でサンプルできたとすると、$\mathrm{P}^{\#\mathrm{P}}$ に属している任意の問題について $\mathrm{BPP}^{\mathrm{NP}}$ のアルゴリズムが存在する。つまり、多項式階層が第三レベルで崩壊する。

仮定 2. $f:\{0,1\}^N\to\{0,1\}$ は一様ランダムな F_2 上の 3 次多項式とする。このとき $\frac{1}{24}$ の割合の多項式 f について $\frac{gap(f)}{2^N}^2$ を乗的エラー $\frac{1}{4}+o(1)$ で近似することが #P 困難である。ここで、$gap(f)\equiv|\{x:f(x)=0\}|-|\{x:f(x)=1\}|$ である。また、乗的エラー ϵ である確率分布 $\{p(x)\}$ をサンプルするとは以下を満たす出力確率分布 $\{q(x)\}$ で x のサンプリングを行うことである。

$$|p(x)-q(x)|\le\epsilon p(x)\qquad\forall x\in\{0,1\}^n$$

2.3 FK protocol

このプロトコルでは 1 量子ビットを作り出せる検証者が任意の量子計算ができる証明者に量子計算を委託し、計算が正しく行われていることを検証できる。初めに検証者は証明者に 10 通りのランダム 1 量子ビット状態を多数送りグラフ状態 [10] を証明者に作成してもらう。その後検証者は証明者に対してどのような基底で状態を測定してほしいかを古典メッセージを送ることで伝え、証明者は送られてきた古典メッセージに対応する基底で測定し得られた結果を検証者に伝える。グラフ状態を測定することで任意の量子計算を行うことが可能であるため [10]、もし証明者が正直であり、検証者の指示通り状態を測定しているとき検証者は望みの量子計算の結果を得ることができる。一方証明者が悪意があり、検証者の指示と異なる操作をしても検証者はある一定の確率でその攻撃を検出できる。しかし、そのためには、「正しい計算結果」を定義できる必要がある。決定問題（Yes または No で答えられる問題）や量子状態を生成するタスクなどでは簡単に定義することができるが、サンプリング問題の場合は自明ではない。そのため、FK プロトコルをオフライン量子通信で直接サンプリング問題に適応することはできない。我々は次章で示すように「正しい測定」を定義し、それを検証するプロトコルを提案することで、この問題を解決した。

3. 検証プロトコル

以下のように「正しい測定」を定義する。

定義 3. $(n+k)$-qubit ユニタリー U が ϵ-correct であるとは、$\frac{1}{2}\sum_x |P(x)-P_U(x)| = \epsilon$ を満たすことである。ここで、$\Pi(x) \equiv |x\rangle\langle x| \quad (x \in \{0,1\}^n)$ に対して、$P(x)$、$P_U(x)$ は以下の通りである。$P(x) \equiv \frac{1}{2^n}\sum_{a\in\{0,1\}^n} \mathrm{Tr}[\Pi(x+a)|a\rangle\langle a|]$、$P_U(x) \equiv \frac{1}{2^n}\sum_{a\in\{0,1\}^n} \mathrm{Tr}[(\Pi(x+a)\otimes I^{\otimes k})U(|a\rangle\langle a| \otimes |0^k\rangle\langle 0^k|)U^\dagger]$ である。

以下では、上の定義 3 を満たすようなユニタリーを ϵ-correct unitary と呼ぶ。ϵ-correct unitary は以下の性質を満たす。

定理 4. $|\Psi\rangle$ は任意の n-qubit 状態とする。また、$\Pi(x) \equiv |x\rangle\langle x| \quad (x \in \{0,1\}^n)$、$U$ は ϵ-correct unitary とする。ここで

$$P^c(x) \equiv \mathrm{Tr}[\Pi(x)|\Psi\rangle\langle\Psi|]$$
$$P_U^c(x) \equiv \frac{1}{4^n}\sum_{a,b\in\{0,1\}^n} \mathrm{Tr}[(\Pi(x+a)\otimes I^{\otimes k}) U(X^aZ^b|\Psi\rangle\langle\Psi|Z^bX^a \otimes |0^k\rangle\langle 0^k|)U^\dagger]$$

の l_1-norm は以下を満たす。

$$\frac{1}{2}\sum_x |P_U^c(x) - P^c(x)| \le \epsilon \qquad (2)$$

証明 付録 A.3 に記載。
U を ϵ-correct unitary とすると、定理 4 は

$$\frac{1}{4^n}\sum_{a,b\in\{0,1\}^n} U(X^aZ^b|\Psi\rangle\langle\Psi|Z^bX^a \otimes |0^k\rangle\langle 0^k|)U^\dagger$$

の $|\Psi\rangle$ 部分（はじめの n-qubit）を計算基底で測定し得られる結果の確率分布と、$|\Psi\rangle$ を計算基底で測定し得られる結果の確率分布が l_1-norm の意味で近いことを表している。したがって、検証者は証明者が ϵ-correct unitary を計算用レジスターと補助 qubit に作用させた後、計算用レジスターを計算基底で測定していることを検証すればよい。

以下で測定を検証するプロトコルを導入する。

プロトコル 1

1. 検証者は測定のパラメーター δ を決める $(0 \le \delta \le 1)$。ラウンドの回数を表す i を $i = 1$ とする。テストに合格した回数を表す C を $C = 0$ とする。
2. 検証者は n-qubit レジスターを m 個用意する。検証者は証明者にはわからないように一様ランダムにレジスターを一つ選び、選んだレジスターを計算用のレジスターとする。残りの $(m-1)$ 個についてはテスト用のレジスターとする。計算用のレジスターについては検証者は測定してほしい量子状態 $|\Psi\rangle$ を用意し、テストレジスターについては $|0^n\rangle$ を用意する。
3. 検証者は n ビット長鍵 $a \equiv (a_1, ...a_n) \in \{0,1\}^n$ と $b \equiv (b_1, ...b_n) \in \{0,1\}^n$ を一様ランダムに選ぶ。X^a と Z^b を i 番目のレジスターに作用させる。ここで $X^a \equiv \bigotimes_{j=1}^n X^{a_j}$ であり、$Z^b \equiv \bigotimes_{j=1}^n Z^{b_j}$ である。
4. 証明者が正直な場合は、送られてきた状態に対して計算基底測定を行い、得られた結果を $x \in \{0,1\}^n$ とし x を検証者に送り返す。
証明者が悪意のある場合は、送られてきた量子状態に対して任意の操作を行ったのち測定を行い、得られた結果 $x \in \{0,1\}^n$ を検証者に送る。
5. 検証者が送ったレジスターがテストレジスターだった場合、$x = a$ のとき、$C = C + 1$ とする。
検証者が計算レジスターを送った場合は、$C = C$ とする。
6. $i = m$ の時、7 を行う。$i \ne m$ の時、$i = i + 1$ として 3 に戻る。
7. $C = m - 1$ の時、検証者は証明者を受理する。

プロトコル 1 において以下が成り立つ。

定理 5. ϵ^* が $\delta \le \epsilon^* \le 1$ を満たし、U を ϵ^*-correct unitary とする。$\delta \le \frac{1}{m}$ のとき以下が成り立つ。検証者が証明者を受理かつ、証明者が計算用レジスターと補助 qubit に U を作用させた後、計算用レジスターを計算基底測定する確率の上限は $(1-\delta)^{m-1}$ である。

4. 定理 5 の証明

上の定理 5 を証明するのに以下の補題 6 と系 7 が必要である。

補題 6. U を ϵ-correct unitary とする。証明者がテストレジスターと補助 qubit に U を作用させた後、テストレジスターを計算基底測定しているとき $x = a$ となる確率は $1-\epsilon$ となる。

証明は付録 A.4 を参照。
補題 6 を用いると以下の系 7 が成り立つことがわかる。

系 7. ϵ^* が $\delta \le \epsilon^* \le 1$ を満たすとする。U_{ϵ^*} を ϵ^*-correct unitary とする。証明者がテストレジスターと補助 qubit

に U_{ϵ^*} を作用させた後テストレジスターを計算基底測定するとき、$x = a$ となる確率の上限は $1-\delta$ となる。

以上の補題 6、系 7 から定理 5 を示すことができる。

証明

以下の証明では $0 \leq \epsilon < \delta$、$\delta \leq \epsilon^* \leq 1$ とする。また、U_ϵ は ϵ-correct unitary で、U_{ϵ^*} は ϵ^*-correct unitary だとする。

証明者は送られてきた量子状態について何らかの操作を行いその後測定を行う。どのような測定も注目している系と補助系のユニタリー発展と計算基底での測定で表すことができるので証明者の操作は補助系をあわせたユニタリーを考えるだけで十分である。証明者がどのようなユニタリーを状態にかけるかは、一般に証明者の乱数、検証者が送る状態、ラウンド数に依存するが、証明者の乱数に対する依存性は量子回路で表現することができ、一つのユニタリーとしてまとめることができる。また検証者の送る状態についてはプロトコル 1 については量子ワンタイムパッドされており完全混合状態になっているので証明者には区別できない。したがって、証明者がどのようなユニタリーを状態に作用させるかはラウンド数にのみ依存すると考えてよい。ユニタリーは定義 3 のように ϵ で特徴づけることができる。i 番目のレジスターにかかるユニタリーを ϵ_i-correct unitary として、U_{ϵ_i} と書くこととする。

検証者が証明者を受理かつ証明者が計算用のレジスターと補助 qubit に U_{ϵ^*} を作用させて、計算用レジスターを計算基底で測定する確率を $\Pr(acc \cap \epsilon^*)$ と定義する。$\Pr(acc \cap \epsilon^*)$ は証明者がラウンドごとに U_ϵ を状態に作用させるか、U_{ϵ^*} を状態に作用させるかに依存するので、ラウンド毎に U_ϵ を作用させているか U_{ϵ^*} を作用させているかで場合分けを行い計算を進める。

いま検証者が計算用のレジスターを何番目に選ぶかは一様ランダムなので、U_ϵ が作用されているレジスターの数で場合分けを行うとよい。

証明者が測定している m 個のレジスターのうち k 個のレジスターについては U_{ϵ^*} を作用させた後、計算基底測定を行い、$(m-k)$ 個については U_ϵ を作用させた後、計算基底測定を行う場合を考える。このとき計算用レジスターに U_{ϵ^*} を作用させた後、計算基底で測定する確率は $\frac{k}{m}$ となる。このとき検証者が証明者を受理する確率 $\Pr(acc)$ は以下の通りになる。以下の等式で補題 6 を用いた。

$$\Pr(acc) = \prod_{i:0\leq\epsilon_i<\delta} (1-\epsilon_i) \prod_{j:\delta\leq\epsilon_j\leq 1}^{\bar{c}} (1-\epsilon_j)$$

ここで $\prod_{i:0\leq\epsilon_i<\delta}$ は $0 \leq \epsilon_i < \delta$ を満たす i について積をとるという意味であり、$\prod^{\bar{c}}_{j:\delta\leq\epsilon_j\leq 1}$ は計算用レジスターに作用させたものを除く $\delta \leq \epsilon_j \leq 1$ を満たす j について積をとるという意味である。

したがって、$\Pr(acc \cap \epsilon^*)$ は以下のように計算される。

$$\begin{aligned}\Pr(acc \cap \epsilon^*) &= \frac{1}{m} \sum_{\bar{c}} \prod_{i:0\leq\epsilon_i<\delta} (1-\epsilon_i) \prod_{j:\delta\leq\epsilon_j\leq 1}^{\bar{c}} (1-\epsilon_j) \\ &\leq \frac{k}{m}(1-\delta)^{k-1}\end{aligned}$$

二つ目の不等式の変形について系 7 を用いた。また、$\sum_{\bar{c}}$ は省かれる計算レジスター毎の和をとることを表している。$\delta \leq \frac{1}{m}$ の時 $k = m$ で以下のように上界が与えられる。

$$\Pr(acc \cap \epsilon^*) \leq (1-\delta)^{m-1}$$

5. 応用

プロトコル 1 では検証者が量子状態の準備と量子操作を行うことができるときに、証明者に測定を委託し、証明者が正しく状態を測定していることを検証することができた。プロトコル 1 と FK プロトコルを併用して用いることで計算内容に依存しない量子通信は初めにのみ行い、その後の計算に依存する通信はすべて古典通信のみ行うことにより検証者は量子サンプリングの検証を行うことができる。

検証者は m 回レジスターを送るのだが、そのうちの 1 つのレジスターについては通常の FK プロトコル通り、10 通りの 1 量子ビット状態を一様ランダムに生成し多数送り、グラフ状態を生成してもらう。その後古典メッセージのやりとりで検証者が証明者を受理したとき、最終的に生成された量子状態は確率 $1-(\frac{5}{6})^{\lceil\frac{2d}{5}\rceil}$（ここで d は FK プロトコルでのコードディスタンス）で検証者の望む状態である。残りの $(m-1)$ 個のレジスターについては測定が正しく行われているかを検証する。テストを行う際は Z 基底固有状態を作成する必要があるが、これは検証者自らが行うことができる。証明者にテストと計算が区別できないようにするため、検証者は一様ランダムに Z 基底固有状態を生成し、多数送る。この時量子状態は一様ランダムなので、証明者には計算とテストは区別できない。証明者が正直な場合、証明者は送られてきた状態に FK プロトコル同様 CZ をかけてグラフ状態を生成しようとするが Z 基底固有状態に CZ をかけても量子もつれは生じない。したがって、最終的に生成される状態以外の状態をどのような基底で測定しても最終的に生成される状態は変化することがなく、測定の検証を行うことができる。同様に証明者が正直でない場合、証明者は任意の量子操作を行うが、そのような量子操作はそもそも検証者が検証したいものなので、確率 1 で測定のテストを行うことができる。

上記において検証者が証明者を受理したとき、実際に計算を行っているレジスターについて $1-(1-\delta)^{m-1}$ の確率で正しく状態を測定していることがいえる。一方 FK プロトコル

において、確率 $1-(\frac{5}{6})^{\lceil \frac{2d}{5} \rceil}$ の確率で正しく状態を生成していることがいえる。したがって二つのプロトコルにおいて、検証者が証明者を受理したとき $\left(1-(1-\delta)^{m-1}\right)(1-(\frac{5}{6})^{\lceil \frac{2d}{5} \rceil})$ の確率で、証明者から得られた結果は検証者が行いたい量子計算の確率分布に対して l_1-norm エラー $\frac{\delta}{2}$ の確率分布でサンプルされたものである。

参考文献

[1] T. Vidick and J. Watrous, Quantum Proofs. arxiv:1610.01664
[2] J. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation. Phys. Rev. A. **96**, 012303 (2017).
[3] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States. Phys. Rev. X. **8**, 021060 (2018).
[4] A. Broadbent, How to verify quantum computation. Theory of Computing. **14**:1-37 (2018).
[5] M. Hayashi and T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing. Phys. Rev. Lett. **115**, 220502 (2015).
[6] J. Fitzsimons, M. Hajdušek, and T. Morimae, *Posthoc* Verification of Quantum Computation. Phys. Rev. Lett. **120**, 040501 (2018).
[7] M. J. Bremner, A. Montanaro, and D. J. Shpherd, Average-case complexity versus approximate simulation of commuting quantum computations. Phys. Rev. Lett. **117**, 080501 (2016).
[8] B. M. Terhal and D. P. DiVincenzo, Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games. Quant. Inf. Comput. **4**, 134 (2004).
[9] S. Aaronson and A.Arkhipov, The Computational Complexity of Linear Optics. Proccedings of 43rd Annual ACM Symposium on Theory of Computing (ACM, New York), 333. (2011)
[10] R. Rausendorf and H. J. Briegel, A One-Way Quantum Computer. Phys. Rev. Lett. **86**, 5188 (2001).

付　　録

A.1 Pauli Twirling

以下の付録で用いる Pauli Twirling を導入する。

Pauli Twirling . n-qubit 状態 ρ について以下が成り立つ。

$$\frac{1}{|P_n|}\sum_{Q\in P_n} QPQ\rho QP'Q = \begin{cases} P\rho P & (P=P') \\ 0 & (P\neq P') \end{cases} \quad \text{(A.1)}$$

ここで n-qubit にかかるパウリ行列の集合を P_n とする。また、$Q,P,P' \in P_n$ である。以下特に断りの無い限り、$Q \in P_n$ とする。

A.2 補題 8

以下では定理 4 の証明に必要な補題 8 を導入する。

まず初めに補題 8 に必要な種々の記法を導入する。U_ϵ を ϵ-correct unitary とする。このとき次のようなマップを F_ϵ と定義する。

$$F_\epsilon(\rho) \equiv \mathrm{Tr}_{aux}[U_\epsilon \rho \otimes |0^k\rangle\langle 0^k| U_\epsilon^\dagger]$$

任意のマップはクラウス表示で表される。マップ F_ϵ に対してクラウス表示を以下のように定義する。

$$F_\epsilon(\rho) = \sum_k F_\epsilon^{k\dagger} \rho F_\epsilon^k$$

さらにこのような F_ϵ^k をパウリ行列で以下のように展開する。

$$F_\epsilon^k = \sum_Q \alpha_{k,Q}^\epsilon Q \text{ and } F_\epsilon^{k\dagger} = \sum_Q \alpha_{k,Q}^{\epsilon *} Q$$

ここで $\alpha_{k,Q}^\epsilon$ は完全性 ($\sum_k F_\epsilon^k F_\epsilon^{k\dagger} = I$) により以下を満たしている。

$$\sum_k \sum_Q |\alpha_{k,Q}^\epsilon|^2 = 1$$

ここで、$\sum_Q$ は P_n について和をとるという意味である。このとき $|\alpha_{k,Q}^\epsilon|^2$ と ϵ が次のような関係を持っていることがわかる。

補題 8. $\alpha_{k,Q}^\epsilon$ を F_ϵ^k をパウリ行列で展開した時の係数とする。このとき以下が成り立つ。

$$\sum_k \sum_{|X|+|Y|\geq 1} |\alpha_{k,Q}^\epsilon|^2 = \epsilon \quad \text{(A.2)}$$

ここで $\sum_{|X|+|Y|\geq 1}$ は Q の要素で X,Y が存在している数が 1 つ以上あるような Q について和をとることを表している。

証明

はじめに $P_U(x)$ を計算する。

$$P_U(x) = \frac{1}{2^n}\sum_{a\in\{0,1\}^n} \mathrm{Tr}[(\Pi(x+a)\otimes I^{\otimes k}) U_\epsilon(|a\rangle\langle a| \otimes |0^k\rangle\langle 0^k|) U_\epsilon^\dagger]$$

ここで補助系についてトレースアウトを行う。

$$\begin{aligned}(\text{上式}) &= \frac{1}{2^n}\sum_{a\in\{0,1\}^n}\sum_k \mathrm{Tr}[(X^a|x\rangle\langle x|X^a) F_\epsilon^{k\dagger} X^a |0^n\rangle\langle 0^n| X^a F_\epsilon^k] \\ &= \frac{1}{4^n}\sum_{a,b\in\{0,1\}^n}\sum_k \mathrm{Tr}[(X^aZ^b|x\rangle\langle x|Z^bX^a) \\ &\qquad F_\epsilon^{k\dagger} X^aZ^b|0^n\rangle\langle 0^n|Z^bX^aF_\epsilon^k]\end{aligned}$$

F_ϵ^k をパウリ行列で展開する。

$$\begin{aligned}(\text{上式}) &= \frac{1}{4^n}\sum_{a,b\in\{0,1\}^n}\sum_k\sum_{Q,Q'} \alpha_{k,Q}^\epsilon \alpha_{k,Q'}^{\epsilon *} \mathrm{Tr}[X^aZ^b|x\rangle\langle x|Z^bX^a \\ &\qquad QX^aZ^b|0^n\rangle\langle 0^n|Z^bX^aQ'] \\ &= \frac{1}{4^n}\sum_{a,b\in\{0,1\}^n}\sum_k\sum_{Q,Q'} \alpha_{k,Q}^\epsilon \alpha_{k,Q'}^{\epsilon *} \mathrm{Tr}[|x\rangle\langle x|Z^bX^a \\ &\qquad QX^aZ^b|0^n\rangle\langle 0^n|Z^bX^aQ'X^aZ^b]\end{aligned}$$

ここで a と b について和をとって、Pauli Twirling を使う。

$$\begin{aligned}(\text{上式}) &= \sum_k \sum_Q |\alpha^\epsilon_{k,Q}|^2 \mathrm{Tr}[|x\rangle\langle x|Q|0^n\rangle\langle 0^n|Q] \\ &= \sum_k \sum_Q |\alpha^\epsilon_{k,Q}|^2 |\langle x|Q|0^n\rangle|^2\end{aligned}$$

上式の $|\langle x|Q|0^n\rangle|^2$ が 0 にならないのは、n-bit 列 $x = (x_1, \dots x_n) \in \{0,1\}^n$ について、$x_i = 1$ となる i について Q_i が X あるいは Y であり、$x_j = 0$ となる j について Q_j が I あるいは Z のときである。そのような Q について和の取り方を $\sum_{Q=x}$ と書くとする。上式は以下のように変形される。

$$(\text{上式}) = \sum_k \sum_{Q=x} |\alpha^\epsilon_{k,Q}|^2$$

定義 3 における $P(x)$ は

$$P(x) = \begin{cases} 1 & (x = 0) \\ 0 & (x \neq 0) \end{cases} \tag{A.3}$$

であることに注意して、$P_U(x)$ と $P(x)$ の l_1-norm を計算する。

$$\begin{aligned}\frac{1}{2}\sum_x |P(x) - P_U(x)| &= \frac{1}{2}\sum_x |\delta_{x,0} - \sum_k \sum_{Q=x} |\alpha^\epsilon_{k,Q}|^2| \\ &= \frac{1}{2}|1 - \sum_k \sum_{Q=0} |\alpha^\epsilon_{k,Q}|^2| \\ &\quad + \frac{1}{2}\sum_{x\neq 0} |-\sum_k \sum_{Q=x} |\alpha^\epsilon_{k,Q}|^2| \\ &= \frac{1}{2}|1 - \sum_k \sum_{|I|+|Z|=N} |\alpha^\epsilon_{k,Q}|^2| \\ &\quad + \frac{1}{2}\sum_{x\neq 0} |\sum_k \sum_{Q=x} |\alpha^\epsilon_{k,Q}|^2| \\ &= \frac{1}{2}|1 - \sum_k \sum_{|I|+|Z|=N} |\alpha^\epsilon_{k,Q}|^2| \\ &\quad + \frac{1}{2}|\sum_k \sum_{|X|+|Y|\geq 1} |\alpha^\epsilon_{k,Q}|^2|\end{aligned}$$

ここで $\sum_{|I|+|Z|=N}$ は Q において I と Z の要素数が N 個のもので和をとることを表している。

次のような関係に着目する。

$$\sum_k \Big(\sum_{|I|+|Z|=N} |\alpha^\epsilon_{k,Q}|^2 + \sum_{|X|+|Y|\geq 1} |\alpha^\epsilon_{k,Q}|^2 \Big) = 1$$

そうすると上の式は以下のように変形できる。

$$\frac{1}{2}|1 - \sum_k \sum_{|I|+|Z|=N} |\alpha^\epsilon_{k,Q}|^2| + \frac{1}{2}|\sum_k \sum_{|X|+|Y|\geq 1} |\alpha^\epsilon_{k,Q}|^2| = \sum_k \sum_{|X|+|Y|\geq 1} |\alpha^\epsilon_{k,Q}|^2$$

$\frac{1}{2}\sum_x |P(x) - P_U(x)| = \epsilon$ なので、

$$\sum_k \sum_{|X|+|Y|\geq 1} |\alpha^\epsilon_{k,Q}|^2 = \epsilon$$

が成り立つ。

A.3 定理 4 の証明

以下で定理 4 の証明を行う。補題 8 の証明と同様の計算を行うとよい。初めに $P^c_U(x)$ の計算を行う。

$$\begin{aligned}P^c_U(x) &= \frac{1}{4^n} \sum_{a,b\in\{0,1\}^n} \mathrm{Tr}[(\Pi(x+a) \otimes I^{\otimes k}) U_\epsilon (X^a Z^b |\Psi\rangle\langle\Psi| Z^b X^a \otimes \\ &\qquad |0^k\rangle\langle 0^k|) U^\dagger_\epsilon] \\ &= \frac{1}{4^n} \sum_{a,b\in\{0,1\}^n} \mathrm{Tr}[(|x+a\rangle\langle x+a| \otimes I^{\otimes k}) \\ &\qquad U_\epsilon (X^a Z^b |\Psi\rangle\langle\Psi| Z^b X^a \otimes |0^k\rangle\langle 0^k|) U^\dagger_\epsilon] \\ &= \frac{1}{4^n} \sum_{a,b\in\{0,1\}^n} \mathrm{Tr}[(X^a Z^b |x\rangle\langle x| Z^b X^a \otimes I^{\otimes k}) \\ &\qquad U_\epsilon (X^a Z^b |\Psi\rangle\langle\Psi| Z^b X^a \otimes |0^k\rangle\langle 0^k|) U^\dagger_\epsilon]\end{aligned}$$

ここで部分系についてトレースアウトすると以下のように変形される。

$$\begin{aligned}(\text{上式}) = \frac{1}{4^n} \sum_k \sum_{a,b\in\{0,1\}^n} &\mathrm{Tr}[(X^a Z^b |x\rangle\langle x| Z^b X^a) \\ &F^{k\dagger}_\epsilon X^a Z^b |\Psi\rangle\langle\Psi| Z^b X^a F^k_\epsilon]\end{aligned}$$

ここで F^k_ϵ をパウリ行列で展開すると以下のように変形される。

$$\begin{aligned}(\text{上式}) &= \frac{1}{4^n} \sum_{a,b\in\{0,1\}^n} \sum_k \sum_{Q,Q'} \alpha^\epsilon_{k,Q} \alpha^{\epsilon *}_{k,Q'} \\ &\qquad \mathrm{Tr}[(X^a Z^b |x\rangle\langle x| Z^b X^a Q X^a Z^b |\Psi\rangle\langle\Psi| Z^b X^a Q'] \\ &= \frac{1}{4^n} \sum_{a,b\in\{0,1\}^n} \sum_k \sum_{Q,Q'} \alpha^\epsilon_{k,Q} \alpha^{\epsilon *}_{k,Q'} \\ &\qquad \mathrm{Tr}[(|x\rangle\langle x| Z^b X^a Q X^a Z^b |\Psi\rangle\langle\Psi| Z^b X^a Q' X^a Z^b] \\ &= \sum_k \sum_Q |\alpha^\epsilon_{k,Q}|^2 \mathrm{Tr}[(|x\rangle\langle x|Q|\Psi\rangle\langle\Psi|Q] \\ &= \sum_k \sum_Q |\alpha^\epsilon_{k,Q}|^2 |\langle x|Q|\Psi\rangle|^2 \\ &= \sum_k \Big(\sum_{|I|+|Z|=N} |\alpha^\epsilon_{k,Q}|^2 P^c(x) + \sum_{\delta\neq 0} \sum_{Q=\delta} |\alpha^\epsilon_{k,Q}|^2 P^c(x+\delta) \Big)\end{aligned}$$

$\delta \equiv (\delta_1, \dots \delta_n) \in \{0,1\}^n$ であり、$\sum_{\delta\neq 0}$ は $\delta = 0$ 以外につ

いて和をとることを意味する。

次に $P^c(x)$ と $P^c_U(x)$ の l_1-norm を計算する。

$$\begin{aligned}
&\frac{1}{2}\sum_x |P^c(x) - P^c_U(x)| \\
&= \frac{1}{2}\sum_x \Big| P^c(x) \\
&\quad - \sum_k \Big(\sum_{|I|+|Z|=N} |\alpha^\epsilon_{k,Q}|^2 P^c(x) + \sum_{\delta\neq 0}\sum_{Q=\delta} |\alpha^\epsilon_{k,Q}|^2 P^c(x+\delta) \Big) \Big| \\
&= \frac{1}{2}\sum_x \Big| (1 - \sum_k \sum_{|I|+|Z|=N} |\alpha^\epsilon_{k,Q}|^2) P^c(x) \\
&\quad - \sum_k \sum_{\delta\neq 0}\sum_{Q=\delta} |\alpha^\epsilon_{k,Q}|^2 P^c(x+\delta) \Big| \\
&= \frac{1}{2}\sum_x \Big| \epsilon P^c(x) - \sum_k \sum_{\delta\neq 0}\sum_{Q=\delta} |\alpha^\epsilon_{k,Q}|^2 P^c(x+\delta) \Big|
\end{aligned}$$

ここで三角不等式を使い、x について和をとると以下のように変形できる。

$$\begin{aligned}
(\text{上式}) \leq & \frac{1}{2}\sum_x \Big(\epsilon P^c(x) + \sum_{\delta\neq 0}\sum_k\sum_{Q=\delta} |\alpha^\epsilon_{k,Q}|^2 P^c(x+\delta) \Big) \\
&= \frac{1}{2}\sum_x \epsilon P^c(x) + \sum_{\delta\neq 0}\sum_k\sum_{Q=\delta} |\alpha^\epsilon_{k,Q}|^2 \sum_x P^c(x+\delta) \Big) \\
&= \frac{\epsilon}{2} + \frac{1}{2}\sum_{\delta\neq 0}\sum_k\sum_{Q=\delta} |\alpha^\epsilon_{k,Q}|^2 \\
&= \frac{\epsilon}{2} + \frac{1}{2}\sum_k \sum_{|X|+|Y|\geq 1} |\alpha^\epsilon_{k,Q}|^2 = \epsilon
\end{aligned}$$

A.4 補題 6 の証明

$x = a$ となる確率 $P(x = a)$ は証明者が鍵と同じ値を検証者に送る確率であるので下記のようになる。

$$P(x=a) = \frac{1}{2^n}\sum_{a\in\{0,1\}^n} \mathrm{Tr}[(\Pi(a)\otimes I^k) U_\epsilon (|a\rangle\langle a| \otimes |0^k\rangle\langle 0^k|) U_\epsilon^\dagger]$$

部分系についてトレースアウトを行うと以下のように変形できる。

$$\begin{aligned}
(\text{上式}) &= \frac{1}{2^n}\sum_{a\in\{0,1\}^n}\sum_k \mathrm{Tr}[\Pi(a) F^{k\dagger}_\epsilon |a\rangle\langle a| F^k_\epsilon] \\
&= \frac{1}{4^n}\sum_{a,b\in\{0,1\}^n}\sum_k \mathrm{Tr}[X^a Z^b |0^n\rangle\langle 0^n| Z^b X^a F^{k\dagger}_\epsilon X^a Z^b |0^n\rangle\langle 0^n| Z^b X^a F^k_\epsilon] \\
&= \frac{1}{4^n}\sum_{a,b\in\{0,1\}^n}\sum_k\sum_{Q,Q'} \alpha^{\epsilon *}_{k,Q'} \alpha^\epsilon_{k,Q} \\
&\qquad \mathrm{Tr}[X^a Z^b |0^n\rangle\langle 0^n| Z^b X^a Q X^a Z^b |0^n\rangle\langle 0^n| Z^b X^a Q'] \\
&= \sum_k\sum_Q |\alpha^\epsilon_{k,Q}|^2 |\langle 0^n|Q|0^n\rangle|^2 \\
&= \sum_k \sum_{|I|+|Z|=N} |\alpha^\epsilon_{k,Q}|^2 = 1 - \epsilon
\end{aligned}$$