高接続性ハイパーグラフ状態の検証 と その量子計算への応用

竹内勇貴¹, 森前智行^{2,3}

¹NTT コミュニケーション科学基礎研究所 ²京都大学 基礎物理学研究所 ³JST, PRESTO

Phys. Rev. X 8, 021060 (2018).

目次

- 2. ハイパーグラフ状態
- 3. 適応的スタビライザーテスト
- 4. ハイパーグラフ状態の検証
- 5. 応用
- ▶ IQP回路を用いた量子スプレマシーの実証





1. イントロダクション

(i)指数時間かかっても良い



(ii)検証者は何でも出来る





検証プロトコルに要求したい条件

✓ 量子状態のサイズに対して多項式時間で動作する
 ✓ 検証者が必要な操作はsingle-qubit operationのみ
 ✓ サンプルの分布(i.i.d.など)を仮定しない

検証プロトコルに要求したい条件

✓ 量子状態のサイズに対して多項式時間で動作する
 ✓ 検証者が必要な操作はsingle-qubit operationのみ
 ✓ サンプルの分布(i.i.d.など)を仮定しない



どんな状態なら検証出来るのか?

- グラフ状態[Hayashi-Morimae '15, Markham et al. '18]
- 低接続性ハイパーグラフ状態^{[Morimae-Takeuchi-Hayashi}

検証プロトコルに要求したい条件

✓ 量子状態のサイズに対して多項式時間で動作する
 ✓ 検証者が必要な操作はsingle-qubit operationのみ
 ✓ サンプルの分布(i.i.d.など)を仮定しない



どんな状態なら検証出来るのか?

- グラフ状態[Hayashi-Morimae '15, Markham et al. '18]
- 低接続性ハイパーグラフ状態^{[Morimae-Takeuchi-Hayashi}
- 高接続性ハイパーグラフ状態[Takeuchi-Morimae '17]

検証プロトコルに要求したい条件

✓ 量子状態のサイズに対して多項式時間で動作する
 ✓ 検証者が必要な操作はsingle-qubit operationのみ
 ✓ サンプルの分布(i.i.d.など)を仮定しない



どんな状態なら検証出来るのか?

- グラフ状態[Hayashi-Morimae '15, Markham et al. '18]
- 低接続性ハイパーグラフ状態^{[Morimae-Takeuchi-Hayashi}
- 高接続性ハイパーグラフ状態[Takeuchi-Morimae '17]

多項式時間で生成出来る任意のハイパーグラフ状態

検証プロトコルに要求したい条件

✓ 量子状態のサイズに対して多項式時間で動作する
 ✓ 検証者が必要な操作はsingle-qubit operationのみ
 ✓ サンプルの分布(i.i.d.など)を仮定しない



どんな状態なら検証出来るのか?

- グラフ状態[Hayashi-Morimae '15, Markham et al. '16]
- 低接続性ハイパーグラフ状態^{[Morimae-Takeuchi-Hayashi}
- 高接続性ハイパーグラフ状態[Takeuchi-Morimae '17]
- ・一部のハミルトニアンの基底状態["]
- ・一部の量子回路の出力状態["]











N = 5





2. ハイパーグラフ状態
接続性:
$$\xi \equiv \max_{v \in V} \xi_v$$

頂点 v に作用しているgeneralized CZの数
 $k = \text{const.}$
 $\xi = \text{const.}$
 $\xi = \text{poly}(N)$
 $k = 5$

今まで
 $\xi = \text{const.}$
 $|E| \leq \text{poly}(N)$
 $|E|: \wedge \eta^{n-xy^{y}} \text{ogs}$





・ 量子状態 ρ における g_i に対しての適応的スタビライザーテスト

$$g_{i} = \sum_{\mathbf{a} \in \{0,1\}^{|\tilde{W}_{P}^{(i)}|}} (-1)^{\alpha^{(i,\mathbf{a})}} X_{v_{i}} \left(\prod_{v_{i'} \in \tilde{W}_{Z}^{(i,\mathbf{a})}} Z_{v_{i'}} \right) \left(\prod_{v_{i'} \in \tilde{W}_{P}^{(i)}} |a_{v_{i'}}\rangle \langle a_{v_{i'}}|_{v_{i'}} \right)$$

1. v_i に対応するqubitをX基底で測定し、 他の全てのqubitをZ基底で測定する。

・ 量子状態 ρ における g_i に対しての適応的スタビライザーテスト

$$g_{i} = \sum_{\mathbf{a} \in \{0,1\}^{|\tilde{W}_{P}^{(i)}|}} (-1)^{\alpha^{(i,\mathbf{a})}} X_{v_{i}} \left(\prod_{v_{i'} \in \tilde{W}_{Z}^{(i,\mathbf{a})}} Z_{v_{i'}}\right) \left(\prod_{v_{i'} \in \tilde{W}_{P}^{(i)}} |a_{v_{i'}}\rangle \langle a_{v_{i'}}|_{v_{i'}}\right)$$

- 1. v_i に対応するqubitをX基底で測定し、 他の全てのqubitをZ基底で測定する。
- 2. $ilde{W}_P^{(i)}$ を求める。 $ilde{W}_P^{(i)}$ と測定結果 $z_{i'}$ $(i' \neq i)$ より、 $lpha^{(i,\mathbf{a})}$ と $ilde{W}_Z^{(i,\mathbf{a})}$ も求まる。

・ 量子状態 ρ における g_i に対しての適応的スタビライザーテスト

$$g_{i} = \sum_{\mathbf{a} \in \{0,1\}^{|\tilde{W}_{P}^{(i)}|}} (-1)^{\alpha^{(i,\mathbf{a})}} X_{v_{i}} \left(\prod_{v_{i'} \in \tilde{W}_{Z}^{(i,\mathbf{a})}} Z_{v_{i'}}\right) \left(\prod_{v_{i'} \in \tilde{W}_{P}^{(i)}} |a_{v_{i'}}\rangle \langle a_{v_{i'}}|_{v_{i'}}\right)$$

- 1. v_i に対応するqubitをX基底で測定し、 他の全てのqubitをZ基底で測定する。
- 2. $ilde{W}_P^{(i)}$ を求める。 $ilde{W}_P^{(i)}$ と測定結果 $z_{i'}$ $(i' \neq i)$ より、 $lpha^{(i,\mathbf{a})}$ と $ilde{W}_Z^{(i,\mathbf{a})}$ も求まる。
- 3. 以下を満たしていればテストにパス。

・ 量子状態 ρ における g_i に対しての適応的スタビライザーテスト

$$g_{i} = \sum_{\mathbf{a} \in \{0,1\}^{|\tilde{W}_{P}^{(i)}|}} (-1)^{\alpha^{(i,\mathbf{a})}} X_{v_{i}} \left(\prod_{v_{i'} \in \tilde{W}_{Z}^{(i,\mathbf{a})}} Z_{v_{i'}}\right) \left(\prod_{v_{i'} \in \tilde{W}_{P}^{(i)}} |a_{v_{i'}}\rangle \langle a_{v_{i'}}|_{v_{i'}}\right)$$

- 1. v_i に対応するqubitをX基底で測定し、 他の全てのqubitをZ基底で測定する。
- 2. $ilde{W}_P^{(i)}$ を求める。 $ilde{W}_P^{(i)}$ と測定結果 $z_{i'}$ $(i' \neq i)$ より、 $lpha^{(i,\mathbf{a})}$ と $ilde{W}_Z^{(i,\mathbf{a})}$ も求まる。
- 3. 以下を満たしていればテストにパス。

以降、 ρ_B は(Nk + m + 1)個のレジスタで構成されているとする。

以降、 ρ_B は(Nk + m + 1)個のレジスタで構成されているとする。

2. Aliceはm個のレジスタを一様randomに選び、捨てる。

量子de Finetti定理[Li et al. '15]

残りの(Nk+1)個のレジスタはi.i.d.に近い分布となる。

(ただし、どういう量子状態のテンソル積になっているかは分からない。)

$$\frac{K_i}{k} \ge 1 - \epsilon$$

を満たせば、AliceはBobを受理する。

$$\frac{K_i}{k} \ge 1 - \epsilon$$

を満たせば、AliceはBobを受理する。

Soundness: AliceがBobを受理したならば、targetレジスタの状態は、 $1 - k^{-1/7}$ 以上の確率で $\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - k^{-1/7}$ を満たす。ただし、 $\epsilon = \frac{1}{4Nk^{2/7}}, m \geq 2N^3 k^{18/7} \log 2, k \geq (4N)^7$

$$\frac{K_i}{k} \ge 1 - \epsilon$$

を満たせば、AliceはBobを受理する。

4. Aliceは残っているレジスタ(targetレジスタ)を使って、 行いたい量子情報処理を行う。

$$\frac{K_i}{k} \ge 1 - \epsilon$$

を満たせば、AliceはBobを受理する。

4. Aliceは残っているレジスタ(targetレジスタ)を使って、 行いたい量子情報処理を行う。

5. 応用

5. 応用

5. 応用

5. 応用

5. 応用

5. 応用

5. 応用

▶ IQP回路を用いた量子スプレマシーの実証

IQP (Instantaneous Quantum Polynomial time)回路[Shepherd et al. '09]

定理: D i Z, CZ, CCZのみで構成されたIQP回路に対して

[Bremner-Montanaro -Shepherd '16]

$$\sum_{\mathbf{z}} |p_{\mathbf{z}} - q_{\mathbf{z}}| \le \frac{1}{192}$$

IQP回路の出力確率

を満たす{*q*_z}_zを古典シミュレータが多項式時間でsample 出来たら多項式階層が第3レベルで崩壊。 (あるconjectureを満たせば)

理想的な(高接続性)ハイパーグラフ状態を生成出来れば、 量子スプレマシーを実証出来る

定理: DがZ, CZ, CCZのみで構成されたIQP回路に対して

[Bremner-Montanaro -Shepherd '16]

IQP回路の出力確率

を満たす $\{q_z\}_z$ を古典シミュレータが多項式時間でsample 出来たら多項式階層が第3レベルで崩壊。 (baconjectureを満たせば) _{実際には}、

- フィデリティ1で作るのは困難...

| <mark>理想的な</mark>(高接続性)ハイパーグラフ状態を生成出来れば、 | 量子スプレマシーを実証出来る

5. 応用

Soundness:
$$\langle G | \rho_{tgt} | G \rangle \ge 1 - k^{-1/7}$$

 $\sum_{\mathbf{x}} |\operatorname{Tr} [M_{\mathbf{x}} \rho_{tgt}] - \langle G | M_{\mathbf{x}} | G \rangle| \le \frac{1}{\operatorname{poly}(k)}$
もし、 $\rho_{tgt} \varepsilon X$ 測定して得られる出力確率分布 $\{p'_{\mathbf{z}}\}_{\mathbf{z}}$ に対して
 $\sum_{\mathbf{z}} |p'_{\mathbf{z}} - q_{\mathbf{z}}| \le \frac{1}{193}$
を満たす古典シミュレータがあれば、多項式階層が崩壊。
検証プロトコルをpassした状態で十分!!