スタビライザー状態の数理とマトロイド理論

量子力学100周年研究会：量子基礎・量子情報のこれまでとこれから

2025年9月12日

森 立平
名古屋大学

量子論と離散性

スタビライザー状態は理論的にも工学的にも重要な量子状態のクラスで

- 測定型量子計算
- 量子誤り訂正符号

などに用いられる。

スタビライザー状態は量子論の状態集合が内包する離散構造と言える。

この発表で伝えたいことは

- スタビライザー状態という**量子論が持っている離散構造**の数理
- 離散数学、計算機科学の分野で発展してきた**マトロイド理論**との関係

パウリ行列

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

単位行列 I 以外は定義を覚える必要はない。**以下の関係**だけ知っていればよい。

- $X^2 = Y^2 = Z^2 = I.$
- $XY = -YX, \quad YZ = -ZY, \quad ZX = -XZ.$
- $XY = iZ, \quad YZ = iX, \quad ZX = iY.$

ベル状態

$$|\Phi\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

はパウリ行列のテンソル積の共通の固有値1の固有ベクトルとして表される。

$$X \otimes X \, |\Phi\rangle = |\Phi\rangle$$
$$Z \otimes Z \, |\Phi\rangle = |\Phi\rangle \, .$$

パウリ群

$$\mathcal{P}_1 \coloneqq \{\{\pm 1, \pm i\}P \mid P \in \{I, X, Y, Z\}\}$$

$$\mathcal{P}_n \coloneqq \left\{ \{\pm 1, \pm i\} \bigotimes_{k=1}^{n} P_k \mid P_k \in \{I, X, Y, Z\} \quad \forall k \in \{1, \ldots, k\} \right\}.$$

任意の $A,\ B \in \mathcal{P}_n$ について

$$AB = BA \qquad \text{or} \qquad AB = -BA$$

Example 1 **(パウリ群の交換関係)**.

$$\begin{aligned}(X \otimes X \otimes Y \otimes Z)\,(X \otimes Y \otimes I \otimes X) &= (XX) \otimes (XY) \otimes (YI) \otimes (ZX) \\ &= (XX) \otimes (-YX) \otimes (IY) \otimes (-XZ) \\ &= (X \otimes Y \otimes I \otimes X)\,(X \otimes X \otimes Y \otimes Z)\end{aligned}$$

反交換な系の数が**偶数個**(奇数個)だと**交換**(反交換)となる。

スタビライザー群と符号空間

Definition 2 (スタビライザー群).

パウリ群 $\mathcal{P}_n$ の部分群 $\mathcal{S}$ が以下の条件を満たすものを **スタビライザー群** という。

1. $-I \notin \mathcal{S}$.
2. 任意の $A, B \in \mathcal{S}$ について、$AB = BA$.

さらにスタビライザー群 $\mathcal{S}$ について

$$V_{\mathcal{S}} := \left\{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \mid A|\psi\rangle = |\psi\rangle \quad \forall A \in \mathcal{S} \right\}$$

を $\mathcal{S}$ の **スタビライザー符号空間** という。

Example 3 (スタビライザー群).

$$\mathcal{S} := \{ I \otimes I,\ X \otimes X,\ Z \otimes Z,\ -Y \otimes Y \}$$

とすると、$V_{\mathcal{S}} = \mathrm{span}_{\mathbb{C}}(|\Phi\rangle)$.

スタビライザー群の生成元

n-qubit のスタビライザー群 $\mathcal{S} = \langle S_1, \ldots, S_m \rangle$ を考える。

ここで $S_1, \ldots, S_m$ は**独立**であるとする。つまり、$T \subseteq \{1, \ldots, m\}$ について、

$$\prod_{k \in T} S_k = I \iff T = \varnothing$$

とする。このとき、$V_{\mathcal{S}}$ への射影行列は $\prod_{k=1}^{m} \frac{I+S_k}{2}$ と書けるので。

$$\begin{aligned}
\dim\left(V_{\mathcal{S}}\right) &= \mathsf{Tr}\left(\prod_{k=1}^{m} \frac{I + S_k}{2}\right) \\
&= \frac{1}{2^m} \sum_{T \subseteq \{1,\ldots,m\}} \mathsf{Tr}\left(\prod_{k \in T} S_k\right) \\
&= 2^{n-m}
\end{aligned}$$

である。よって $m = n$ のとき、$V_{\mathcal{S}}$ は一次元となる。

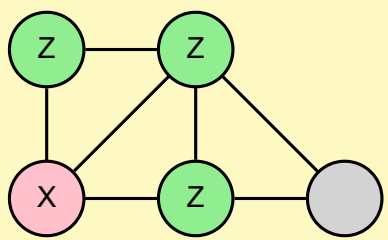
グラフ状態

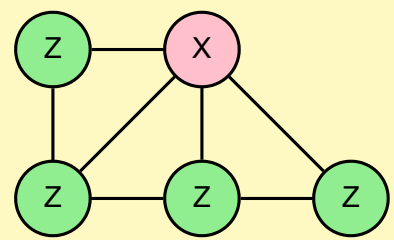
Definition 4 (グラフ状態 (⊆スタビライザー状態)).

グラフ $G = (V, E)$ について、$|V|$ 量子ビットのパウリ行列

$$S_v := X_v \otimes \bigotimes_{w \in N(v)} Z_w \qquad \forall v \in V.$$

はスタビライザー群の生成元となる。ここで $N(v)$ は v の近傍。これで定義されるスタビライザー状態を**グラフ状態**という。





マトロイド (matroid; 線形独立性を抽象化したもの)

Definition 5 (マトロイド [Whitney 1935], [Nakasawa 1935]).

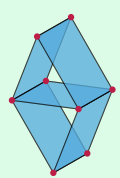
空でない有限集合 E と $\mathcal{I} \subseteq 2^E$ が以下を満たすとき $(E, \mathcal{I})$ を**独立性システム**という。

1. $\varnothing \in \mathcal{I}$.
2. $\forall B \subseteq A \subseteq E, \quad A \in \mathcal{I} \implies B \in \mathcal{I}$.

さらに $(E, \mathcal{I})$ が以下の条件を満たすとき **マトロイド** という。

3. $\forall A, B \in \mathcal{I}, \quad |A| > |B| \implies \exists a \in A \setminus B \quad \text{s.t.} \quad B \cup \{a\} \in \mathcal{I}$.

Example 6 (マトロイドの例).

- 線形マトロイド: E：ベクトルの集合, $\mathcal{I}$：線形独立なベクトルの集合。
- 一様マトロイド U_n^r: E：要素数 n の集合, $\mathcal{I}$：要素数 r 以下の部分集合。
- Vámos マトロイド: E：  の頂点(要素数 8), $\mathcal{I}$：の面を含まない頂点集合。

量子論とマトロイド理論

年	量子論 (量子情報)	マトロイド理論
1925	ハイゼンベルク行列力学 [1925] シュレディンガー波動方程式 [1926]	
1935	EPR パラドックス [Einstein, Podolsky, Rosen]	**マトロイドの定義** [Whitney], ([van der Waerden],) [Nakasawa]
1940–60's	ベルの不等式 [Bell], [Clauser, Horne, Shimony, Holt] 量子推定 [Helstrom]	独立横断定理 [Rado] 正則マトロイドとグラフィックマトロイドの禁止マイナー, Tutte 多項式 [Tutte], マトロイド分割 [Edmonds, Fulkerson]
1970's	量子通信路の数理 [Kraus], [Jamiołkowski], [Choi] 量子情報理論 [Holevo]	マトロイド交叉 [Edmonds], Rota予想 [Rota] 線形マトロイドパリティ [Lawler], [Lovász]
1980's	量子コンピュータの提案 [Feynman], [Deutch] 量子暗号 [Bennet, Brassard]	正則マトロイドの構造定理 [Seymour], **等方的システム** [Bouchet] 劣モジュラ関数最小化 [Grötschel, Lovász, and Schrijver]
1990's —	素因数分解アルゴリズム [Shor] **スタビライザー符号** [Shor], [Gottesman] **グラフ状態** [Raussendorf, Briegel], [Hein, Eisert, Briegel], [Van den Nest, Dehaene, De Moor]	マトロイドマイナープロジェクト [Geelen et al.] 劣モジュラ関数最小化強多項式時間 [Schrijver], [Iwata, Fleischer, Fujishige]

計算機科学、数学におけるマトロイド関連の受賞

年	受賞	受賞者
1979	Fulkerson Prize	Paul Saymour
1985	John von Neumann Theory Prize	Jack Edmonds
1991	Fulkerson Prize	Nikolai Mnëv
2003	Fulkerson Prize	Jim F. Geelen, Albertus M. H. Gerards, and Ajai Kapoor
2003	Fulkerson Prize	Satoru Iwata, Lisa Fleischer, Satoru Fujishige, and Alexander Schrijver
2017	STOC Best Paper Award	Satoru Iwata and Yusuke Kobayashi
2019	STOC Best Paper Award	Nima Anari, Kuikui Liu, Shayan Oveis Gharan, and Cynthia Vinzant

バイナリマトロイド

Definition 7 (バイナリマトロイド).

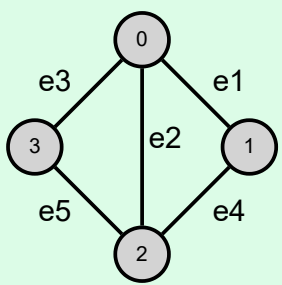
マトロイド $M = (E, \mathcal{I})$ は **バイナイマトロイド** $\overset{\text{def}}{\iff}$ ある $B \in \mathbb{F}_2^{k \times |E|}$ が存在して、

$$\mathcal{I} := \{S \subseteq E \mid B \text{ の } S \text{ に対応する列が線形独立}\}.$$

Example 8 (グラフィックマトロイド).

グラフ $G = (V, E)$ について、**グラフィックマトロイド** $M(G) = (E, \mathcal{I})$ は以下で定義される。

$$\mathcal{I} := \{S \subseteq E \mid S \text{ がサイクルを含まない}\}.$$



$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$ (表現行列)

双対マトロイド

Definition 9 (双対マトロイド).

バイナリマトロイド M が表現行列 $B \in \mathbb{F}_2^{k\times n}$ を持つとする。このとき、B の行と直交する線形空間の基底を行として持つ行列 $B^\perp \in \mathbb{F}_2^{(n-k)\times n}$ で表わされるバイナリマトロイドを M の**双対マトロイド**という。

Example 10 (双対マトロイド).

$$B_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

のとき、

$$B_1^\perp = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}, \quad B_2^\perp = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B_3^\perp = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

と取れる。

等方的システム (Isotropic systems)

Definition 11 (等方的システム [Bouchet 1987]).

独立性システム $S = (\{1, \ldots, n\}, \mathcal{I})$ は**バイナリ2-拡張可能システム** $\overset{\text{def}}{\iff}$ ある行列 $M \in \mathbb{F}_2^{k \times 2n}$ が存在して、要素 $v \in \{1, \ldots, n\}$ について、M の v 列目と $n + v$ 列目が対応していると考えたとき、

$$\mathcal{I} = \{W \subseteq \{1, \ldots, n\} \mid W \text{ に対応する } M \text{ の } 2|W| \text{ 列が線形独立}\}.$$

バイナリ2-拡張可能システム は **等方的独立性システム** $\overset{\text{def}}{\iff}$ ある行列 $M \in \mathbb{F}_2^{n \times 2n}$ が存在して、M のランクは n であり

$$M \begin{bmatrix} O_n & I_n \\ I_n & O_n \end{bmatrix} M^T = O_n.$$

を満たし、バイナリ2-拡張可能システムを表す。

(余談) Bouchet は等方的システムを独立性システムとしては見ていない(バイナリマトロイドさえ！)

等方的システムの例

Lemma 12 (バイナリマトロイドを用いた等方的システムの構成).

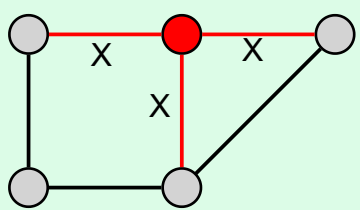
バイナリマトロイドの(冗長性のない)表現行列 $B \in \mathbb{F}_2^{k\times n}$ とその双対マトロイドの表現行列 $B^\perp \in \mathbb{F}_2^{(n-k)\times n}$ について

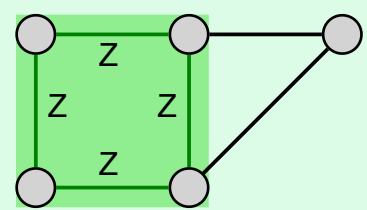
$$\left[\begin{array}{c|c} B & O_{k\times n} \\ O_{(n-k)\times n} & B^\perp \end{array}\right]$$

は等方的システムになる。

Example 13 (平面マトロイド (⊆ グラフィックマトロイド ⊆ バイナリマトロイド)を用いた構成).

平面符号状態 (planar code state) [Bravyi and Raussendorf 2007]: 平面グラフの辺が量子ビットに対応。各頂点に対応するスタビライザーは頂点に接続する辺に X を持つ。各面に対応するスタビライザーは面をを構成する辺に Z を持つ。





基本グラフ

M の**行に可逆な線形操作**をしても列の線形独立性には影響しない。

M の v **列目と**$(n+v)$ **列目に可逆な線形操作** をしても2列ずつ選んだ場合の線形独立性には影響しない。

Theorem 14 (基本グラフ [Bouchet 1988]).

等方的システムの表現行列は行基本変形と2列の基本変形により、

$$M = \begin{bmatrix} I & | & A \end{bmatrix}$$

の形にできる。ここで $A \in \mathbb{F}_2^{n\times n}$ は対角成分が 0 の対称行列。

この A を隣接行列として持つグラフを等方的システムの **基本グラフ** という(一意ではない)。

Theorem 15 (上記と等価な定理 [Van den Nest, Dehaene, De Moor 2004]).

任意のスタビライザー状態は **局所クリフォード変換** でグラフ状態に変換できる。

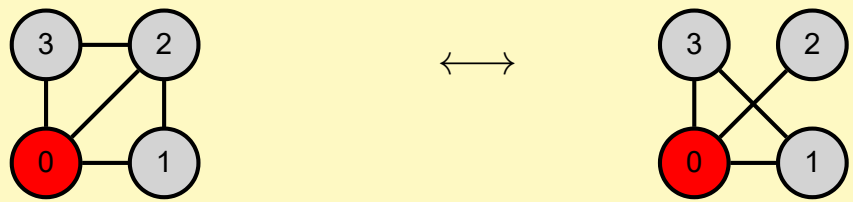
二部グラフはバイナリマトロイドから構成した等方的システムの基本グラフとみなせる。

局所反転

Definition 16 (局所反転 [Kotzig 1968]).

グラフ $G = (V, E)$ と頂点 $v \in V$ について、局所反転 $G * v = (V, E')$ は以下で定義される。

$$E' := E \triangle \{\{s, t\} \subseteq V \mid s \in N(v) \wedge t \in N(v) \wedge s \neq t\}$$



Theorem 17 (局所反転 [Bouchet 1988], [Van den Nest, Dehaene, De Moor 2004]).

グラフ G と H が同じ等方的システムの基本グラフ $\iff$ G と H が**局所反転等価**。

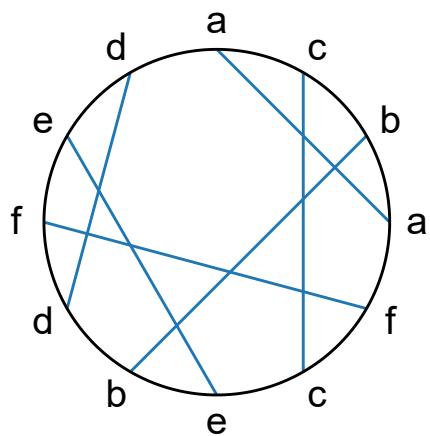
言い換えると、

グラフ状態 $|G\rangle$ と $|H\rangle$ が局所クリフォード等価 $\iff$ G と H が**局所反転等価**。

グラフィック等方的システムと円グラフ [Bouchet 1987]

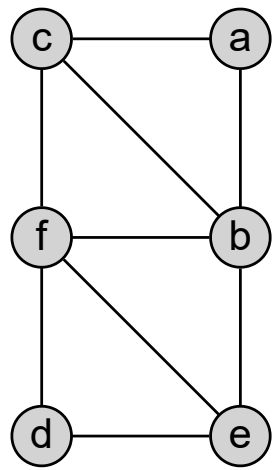
Double ocurrance word

a c b a f c e b d f e d



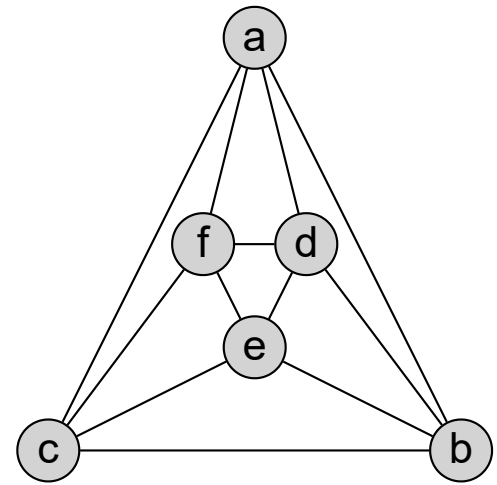
コードダイアグラム

コードで定義される区間の反転



円グラフ (circle graph)

局所反転



連結4正則グラフ(単純とは限らない)
上のオイラー閉路

オイラー閉路のKotzig変換 [Kotzig 1968]

マイナー理論

Definition 18 (頂点マイナー [Bouchet 1987], [Oum 2005]).

グラフ G について、頂点削除と局所反転で得られるグラフ H を G の**頂点マイナー**という。

グラフ状態 $|G\rangle$ と $|H\rangle$ について、

$|G\rangle$ に対する**局所クリフォード演算とパウリ測定**でグラフ状態 $|H\rangle$ が得られる $\iff$ H は G の頂点マイナー.

頂点マイナーはグラフマイナー、マトロイドマイナーと類似の概念である。**グラフマイナー理論で得られた豊富な結果の類似**が頂点マイナーでも成り立つと予想されており、その一部は証明されている [Oum et al.], [Geelen et al.]。

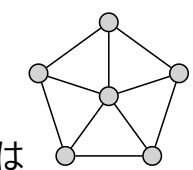
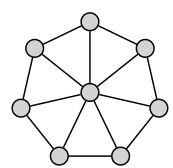
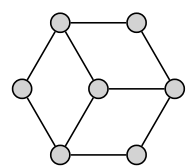
グラフマイナー	頂点マイナー
ブランチ幅	ランク幅
平面グラフ	円グラフ

頂点マイナー理論の結果は自然とスタビライザー状態の言葉に翻訳できる。

グラフマイナー理論の類似としての頂点マイナー理論

- 二つのグラフが局所反転等価であるかどうか $O(n^4)$ 時間判定アルゴリズム [Bouchet 1991].

グラフマイナー理論で得られた豊富な結果の類似が頂点マイナーでも成り立つと予想されており、その一部は証明されている。

- **頂点マイナー**に閉じたグラフクラスでランク幅有界のものは**有限個の禁止頂点マイナー**で特徴付けられる [Oum 2008].
- 固定したグラフ H と与えられたグラフ G (ランク幅が定数)について、G が H と同型なグラフを**頂点マイナー**として含むか $O(n^3)$ 時間判定アルゴリズム [Courcelle, Oum 2007].
- 与えられたグラフ G, H について、G が H を**頂点マイナー**として含むかどうかの判定はNP困難 [Dahlberg, Helsen, Wehner 2020].
- 任意の**円グラフ** H についてある r が存在し、**ランク幅**が r 以上の任意のグラフは H と同型なグラフを**頂点マイナー**として含む [Geelen, Kwon, McCarty, Wollan 2023].
- **円グラフ**の**禁止頂点マイナー**は  ,  ,  [Bouchet 1994].

まとめ

- 量子論の中には**豊かな離散構造**があり**マトロイド理論**と関係が深い。
- スタビライザー状態は**パウリ群のアーベル部分群で $-I$ を含まないもの**で定義される。
- スタビライザー状態は(スタビライザーの符号を無視すると) **$\mathbb{F}_2$ 上の $n \times 2n$ 行列**で表される。
- **等方的システム** [Bouchet 1987] はスタビライザー状態(スタビライザーの符号を無視したもの)と数理的に等価なものである。
- **バイナリマトロイドとその双対**から等方的システムが定義できる。
- 一方で**4正則グラフ**から等方的システムを定義することもできる。

その他の話題

- 等方的システムはある種の **$\mathbb{F}_4$ 上の自己双対加法的符号** と等価である。
- 部分系が2次元でない場合も、同様の議論ができる。ただし、**次元が素数冪でない場合は有限体上のシンプレクティック空間の理論に持ち込めない**。
- グラフマイナー、マトロイドマイナー理論と同様に等方的システムについて**頂点マイナー理論**が展開される。
- グラフ、マトロイドのブランチ幅と同様に等方的システムについては**ランク幅**という量が定義される。
- 一般確率論(例えばジョルダン代数から定まるもの)で**類似の離散構造は存在するのか？**