Clifford group from scratch

Maris Ozols

University of Waterloo

July 28, 2008

Outline

Motivation

- Everybody knows what the Clifford group is

Motivation

- Everybody knows what the Clifford group is, only Maris doesn't know...

Motivation

- Everybody knows what the Clifford group is, only Maris doesn't know...
- I'm obsessed with symmetric structures in the Hilbert space

Motivation

- Everybody knows what the Clifford group is, only Maris doesn't know...
- I'm obsessed with symmetric structures in the Hilbert space
- Clifford group has lots of applications

Motivation

- Everybody knows what the Clifford group is, only Maris doesn't know. . .
- I'm obsessed with symmetric structures in the Hilbert space
- Clifford group has lots of applications
- I know the results, but I haven't seen the proofs

Motivation

- Everybody knows what the Clifford group is,
  only Maris doesn't know...
- I'm obsessed with symmetric structures in the Hilbert space
- Clifford group has lots of applications
- I know the results, but I haven't seen the proofs
- Some folklore results with no proofs available

Pauli matrices

Single qubit

The set of *Pauli matrices* is $P = \{I, X, Y, Z\}$, where

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

Pauli matrices

Single qubit

The set of *Pauli matrices* is $P = \{I, X, Y, Z\}$, where

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

For n qubits

$$P_n = \{\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \,|\, \sigma_i \in P\}.$$

Pauli matrices

Single qubit

The set of *Pauli matrices* is $P = \{I, X, Y, Z\}$, where

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

For n qubits

$$P_n = \{\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \,|\, \sigma_i \in P\}.$$

Vector space structure

The group $P_n/U(1)$ is isomorphic to a vector space over $\mathbb{F}_2$ with dimension $2n$ via identification

$$\begin{array}{ccc} Z & — & Y \\ | & & | \\ I & — & X \end{array} \quad \Longleftrightarrow \quad \begin{array}{ccc} (0,1) & — & (1,1) \\ | & & | \\ (0,0) & — & (1,0) \end{array}$$

multiply add

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1.

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in P_n^* have eigenvalues ± 1 with equal multiplicity.

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$,

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$,

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$, e.g., $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$, e.g., $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

You cannot

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$, e.g., $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

You cannot

- $X \mapsto I$,

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$, e.g., $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

You cannot

- $X \mapsto I$,
- $X \mapsto iX$.

Clifford group

Definition (sloppy)

Unitaries that take Paulis to Paulis via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$, e.g., $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

You cannot

- $X \mapsto I$,
- $X \mapsto iX$.

Clifford group

Definition (sloppy)

Unitaries that take $\pm P_n^*$ to $\pm P_n^*$ via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$, e.g., $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

You cannot

- $X \mapsto I$,
- $X \mapsto iX$.

Clifford group

Definition (sloppy)

Unitaries that take $\pm P_n^*$ to $\pm P_n^*$ via conjugation.

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$, e.g., $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

You cannot

- $X \mapsto I$,
- $X \mapsto iX$.

Global phase

U and $e^{i\varphi}U$ act identically, i.e., $UMU^\dagger = (e^{i\varphi}U)M(e^{i\varphi}U)^\dagger$.

Clifford group

Definition

The *Clifford group* $\mathcal{C}_n$ on n qubits is

$$\mathcal{C}_n = \left\{ U \in U(2^n) \,|\, \sigma \in \pm P_n^* \Rightarrow U\sigma U^\dagger \in \pm P_n^* \right\} / U(1).$$

Eigenvalues

The eigenvalues of X, Y, Z are ± 1. Let $P_n^* = P_n \setminus \{I^{\otimes n}\}$.
All matrices in $\pm P_n^*$ have eigenvalues ± 1 with equal multiplicity.

You can

- $X \mapsto -X$, e.g., $ZXZ = -X$,
- $X \otimes I \mapsto X \otimes X$, e.g., $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

You cannot

- $X \mapsto I$,
- $X \mapsto iX$.

Global phase

U and $e^{i\varphi}U$ act identically, i.e., $UMU^\dagger = (e^{i\varphi}U)M(e^{i\varphi}U)^\dagger$.

Clifford group $\mathcal{C}_1$

Single qubit

$\pm P_1^* = \{\pm X, \pm Y, \pm Z\}.$

Clifford group $\mathcal{C}_1$

Single qubit

$\pm P_1^* = \{\pm X, \pm Y, \pm Z\}$.

Restrictions

Conjugation must preserve the structure of Pauli matrices.

Clifford group $\mathcal{C}_1$

Single qubit

$\pm P_1^* = \{\pm X, \pm Y, \pm Z\}$.

Restrictions

Conjugation must preserve the structure of Pauli matrices.

- $Y = iXZ$, thus $UYU^\dagger = i(UXU^\dagger)(UZU^\dagger)$,

Clifford group $\mathcal{C}_1$

Single qubit

$\pm P_1^* = \{\pm X, \pm Y, \pm Z\}$.

Restrictions

Conjugation must preserve the structure of Pauli matrices.

- $Y = iXZ$, thus $UYU^\dagger = i(UXU^\dagger)(UZU^\dagger)$,
- $U(-X)U^\dagger = -UXU^\dagger$ and similarly for Z.

Clifford group $\mathcal{C}_1$

Single qubit

$\pm P_1^* = \{\pm X, \pm Y, \pm Z\}$.

Restrictions

Conjugation must preserve the structure of Pauli matrices.

- $Y = iXZ$, thus $UYU^\dagger = i(UXU^\dagger)(UZU^\dagger)$,
- $U(-X)U^\dagger = -UXU^\dagger$ and similarly for Z.

Thus it is enough to specify where X and Z go.

Clifford group $\mathcal{C}_1$

Single qubit

$\pm P_1^* = \{\pm X, \pm Y, \pm Z\}$.

Restrictions

Conjugation must preserve the structure of Pauli matrices.

- $Y = iXZ$, thus $UYU^\dagger = i(UXU^\dagger)(UZU^\dagger)$,
- $U(-X)U^\dagger = -UXU^\dagger$ and similarly for Z.

Thus it is enough to specify where X and Z go. However, since X and Z anti-commute, so must $UXU^\dagger$ and $UZU^\dagger$.

Clifford group $\mathcal{C}_1$

Single qubit

$\pm P_1^* = \{\pm X, \pm Y, \pm Z\}$.

Restrictions

Conjugation must preserve the structure of Pauli matrices.

- $Y = iXZ$, thus $UYU^\dagger = i(UXU^\dagger)(UZU^\dagger)$,
- $U(-X)U^\dagger = -UXU^\dagger$ and similarly for Z.

Thus it is enough to specify where X and Z go. However, since X and Z anti-commute, so must $UXU^\dagger$ and $UZU^\dagger$.

All possibilities

- X can go to any element of $\pm P_1^*$,
- Z can go to any element of $\pm P_1^* \setminus \{\pm UXU^\dagger\}$.

Clifford group $\mathcal{C}_1$

Single qubit

$\pm P_1^* = \{\pm X, \pm Y, \pm Z\}$.

Restrictions

Conjugation must preserve the structure of Pauli matrices.

- $Y = iXZ$, thus $UYU^\dagger = i(UXU^\dagger)(UZU^\dagger)$,
- $U(-X)U^\dagger = -UXU^\dagger$ and similarly for Z.

Thus it is enough to specify where X and Z go. However, since X and Z anti-commute, so must $UXU^\dagger$ and $UZU^\dagger$.

All possibilities

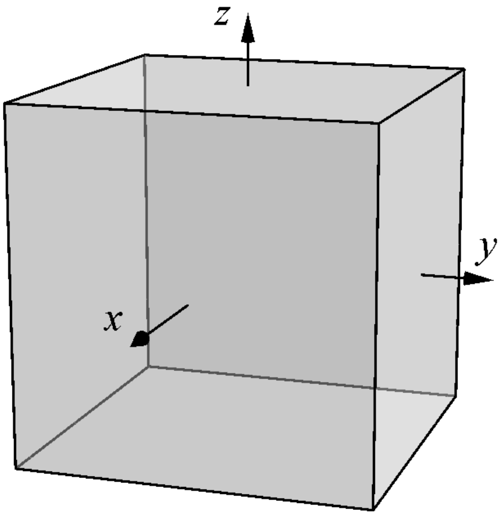
- X can go to any element of $\pm P_1^*$,
- Z can go to any element of $\pm P_1^* \setminus \{\pm UXU^\dagger\}$.

Group order

$|\mathcal{C}_1| = 6 \cdot 4 = 24$.

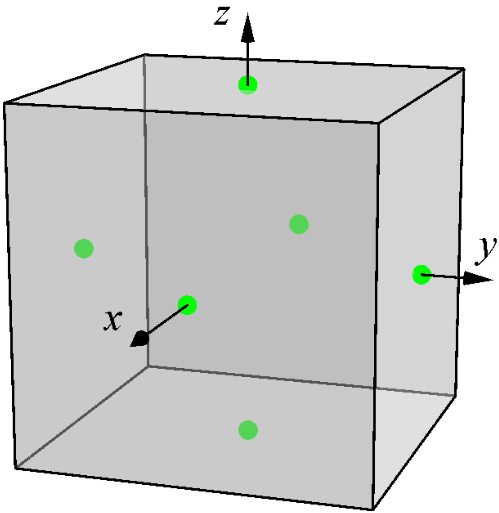
Clifford group $\mathcal{C}_1$

Clifford group rotations



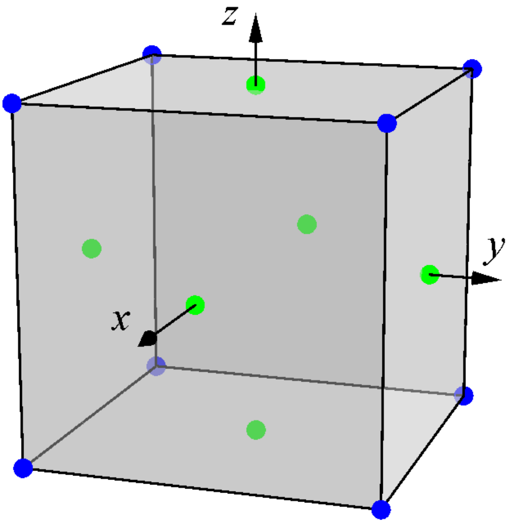
Clifford group $\mathcal{C}_1$

Clifford group rotations



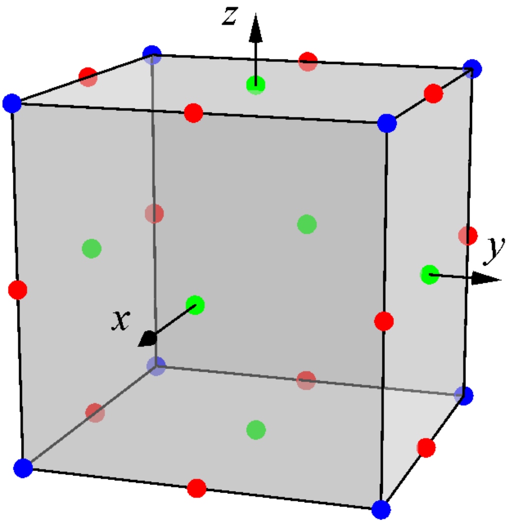
Clifford group $\mathcal{C}_1$

Clifford group rotations



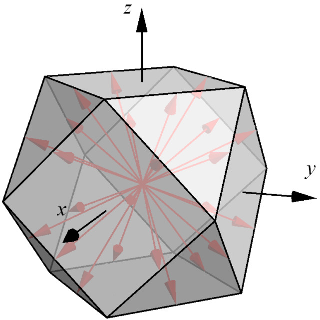
Clifford group $\mathcal{C}_1$

Clifford group rotations



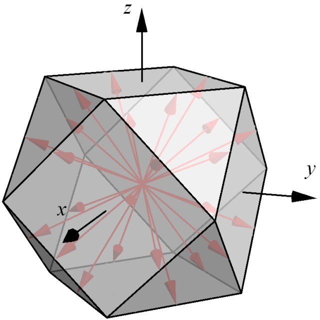
Clifford group $\mathcal{C}_1$

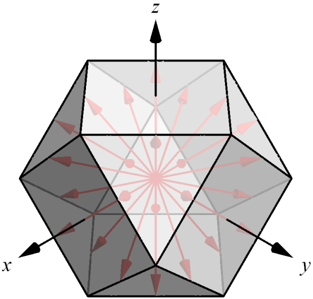
Cuboctahedron



Clifford group $\mathcal{C}_1$

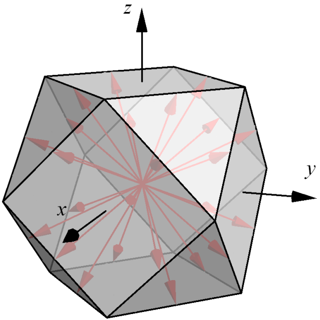
Cuboctahedron

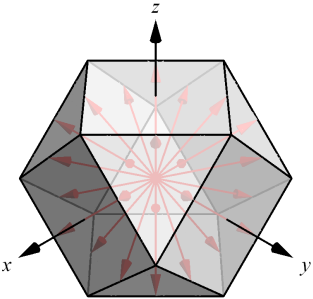




Clifford group $\mathcal{C}_1$

Cuboctahedron



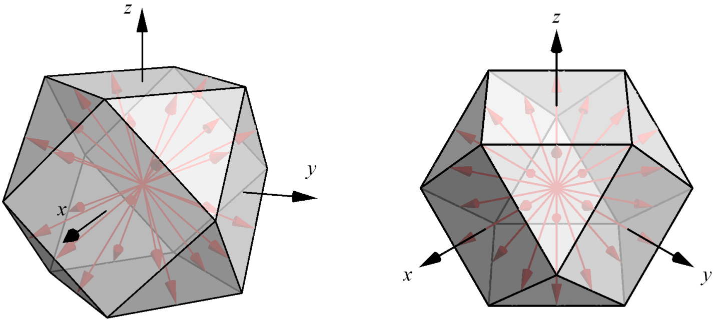


Poll

Guess what's the value of $|\mathcal{C}_2|$?

Clifford group $\mathcal{C}_1$

Cuboctahedron



Poll

Guess what's the value of $|\mathcal{C}_2|$? Answer: $|\mathcal{C}_2| = 11520$.

Order of $\mathcal{C}_n$

Restrictions

It is enough to specify where X_i and Z_i go for all $i \in \{1, \ldots, n\}$.

Order of $\mathcal{C}_n$

Restrictions

It is enough to specify where X_i and Z_i go for all $i \in \{1, \ldots, n\}$.
All X's and Z's commute, except X_i and Z_i that anti-commute:

$$\begin{array}{ccccc} X_1 & X_2 & \ldots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \ldots & Z_{n-1} & Z_n \end{array}$$

Order of $\mathcal{C}_n$

Restrictions

It is enough to specify where X_i and Z_i go for all $i \in \{1, \dots, n\}$.
All X's and Z's commute, except X_i and Z_i that anti-commute:

$$\begin{array}{ccccc} X_1 & X_2 & \dots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \dots & Z_{n-1} & Z_n \end{array}$$

Claim

Each matrix in $\pm P_n^*$ commutes (anti-commutes) with exactly half of Pauli matrices P_n.

Proof.

Let $\sigma \in \pm P_n^*$ and k be a position where σ does not contain I. All Paulis that anti-commute with σ can be constructed as follows:

Order of $\mathcal{C}_n$

Restrictions

It is enough to specify where X_i and Z_i go for all $i \in \{1, \ldots, n\}$.
All X's and Z's commute, except X_i and Z_i that anti-commute:

$$\begin{array}{ccccc} X_1 & X_2 & \ldots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \ldots & Z_{n-1} & Z_n \end{array}$$

Claim

Each matrix in $\pm P_n^*$ commutes (anti-commutes) with exactly half of Pauli matrices P_n.

Proof.

Let $\sigma \in \pm P_n^*$ and k be a position where σ does not contain I. All Paulis that anti-commute with σ can be constructed as follows:

- put any of I, X, Y, Z at each position other than k,

Order of $\mathcal{C}_n$

Restrictions

It is enough to specify where X_i and Z_i go for all $i \in \{1, \ldots, n\}$. All X's and Z's commute, except X_i and Z_i that anti-commute:

$$\begin{array}{ccccc} X_1 & X_2 & \ldots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \ldots & Z_{n-1} & Z_n \end{array}$$

Claim

Each matrix in $\pm P_n^*$ commutes (anti-commutes) with exactly half of Pauli matrices P_n.

Proof.

Let $\sigma \in \pm P_n^*$ and k be a position where σ does not contain I. All Paulis that anti-commute with σ can be constructed as follows:

- put any of I, X, Y, Z at each position other than k,
- fill the kth position in any of two possible ways so that the obtained matrix anti-commutes with σ.

Order of $\mathcal{C}_n$

Restrictions

$$\begin{array}{ccccc} X_1 & X_2 & \dots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \dots & Z_{n-1} & Z_n \end{array}$$

Order of $\mathcal{C}_n$

Restrictions

$$\begin{array}{ccccc} X_1 & X_2 & \dots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \dots & Z_{n-1} & Z_n \end{array}$$

Counting

Where can $U \in \mathcal{C}_n$ send X_n and Z_n?

Order of $\mathcal{C}_n$

Restrictions

$$\begin{array}{ccccc} X_1 & X_2 & \dots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \dots & Z_{n-1} & Z_n \end{array}$$

Counting

Where can $U \in \mathcal{C}_n$ send X_n and Z_n?

- X_n can go to any element of $\pm P_n^*$, i.e., $2(4^n - 1)$ choices,

Order of $\mathcal{C}_n$

Restrictions

$$\begin{array}{ccccc} X_1 & X_2 & \dots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \dots & Z_{n-1} & Z_n \end{array}$$

Counting

Where can $U \in \mathcal{C}_n$ send X_n and Z_n?

- X_n can go to any element of $\pm P_n^*$, i.e., $2(4^n - 1)$ choices,
- Z_n can go to any element of $\pm P_n^*$ that anti-commutes with $U X_n U^\dagger$, i.e., $\frac{2|P_n|}{2} = 4^n$ choices.

Order of $\mathcal{C}_n$

Restrictions

$$\begin{array}{ccccc} X_1 & X_2 & \dots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \dots & Z_{n-1} & Z_n \end{array}$$

Counting

Where can $U \in \mathcal{C}_n$ send X_n and Z_n?

- X_n can go to any element of $\pm P_n^*$, i.e., $2(4^n - 1)$ choices,
- Z_n can go to any element of $\pm P_n^*$ that anti-commutes with $UX_nU^\dagger$, i.e., $\frac{2|P_n|}{2} = 4^n$ choices.

Similarly for the next pair (X_{n-1}, Z_{n-1}), just replace n by $n-1$.

Order of $\mathcal{C}_n$

Restrictions

$$\begin{array}{ccccc} X_1 & X_2 & \dots & X_{n-1} & X_n \\ | & | & & | & | \\ Z_1 & Z_2 & \dots & Z_{n-1} & Z_n \end{array}$$

Counting

Where can $U \in \mathcal{C}_n$ send X_n and Z_n?

- X_n can go to any element of $\pm P_n^*$, i.e., $2(4^n - 1)$ choices,
- Z_n can go to any element of $\pm P_n^*$ that anti-commutes with $U X_n U^\dagger$, i.e., $\frac{2|P_n|}{2} = 4^n$ choices.

Similarly for the next pair (X_{n-1}, Z_{n-1}), just replace n by $n-1$.

Result

$$|\mathcal{C}_n| = \prod_{j=1}^{n} 2(4^j - 1) \cdot 4^j = 2^{n^2+2n} \prod_{j=1}^{n} (4^j - 1).$$

Order of $\mathcal{C}_n$

How does it grow?

n	$\lvert\mathcal{C}_n\rvert$
1	24
2	11520
3	92897280
4	12128668876800
5	25410822678459187200

Order of $\mathcal{C}_n$

How does it grow?

n	$\lvert\mathcal{C}_n\rvert$
1	24
2	11520
3	92897280
4	12128668876800
5	25410822678459187200

This is $\frac{1}{8}$ times "Sloane's A003956".

Order of $\mathcal{C}_n$

How does it grow?

n	$\lvert\mathcal{C}_n\rvert$
1	24
2	11520
3	92897280
4	12128668876800
5	25410822678459187200

This is $\frac{1}{8}$ times "Sloane's A003956".

Upper bound

$$|\mathcal{C}_n| \leq 2^{n^2+2n} \prod_{j=1}^{n} 4^j = 2^{2n^2+3n}.$$

Order of $\mathcal{C}_n$

Search: **id:A003956**

Displaying 1-1 of 1 results found page 1

Format: long | short | internal | text Sort: relevance | references | number Highlight: on | off

A003956 Order of complex Clifford group of degree 2^n arising in quantum coding theory. +0 13

8, 192, 92160, 743178240, 97029351014400, 203286581427673497600, 6819500449352277792129024000, 3660967964237442812098963052691456000, 31446995505814020383166371418359014222725120000 (list; graph; listen)

OFFSET	0,1
REFERENCES	B. Runge, Codes and Siegel modular forms, Discrete Math. 148 (1996), 175-204.
LINKS	G. Nebe, E. M. Rains and N. J. A. Sloane, Self-Dual Codes and Invariant Theory, Springer, Berlin, 2006. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory, 44 (1998), 1369-1387. G. Nebe, E. M. Rains and N. J. A. Sloane, The invariants of the Clifford groups, Des. Codes Crypt. 24 (2001), 99-121.
MAPLE	2^(n^2+2*n+3)*product(4^j-1, j=1..n);
CROSSREFS	Cf. A014116, A014115, A001309, A027672. Equals twice A027638. Sequence in context: A003435 A071303 A128406 this_sequence A041269 A103500 A119299 Adjacent sequences: A003953 A003954 A003955 this_sequence A003957 A003958 A003959
KEYWORD	nonn,easy,nice
AUTHOR	njas, Peter Shor (shor(AT)research.att.com)

page 1

Order of $\mathcal{C}_n$

Their definition

Calderbank R.A., Rains E.M., Shor P.W., Sloane N.J.A.,
Quantum Error Correction Via Codes Over GF(4), `arXiv:quant-ph/9608006v5`.

The *complex Clifford group* L is defined to be the subgroup of the normalizer of E in $U(2^n)$ that contains entries from $\mathbb{Q}[\eta]$, $\eta = (1+i)/\sqrt{2}$. The full normalizer of E in $U(2^n)$ has an infinite center consisting of the elements $e^{2\pi i\theta} I$, $\theta \in \mathbb{R}$. Although these central elements have no effect quantum-mechanically, we wish to work with a finite group. The smallest coefficient ring we can use is $\mathbb{Q}[\eta]$, since

$$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\}^3 = \begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix} .$$

Order of $\mathcal{C}_n$

Their definition

Calderbank R.A., Rains E.M., Shor P.W., Sloane N.J.A.,
Quantum Error Correction Via Codes Over GF(4), `arXiv:quant-ph/9608006v5`.

The *complex Clifford group* L is defined to be the subgroup of the normalizer of E in $U(2^n)$ that contains entries from $\mathbb{Q}[\eta]$, $\eta = (1+i)/\sqrt{2}$. The full normalizer of E in $U(2^n)$ has an infinite center consisting of the elements $e^{2\pi i\theta} I$, $\theta \in \mathbb{R}$. Although these central elements have no effect quantum-mechanically, we wish to work with a finite group. The smallest coefficient ring we can use is $\mathbb{Q}[\eta]$, since

$$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\}^3 = \begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix} .$$

Explanation of factor 8

They assume that $H, P \in \mathcal{C}_n$, i.e., they define $\mathcal{C}_n$ as the group generated by H, P, and $CNOT$. Thus they get 8 times more, since $\eta I \in \mathcal{C}_n$, where $\eta = \frac{1+i}{\sqrt{2}}$ is the 8th root of unity.

Generators of $\mathcal{C}_n$

Theorem

The Clifford group $\mathcal{C}_n$ is generated by H, P, and $CNOT$:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Generators of $\mathcal{C}_n$

Theorem

The Clifford group $\mathcal{C}_n$ is generated by H, P, and $CNOT$:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

More precisely, $\mathcal{C}_n = \langle H_i, P_i, CNOT_{ij} \rangle / U(1)$.

Generators of $\mathcal{C}_n$

Theorem

The Clifford group $\mathcal{C}_n$ is generated by H, P, and $CNOT$:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

More precisely, $\mathcal{C}_n = \langle H_i, P_i, CNOT_{ij} \rangle / U(1)$.

Proof.

It is easy to verify that $\mathcal{C}_1 = \langle H, P \rangle / U(1)$. Use induction on n.

Generators of $\mathcal{C}_n$

Proof (continued).

Let $U \in \mathcal{C}_{n+1}$. Since X_1 and Z_1 anti-commute, so do $UX_1U^\dagger$ and $UZ_1U^\dagger$. We can permute qubits and apply elements of $\mathcal{C}_1$ so that

$$UX_1U^\dagger = X \otimes M',$$
$$UZ_1U^\dagger = Z \otimes N'.$$

for some $M', N' \in \pm P_n$.

Generators of $\mathcal{C}_n$

Proof (continued).

Let $U \in \mathcal{C}_{n+1}$. Since X_1 and Z_1 anti-commute, so do $UX_1U^\dagger$ and $UZ_1U^\dagger$. We can permute qubits and apply elements of $\mathcal{C}_1$ so that

$$UX_1U^\dagger = X \otimes M',$$
$$UZ_1U^\dagger = Z \otimes N'.$$

for some $M', N' \in \pm P_n$. Let

$$U(|0\rangle \otimes |\psi\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi_0\rangle + |1\rangle \otimes |\psi_1\rangle).$$

Define U' by $U' |\psi\rangle = |\psi_0\rangle$. One can show that $U' \in \mathcal{C}_n$.

Generators of $\mathcal{C}_n$

Proof (continued).

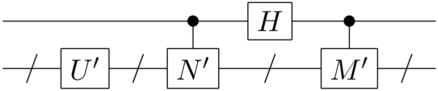
Let $U \in \mathcal{C}_{n+1}$. Since X_1 and Z_1 anti-commute, so do $UX_1U^\dagger$ and $UZ_1U^\dagger$. We can permute qubits and apply elements of $\mathcal{C}_1$ so that

$$UX_1U^\dagger = X \otimes M',$$
$$UZ_1U^\dagger = Z \otimes N'.$$

for some $M', N' \in \pm P_n$. Let

$$U(|0\rangle \otimes |\psi\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi_0\rangle + |1\rangle \otimes |\psi_1\rangle).$$

Define U' by $U'|\psi\rangle = |\psi_0\rangle$. One can show that $U' \in \mathcal{C}_n$. Then we can implement U as follows:



Stabilizer formalism

Stabilizer formalism

Who doesn't know that the stabilizer formalism is?

Gottesman-Knill theorem

Schrödinger vs. Heisenberg

Gottesman-Knill theorem

Schrödinger vs. Heisenberg

- *Schrödinger picture*: quantum states evolve in time,

Gottesman-Knill theorem

Schrödinger vs. Heisenberg

- *Schrödinger picture*: quantum states evolve in time,
- *Heisenberg picture*: operators evolve in time.

Gottesman-Knill theorem

Schrödinger vs. Heisenberg

- *Schrödinger picture*: quantum states evolve in time,
- *Heisenberg picture*: operators evolve in time.

Theorem (Gottesman-Knill)

Any quantum computation involving only:

- *measurements in standard basis,*
- *Clifford group gates (conditioned on classical bits, e.g., measurement outcomes)*

can be perfectly simulated in polynomial time on a probabilistic classical computer.

Gottesman-Knill theorem

Schrödinger vs. Heisenberg

- *Schrödinger picture*: quantum states evolve in time,
- *Heisenberg picture*: operators evolve in time.

Theorem (Gottesman-Knill)

Any quantum computation involving only:

- *measurements in standard basis,*
- *Clifford group gates (conditioned on classical bits, e.g., measurement outcomes)*

can be perfectly simulated in polynomial time on a probabilistic classical computer.

CHP (CNOT-Hadamard-Phase)

Program in C written by Aaronson and Gottesman to simulate such circuits. Can easily handle up to 3000 qubits!

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, `arXiv:math/0001038v2`.

Theorem 6.5 *Let* $m \geq 1$ *and let* G *be a finite group such that* $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. *Then there exists a root of unity* ζ *such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, arXiv:math/0001038v2.

Theorem 6.5 *Let $m \geq 1$ and let G be a finite group such that $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. Then there exists a root of unity ζ such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

In other words

Let $m \geq 1$. Then $\mathcal{C}_m$ together with any other gate not in $\mathcal{C}_m$ form a universal set of quantum gates.

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, `arXiv:math/0001038v2`.

Theorem 6.5 *Let $m \geq 1$ and let G be a finite group such that $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. Then there exists a root of unity ζ such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

In other words

Let $m \geq 1$. Then $\mathcal{C}_m$ together with any other gate not in $\mathcal{C}_m$ form a universal set of quantum gates.

Proof.

...

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, arXiv:math/0001038v2.

Theorem 6.5 *Let $m \geq 1$ and let G be a finite group such that $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. Then there exists a root of unity ζ such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

In other words

Let $m \geq 1$. Then $\mathcal{C}_m$ together with any other gate not in $\mathcal{C}_m$ form a universal set of quantum gates.

Proof.

... $\mathcal{RC}_M$-lattices ...

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, `arXiv:math/0001038v2`.

Theorem 6.5 *Let $m \geq 1$ and let G be a finite group such that $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. Then there exists a root of unity ζ such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

In other words

Let $m \geq 1$. Then $\mathcal{C}_m$ together with any other gate not in $\mathcal{C}_m$ form a universal set of quantum gates.

Proof.

... $\mathcal{RC}_M$-lattices ... natural module ...

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, `arXiv:math/0001038v2`.

Theorem 6.5 *Let* $m \geq 1$ *and let* G *be a finite group such that* $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. *Then there exists a root of unity* ζ *such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

In other words

Let $m \geq 1$. Then $\mathcal{C}_m$ together with any other gate not in $\mathcal{C}_m$ form a universal set of quantum gates.

Proof.

... $\mathcal{RC}_M$-lattices ... natural module ... inertia group ...

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, `arXiv:math/0001038v2`.

Theorem 6.5 *Let $m \geq 1$ and let G be a finite group such that $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. Then there exists a root of unity ζ such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

In other words

Let $m \geq 1$. Then $\mathcal{C}_m$ together with any other gate not in $\mathcal{C}_m$ form a universal set of quantum gates.

Proof.

... $\mathcal{RC}_M$-lattices ... natural module ... inertia group ... is ramified ...

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, `arXiv:math/0001038v2`.

Theorem 6.5 *Let $m \geq 1$ and let G be a finite group such that $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. Then there exists a root of unity ζ such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

In other words

Let $m \geq 1$. Then $\mathcal{C}_m$ together with any other gate not in $\mathcal{C}_m$ form a universal set of quantum gates.

Proof.

... $\mathcal{RC}_M$-lattices ... natural module ... inertia group ... is ramified ... which is a contradiction. □

Universal set of quantum gates

Mathematicians have shown that...

Nebe G., Rains E.M., Sloane N.J.A.,
The Invariants of the Clifford Groups, `arXiv:math/0001038v2`.

Theorem 6.5 *Let $m \geq 1$ and let G be a finite group such that $\mathcal{X}_m \leq G \leq U(2^m, \mathbb{C})$. Then there exists a root of unity ζ such that*

$$G = \langle \mathcal{X}_m, \zeta I_{2^m} \rangle.$$

In other words

Let $m \geq 1$. Then $\mathcal{C}_m$ together with any other gate not in $\mathcal{C}_m$ form a universal set of quantum gates.

Proof.

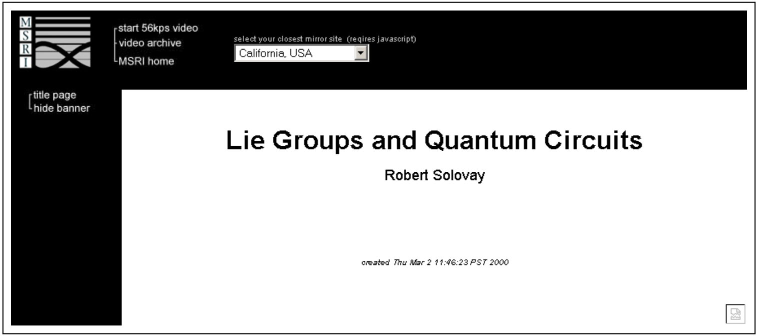
... $\mathcal{RC}_M$-lattices ... natural module ... inertia group ... is ramified ... which is a contradiction. □

Question

Is there an *elementary* proof for this?

Universal set of quantum gates

Another zero-knowledge proof



References

Clifford group

- Calderbank R.A., Rains E.M., Shor P.W., Sloane N.J.A., Quantum Error Correction Via Codes Over GF(4), arXiv:quant-ph/9608006v5.
- Nebe G., Rains E.M., Sloane N.J.A., The Invariants of the Clifford Groups, arXiv:math/0001038v2.
- Planat M., Jorrand P., Group theory for quantum gates and quantum coherence, arXiv:0803.1911v2 [quant-ph].

H, P, and $CNOT$ generate $\mathcal{C}_n$

- Gottesman D., Stabilizer Codes and Quantum Error Correction, PhD thesis, `arXiv:quant-ph/9705052v1`.
- Gottesman D., A Theory of Fault-Tolerant Quantum Computation, `arXiv:quant-ph/9702029v2`.
- Nielsen M.A., Chuang I.L., Quantum Computation and Quantum Information, Cambridge University Press, 2000.

Gottesman-Knill theorem

Gottesman D., The Heisenberg Representation of Quantum Computers, arXiv:quant-ph/9807006v1.

Aaronson S., Gottesman D., Improved Simulation of Stabilizer Circuits, arXiv:quant-ph/0406196v5.

Thank you for your attention!