Canonical form of non-binary stabilizer codes

Vlad Gheorghiu

Department of Physics
Carnegie Mellon University
Pittsburgh, PA 15213, U.S.A.

September 9, 2010

1. Brief of stabilizers
2. Qudit stabilizers
3. Canonical form of qudit stabilizer codes

A summary of this talk is available online at
http://quantum.phys.cmu.edu/QIP

Brief review of stabilizers

- In general, an n-qubit entangled state needs to be described by 2^n complex coefficients.
- This is bad! This is one of the reasons for which quantum computers are hard to simulate on a classical computer.
- But some entangled states are not so bad...
- Consider the maximally entangled state

$$|B_0\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

- Note that $X_1 \otimes X_2 |B_0\rangle = |B_0\rangle$ and $Z_1 \otimes Z_2 |B_0\rangle = |B_0\rangle$.

- We say that $|B_0\rangle$ is stabilized by X_1X_2 and Z_1Z_2.
- Actually it is stabilized as well by $X_1Z_1X_2Z_2$ and trivially by I_1I_2.
- Our state is therefore stabilized by an (Abelian) subgroup of the Pauli group on 2 qubits: $\mathcal{S} = \{I_1I_2, X_1X_2, Z_1Z_2, Y_1Y_2\}$, where we use the convention that $Y = XZ$. What is not so obvious is that, up to a global phase, $|B_0\rangle$ is the only state stabilized by $\mathcal{S}$. We say that $|B_0\rangle$ is a stabilizer state.
- A non-Abelian subgroup of the Pauli *cannot* stabilize a state. Why?
- Any Abelian group $\mathcal{S}$ of size $|\mathcal{S}|$ can be described *compactly* using at most $\log(|\mathcal{S}|)$ generators. In our case, $\mathcal{S} = \langle X_1X_2, Z_1Z_2\rangle$.
- Stabilizer states are more conveniently described by $\log(|\mathcal{S}|)$ generators rather than by their complex coefficients.

- More "dramatic" example:
  $|\psi\rangle = \frac{1}{4}(|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle)$
  is stabilized by
  $$\langle XZZXI, IXZZX, XIXZZ, ZXIXZ, ZZXIX \rangle$$
- In general any Abelian subgroup of the Pauli group on n qubits will stabilize some vector space.
- For example $\mathcal{S} = \langle Z_1 Z_2 \rangle$ stabilizes Span$\{|00\rangle, |11\rangle\}$.
- There is a duality between the vector space and its stabilizer. One uniquely defines the other and vice-versa.
- If the dimension of the stabilized vector space is greater than 1, then we have a stabilizer code.

The Gottesman-Knill theorem in a nutshell

- Recap: Abelian subgroup of Pauli group $\leftrightarrow$ subspace $\leftrightarrow$ stabilizer code (state).
- If $|\psi\rangle$ is stabilized by $\mathcal{S}$, then $U|\psi\rangle$ is stabilized by $U\mathcal{S}U^\dagger$
- The unitaries that map the n qubit Pauli group to itself under conjugation are called Clifford operations.
- They map stabilizer states (codes) to stabilizer states (codes).
- Are easy to simulate on a classical computer! (This is the Gottesman-Knill theorem in a nutshell).

Binary (algebraic) representation of stabilizer states/codes

- Let $\mathcal{S} = \langle g_1, g_2, \ldots g_k \rangle$. We can represent these generators in a compact form, using what is called a binary check matrix.
- A generator consists of I, X, Z and XZ operators (up to a sign, which one can keep track of). Can be generically represented as $X^{\vec{x}} Z^{\vec{z}}$. Group the binary n-dim row vectors $\vec{x}$ and $\vec{z}$ in a $2n$ row vector, denoted generically as $(\vec{x}|\vec{z})$. That's how one gets the k rows of the $k \times 2n$ check matrix.
- Example: $\mathcal{S} = \langle X_1 I_2 I_3, Z_1 Z_2 X_3 \rangle$ is represented by the check matrix

$$S = \begin{pmatrix} 100|000 \\ 001|110 \end{pmatrix}$$

- Conjugating the stabilizer generators by a Clifford operation corresponds to right-multiplying (column operations) the check matrix by an appropriate $2n \times 2n$ invertible binary matrix (symplectic matrix).

- Left multiplication (row operations) do not alter the stabilizer group, although in general changes the check matrix.
- For example, a conjugation by a Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ on the third qubit changes $\mathcal{S}$ to $H\mathcal{S}H^\dagger = \langle X_1 I_2 I_3, Z_1 Z_2 Z_3 \rangle$, and the new check matrix will be

$$S' = \begin{pmatrix} 100|000 \\ 000|111 \end{pmatrix} = \begin{pmatrix} 100|000 \\ 001|110 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Qudit stabilizers

- Stabilizer: an Abelian subgroup of the Pauli group on n qudits.
- Each qudit is assumed to have dimension $D > 2$.
- Instead of X and Z use "generalized" Pauli operators

$$X = \sum_{j=0}^{D-1} |j\rangle \langle j \oplus 1| \,, \quad Z = \sum_{j=0}^{D-1} \omega^j |j\rangle \langle j|, \quad \omega = \mathrm{e}^{2\pi \mathrm{i}/D}.$$

- The check matrix of a stabilizer with k generators is now a $k \times 2n$ matrix over $\mathbb{Z}_D$, the ring of integers mod D.
- By appropriate Clifford operations, one can transform the stabilizer to a simpler "canonical form".

The Smith normal form

- The following hold:

Theorem (Smith normal form)

Let S be an $M \times N$ integer matrix over $\mathbb{Z}_D$. Then there exist invertible integer matrices L and R such that $LSR = S'$ is diagonal.

- Trick: put the X-part of the stabilizer matrix in Smith normal form, through a sequence of column operations (that correspond to appropriate Clifford operations).
- We will use the following Clifford gates: $CNOT_{ab} = \sum_{j=0}^{D-1} |j\rangle\langle j|_a \otimes X_b^j$, $SWAP_{ab} = \sum_{j,k=0}^{D-1} |k\rangle\langle j|_a \otimes |j\rangle\langle k|_b$ and $S_q = \sum_{j=0}^{D-1} |j\rangle\langle jq|$ (with q invertible).
- Each of these operations have a corresponding elementary column operation (on the check matrix)

Column operations

- Corresponding column operations:
  1. $SWAP_{ab}$: interchange cols. a and b (on both X and Z part of the check matrix)
  2. $S^{a}_{q^{-1}}$: X part multiply col. a by invertible integer q; Z part multiply col. a by invertible integer q^{-1}
  3. $CNOT^{-m}_{ba}$: X part add m times col. b to col. a; Z part substract m times col. a from col. b
- Nice fact: the X and Z part of the check matrix do not "mix" during this process
- Put the X part of the check matrix in Smith normal form using a sequence of elementary row/column operations, and construct (step by step) the required Clifford operator C

- During the process the group stays Abelian (conjugation by unitaries preserves commutation relations), so at the end it must be Abelian.
- We end up with generators of the form $\langle X_1^{m_1} Z^{\vec{z_1}}, \ldots, X_k^{m_k} Z^{\vec{z_k}} \rangle$, but the generators *must* commute.
- This imposes

$$ZM = MZ^T$$

- When D is prime, all m_j can be chosen to be 1, so we have shown that the code is Clifford-equivalent to a graph code.
- In Phys. Rev. A **81**, 032326 (2010), *"Location of quantum information in additive graph codes"*, V. Gheorghiu, S. Y. Looi and R. B. Griffiths, we have an explicit unitary encoding circuit for graph codes.
- Use it for general stabilizer codes, not just graph codes, multiplying it by the extra Clifford C (that puts the stabilizer into the canonical form).