Quantum low density parity check codes

Martin Leslie

Department of Mathematics
University of Arizona

May 1, 2012

Qubits

- Let $|0\rangle = [1,0]^T$ and $|1\rangle = [0,1]^T$ be the *computational basis* for $\mathbb{C}^2$.
- The state of a *qubit* is described by a vector in $\mathcal{H}_1 = \{|\psi\rangle = a|0\rangle + b|1\rangle : a, b \in \mathbb{C} \text{ with } |a|^2 + |b|^2 = 1\}$.
- For n qubits, the state is described by an element of $\mathcal{H}_n = \mathcal{H}_1^{\otimes n}$.
- So for $|\psi\rangle \in \mathcal{H}_n$ we can write

$$|\psi\rangle = \sum_{i \in \mathbb{F}_2^n} a_i |i\rangle$$

  where $|i\rangle = |i_1\rangle \otimes \ldots \otimes |i_n\rangle$ and $\sum_i |a_i|^2 = 1$.
- Actually, we're really in projective Hilbert space

$$\mathbb{P}((\mathbb{C}^2)^{\otimes n}) = (\mathbb{C}^2)^{\otimes n} / \sim$$

  where $|\psi\rangle \sim \lambda|\psi\rangle$ (we don't distinguish between states differing only by a *global phase factor*).

Quantum mechanics on qubits

- The evolution of the state $|\psi\rangle$ of a closed quantum system from one time to another is given by a unitary matrix U via

$$|\psi\rangle \mapsto U|\psi\rangle.$$

- A quantum measurement is described by a collection $\{M_m : \mathcal{H}_n \to \mathcal{H}_n\}$ of measurement operators (one for each possible outcome m) satisfying $\sum_m M_m^\dagger M_m = I$. The probability of outcome m is

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

and if outcome m occurs the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}.$$

Measurement in the computational basis

- If
$$|\psi\rangle = \sum_{i \in \mathbb{F}_2^n} a_i |i\rangle$$
then choose the measurement operators to be the projections $M_i = |i\rangle\langle i|$ (so $M_i^\dagger M_i = M_i$ and $\sum_i M_i = I$).
- Then
$$p(i) = \langle\psi|M_i|\psi\rangle = \langle\psi|a_i|i\rangle = a_i^* a_i = |a_i|^2$$
and if the outcome of the measurement is i then the new state is
$$\frac{M_i|\psi\rangle}{\sqrt{p(i)}} = \frac{a_i|i\rangle}{|a_i|}$$
which we consider to be the same state as $|i\rangle$.

Measuring an observable

- If M is a Hermitian operator (i.e. $M^\dagger = M$) then it has a spectral decomposition

$$M = \sum_m m P_m.$$

- When we speak of measuring M we measure the set of operators $\{P_m\}$.
- With probability $p(m) = \langle\psi|P_m|\psi\rangle$ we see outcome m.
- After measuring m the system will be in the state $P_m|\psi\rangle/\sqrt{p(m)}$.
- Commuting observables can be measured simultaneously.

Some quantum gates

- The following Hermitian, unitary operators act on one qubit:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

- We think of X as a bit flip

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle$$

Z as a phase flip

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle$$

and $Y = iXZ$ as both. The Hadamard gate H takes $|0\rangle$ and $|1\rangle$ to the *dual basis*

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Density Matrices

- To describe ensembles of states $\{p_i, |\psi_i\rangle\}$ define the *density matrix*

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i|.$$

- Then unitary evolution U occurs by

$$\rho \mapsto U \rho U^\dagger.$$

- For measurements, outcome m occurs with probability

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \rho)$$

and if outcome m occurs then the new density matrix is

$$\rho_m = \frac{M_m \rho M_m^\dagger}{p(m)}.$$

The depolarizing channel

- This channel acts on density matrices ρ by not altering the state with probability $1-q$ and replacing the state with the maximally mixed state $I/2$ with probability q

$$\rho \mapsto (1-q)\rho + q\frac{I}{2}.$$

- For any density matrix ρ

$$\frac{I}{2} = \frac{I\rho I + X\rho X + Y\rho Y + Z\rho Z}{4}$$

so the depolarizing channel can also be thought of as

$$\rho \mapsto (1-p)\,\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

where $p = 3q/4$ is the probability that input state $|\psi\rangle$ is replaced by $X|\psi\rangle$, $Y|\psi\rangle$ or $Z|\psi\rangle$.

Stabilizer Codes

- Let the *Pauli group* be

$$G_n = \left\{ c \bigotimes_{i=1}^{n} A_i \mid c \in \{\pm 1, \pm i\}, A_i \in \{I, X, Y, Z\} \right\}.$$

- Notice that elements of this group commute iff they have an even number of places with different non-identity matrices. If they do not commute then they anti-commute.
- For $S \leq G_n$ define the subspace of $\mathcal{H}_n$ stabilized by S to be

$$V_S = \{|\psi\rangle : s|\psi\rangle = |\psi\rangle \text{ for all } s \in S\}$$

- For $V_S \neq 0$ we need all elements of S to commute and $-I \notin S$.
- Define a *stabilizer group* to be an abelian subgroup S with $-I \notin S$ and the *stabilizer code* corresponding to S to be V_S.

The 5 qubit code

- Let $S = \langle XZZXI, IXZZX, XIXZZ, ZXIXZ \rangle$. We can write this as a matrix

$$A = \begin{bmatrix} X & Z & Z & X & I \\ I & X & Z & Z & X \\ X & I & X & Z & Z \\ Z & X & I & X & Z \end{bmatrix}$$

- Now consider the set of errors $\{I, X_i, Y_i, Z_i : i = 1, \ldots, 5\}$. Define the *syndrome* of an error to be a vector of ± 1's: $+1$ if it commutes with a stabilizer generator and -1 if it anti-commutes.
- For example X_2 has syndrome $(-1, +1, +1, +1)$.
- If you check through you will see that each of the errors we are considering has a different syndrome.

Decoding the 5 qubit code

- Begin with a state $|\psi\rangle \in V_S$.
- An error $E \in G_n$ occurs, changing the state to $E|\psi\rangle$.
- Now for each stabilizer generator g_l, find $g_l E|\psi\rangle$. We get

$$g_l E|\psi\rangle = \pm E g_l|\psi\rangle = \pm E|\psi\rangle$$

  depending on the syndrome of E.
- Looking at the syndrome, find the unique error E that generates that syndrome.
- Apply $E^\dagger$ to fix it: $E^\dagger E|\psi\rangle = |\psi\rangle$.

Decoding stabilizer codes in general

- We can decode a collection of errors $\{E_j\}$ if all the errors in the collection with the same syndrome differ by an element of the stabilizer.
- To see this: if E_j and E_k have the same syndrome but $E_k^\dagger E_j = s \in S$, then if error E_j occurs we can still correct it by applying $E_k^\dagger$:

$$E_k^\dagger E_j |\psi\rangle = s|\psi\rangle = |\psi\rangle.$$

- Codes which use this property (i.e. the set of decodable errors has some overlapping syndromes) are called *degenerate*.
- Define the *minimum distance* d of a quantum code to be the minimum weight of the set of operators which commute with S but are not in S.
- We will call V_S an $[n, k, d]$ quantum code if it is a 2^k-dimensional subspace of $\mathcal{H}_n$ which has distance d.

Binary check matrices

- Define a function $r\colon G_n \to \mathbb{F}_2^{2n}$ by writing g as a string of X's times a string of Z's, forgetting the constant out the front, and then writing those strings in binary.
- For example $g = XIY = i(XIX)(IIZ)$ and $r(g) = 101001$.
- Notice $r(gg') = r(g) + r(g')$, that $\ker r = \{\pm I, \pm iI\}$ and that r is surjective.
- Thus, $\overline{G}_n = G_n/\{\pm I, \pm iI\} \cong \mathbb{F}_2^{2n}$.
- Now if S is a stabilizer group then since $-I \notin S$ we have no pairs of elements differing by $-I$ or $\pm iI$ so $|S| = |r(S)|$.

Decoding using check matrices

- Write $r(g) = [x(g), z(g)]$ and define the *twisted product*

$$r(g) \odot r(g') = x(g) \cdot z(g') + z(g) \cdot x(g').$$

- Then g and g' commute iff $r(g) \odot r(g') = 0$.
- Thus to define a stabilizer code we can give a matrix of rows with pairwise twisted product of rows zero.
- To find the syndrome of an error E we need to take the twisted product of E with each row.
- Instead we can write our error in binary as $[z(E), x(E)]$ and do our product with normal $\mathbb{F}_2$ matrix-vector product.

Dual-containing codes

- Start with an $M/2 \times N$ binary matrix H and then form a binary check matrix

$$A = \begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}.$$

- The twisted product constraint is equivalent to $HH^T = 0$.
- If we create a classical code $C = \{x \in \mathbb{F}_2^N : Hx = 0\}$ then this is equivalent to $C^\perp \subseteq C$.
- The code given by A is an $[N, k, d]$ quantum code with

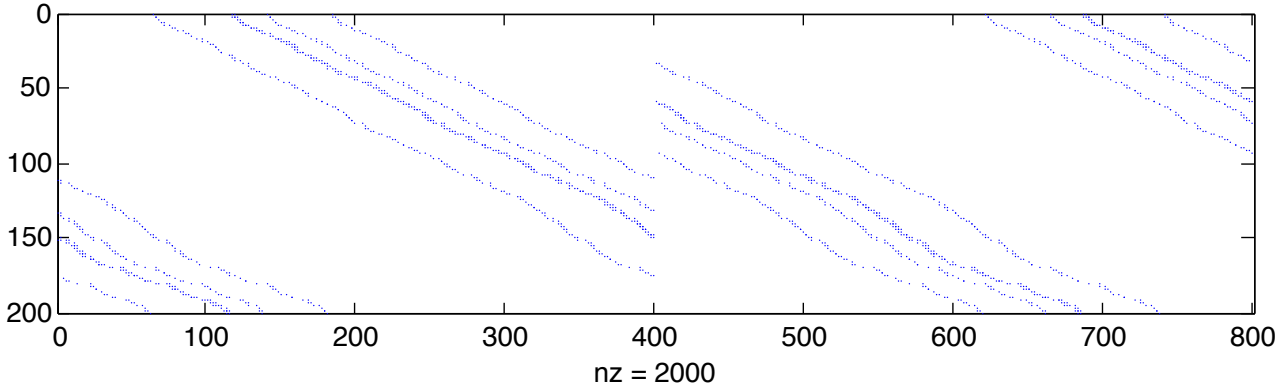
$$k = N - 2\,\mathrm{rank}(H)$$

and

$$d = \min\{\mathrm{wt}(c) : c \in C \setminus C^\perp\}.$$

Quantum LDPC codes ala Mackay

- To construct a $M \times N$ *bicycle code* matrix H with k ones per row:
- Create a random $N/2 \times N/2$ circulant matrix C with row weight $k/2$
- Define $H_0 = \begin{bmatrix} C & C^T \end{bmatrix}$
- Delete $N/2 - M$ rows of H_0, attempting to keep the column weights uniform



Tanner graphs for stabilizer codes

- Represent a stabilizer code by an edge-labeled bipartite graph, called a *Tanner graph*.
- Put an edge between a variable node (qubit) q and a check node (stabilizer generator) c if the qth component of the cth stabilizer differs from the identity.

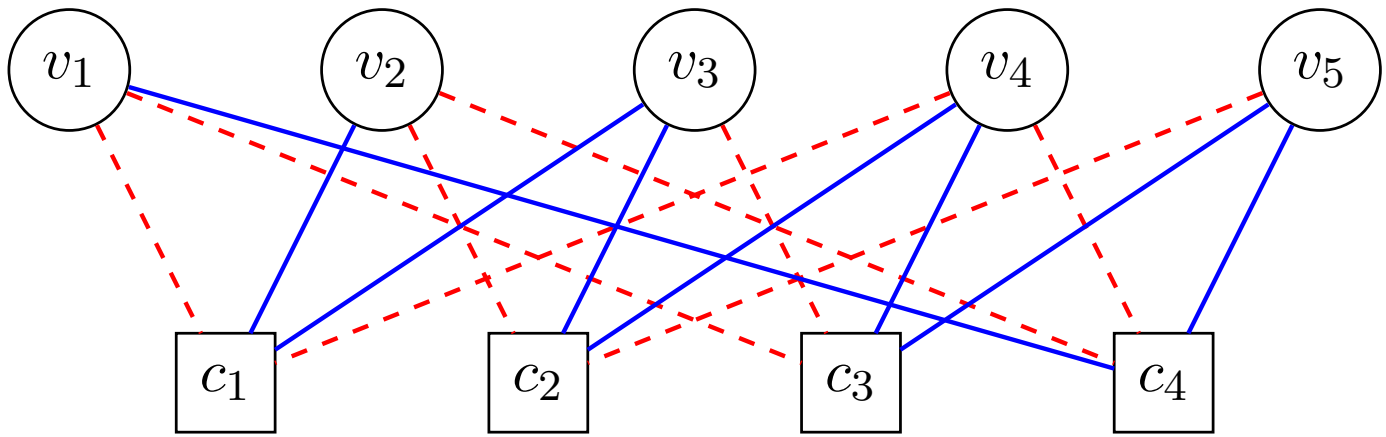


Figure: The Tanner graph for the 5 qubit code. Dashed red lines represent X and solid blue lines represent Z.

Belief propagation decoding I

- We are aiming to find the most likely $E \in \overline{G}_n$ with syndrome s. We do this via an iterative message passing algorithm.
- Let $n(c)$ be the set of variable nodes connected to check node c, let $n(c) \setminus q$ be shorthand for $n(c) \setminus \{q\}$ and make similar definitions for $n(q)$ and $n(q) \setminus c$.
- We send probability distributions for $E_q \in \{I, X, Y, Z\}$ i.e. functions with four possible inputs.

Belief propagation decoding II

- To initialize the messages we first send a message from a qubit to each check it is connected to

$$p^{(0)}_{q\to c}(b) = p^{\mathrm{ch}}_q(b) = P(E_q = b).$$

- From each check to qubit

$$p^{(i)}_{c\to q}(b) = P(\text{check } c \text{ is satisfied} \mid E_q = b, s).$$

- From qubit to check

$$p^{(i)}_{q\to c}(b) = P(E_q = b \mid \text{checks } c' \in n(q) \setminus c \text{ satisfied}).$$

- Then we calculate

$$p^{(i)}_q(b) = P(E_q = b \mid \text{checks } c' \in n(q) \text{ satisfied})$$

and from this decide the most likely E^*. If this error has the correct syndrome then we are done, otherwise we send messages from check to qubit again.

Belief propagation decoding III

- Using some simple probability calculations we can find these probabilities, assuming conditional independence of the inputs:

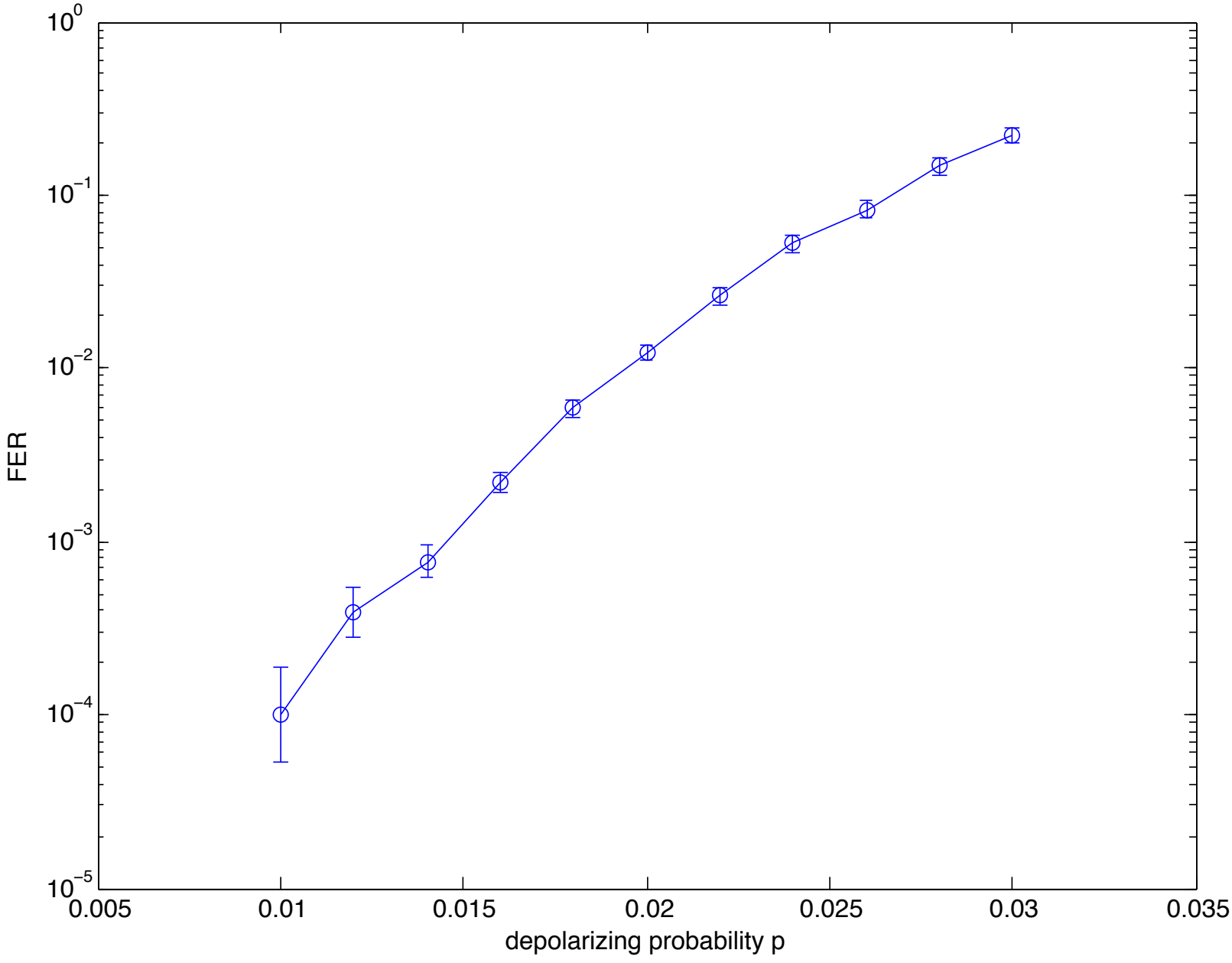
$$p_q^{\text{ch}} = (1-p, p/3, p/3, p/3),$$

$$p_{c\to q}^{(i)}(b) = \sum_{E \text{ with } E_q=b} \mathbb{1}\left[A_c \cdot E = s_c\right] \prod_{q'\in n(c)\setminus q} p_{q'\to c}^{(i-1)}(E_{q'}),$$

$$p_{q\to c}^{(i)}(b) \propto p_q^{\text{ch}}(b) \prod_{c'\in n(q)\setminus c} p_{c'\to q}^{(i)}(b),$$

$$p_q^{(i)}(b) \propto p_q^{\text{ch}}(b) \prod_{c'\in n(q)} p_{c'\to q}^{(i)}(b).$$

Performance of a QLDPC code



Performance bounds for QLDPC codes