Recent constructions of asymptotically good quantum LDPC codes

Gilles Zémor

Scribed by Hugo Delavenne

Caipi Symposium — 10th, November, 2023

Contents

1 Quantum error correcting codes

1.1 Qubits

A qubit can be seen as a superposition of classical bits.

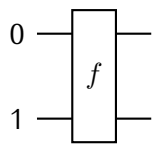
Definition 1.1 **Qubit**

A qubit is described by an expression $\alpha|0\rangle+\beta|1\rangle \in \mathcal{H}$, with $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2+|\beta|^2=1$. Formally, the space of states of a single qubit is a Hilbert space $\mathcal{H}$ of dimension 2.

An example of a qubit state is $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. The states $(|0\rangle, |1\rangle)$ form a basis of the Hilbert space. They are column orthogonal vectors. In a more traditional mathematical notation they would be written e_0 and e_1.

A vector of two qubits is written $\alpha_{00}|00\rangle + \alpha 01|10\rangle + \alpha 01|10\rangle + \alpha 11|11\rangle$, a vector of three qubits $\alpha 000|000\rangle + ...$ More generally, a n qubits vector is an element of the space $\mathcal{H}^{\otimes n}$, with basis $\mathbb{F}_2^n$.

A two-bit input classical function $f : \mathbb{F}_2^2 \to \mathbb{F}_2^2$



naturally extends to qubits (when f is one-to-one), and applied on a superposition $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ gives the result $\frac{1}{2}(f(|00\rangle) + f(|01\rangle) + f(|10\rangle) + f(|11\rangle))$. This illustrates the power of quantum computation because it is possible to evaluate simultaneously several values of f with a single execution of the circuit. Quantum computation allows therefore a form of parallelism which sometimes results in exponential speedups over classical computation.

The role of quantum error correcting codes is to protect the quantum states involved in quantum computations.

Quantum operations must be unitary and are represented by matrices.

Example 1.2

The bit-flip operator $X : \begin{matrix} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{matrix}$ is represented by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Operators can be extended to several qubits with tensor products: $X \otimes I : \begin{matrix} |00\rangle & \mapsto & |10\rangle \\ |10\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |01\rangle \end{matrix}$.

An important result relevant to quantum computation is the no-cloning theorem.

Theorem 1.3 **No cloning theorem**

There is no procedure to clone any state $|\psi\rangle \to |\psi\rangle\,|\psi\rangle$.

Essentially it is because there is no unitary transformation that allows this. For a short while it made people think that no quantum error correction is possible since the basic classical repetition code has no quantum equivalent.

1.2 Quantum error-correcting codes

Consider an orthogonal direct sum decomposition of a Hilbert space of the form $\mathcal{H}^{\otimes n} = A \overset{\perp}{\oplus} B$. A *measurement* is an operation such that given an input $|\psi\rangle = \alpha_A\,|\psi_A\rangle + \alpha_B\,|\psi_B\rangle$, with $|\psi_A\rangle \in A$, $|\psi_B\rangle \in B$, it projects $|\psi\rangle$ on $|\psi_A\rangle$ with probability $|\alpha_A|^2$ and $|\psi_B\rangle$ with probability $|\alpha_B|^2$, and tells us which projection occured.

To illustrate, we can easily enough correct a single bit-flip error occuring on a qubit in a way that mimicks the classical repetition code. Starting with the single qubit state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, we can adjoin to it two auxiliary qubits in the state $|00\rangle$ to obtain $|\psi\rangle \otimes |00\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |00\rangle$, from which there is a unitary transformation that yields $|\phi\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$.

Consider the parity-check matrix of the repetition code $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$.

There is a quantum measurement that computes the "syndrome" of a bit-flip error.

Let the subspace A_{00} be generated by $|000\rangle, |111\rangle$, the subspace A_{01} by $|001\rangle, |110\rangle$, A_{10} by $|100\rangle, |011\rangle$ and A_{11} by $|010\rangle, |101\rangle$. The Hilbert space $\mathcal{H}$ (of dimension 8) over three qubits is then the direct sum

$$\mathcal{H} = A_{00} \overset{\perp}{\oplus} A_{01} \overset{\perp}{\oplus} A_{10} \overset{\perp}{\oplus} A_{11}. \tag{1}$$

Suppose that we apply X on the first qubit of $|\phi\rangle$, which yields $|\varphi\rangle = \alpha\,|100\rangle + \beta\,|011\rangle$. We go from A_{00} to A_{10}. By applying twice the $X \otimes I \otimes I$ (shorthand XII) operator, we can correct an error on the first qubit since $(XII)(XII)\,|\varphi\rangle = |\varphi\rangle$.

Consider the operator $aIII + bXII : |\varphi\rangle \mapsto a\,|\varphi\rangle + bXII\,|\varphi\rangle$, with $|\varphi\rangle \in A_{00}$ and $XII\,|\varphi\rangle \in A_{10}$. If we measure the resulting state and get $|\varphi\rangle$ then no error occured. If we get $XII\,|\varphi\rangle$ then we apply again XII to get $|\varphi\rangle$.

In the classical world there is usually a quantity that is continuous, for example an electric charge describing the bit, which initially is $+A$ or $-A$. And when we measure the sign of an electric charge we can put it back to its original real value. What is going on here is somewhat similar.

Consider the following operator: $Z : \begin{matrix} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{matrix}$. It is represented by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. If a ZII error occurs, then the encoded state ϕ is transformed to $\alpha\,|000\rangle - \beta\,|111\rangle$. This state belongs to A_{00}, so measuring according to the decomposition (1) does not tell us that an error occurred. The quantum "repetition" code cannot correct all possible errors on a single qubit.

What we need is to find a decomposition of the Hilbert space $\mathcal{H}$ of the form

$$C \overset{\perp}{\oplus} C_{XII\ldots} \overset{\perp}{\oplus} C_{ZII\ldots} \overset{\perp}{\oplus} C_{(XZ)II\ldots} \overset{\perp}{\oplus} C_{IXI\ldots} \overset{\perp}{\oplus} C_{IZI\ldots} \overset{\perp}{\oplus} \ldots \tag{2}$$

where an X error on the first qubit of a state in C takes it to $C_{XII\ldots}$, a Z error on the first qubit takes it to $C_{ZII\ldots}$ and so on...

Any unitary matrix $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ can be written $\alpha I + \beta X + \gamma Z + \delta XZ$. We note that if $|\varphi\rangle$ is transformed to $UIII\cdots|\phi\rangle$, then measuring according to (2) gives us one of the four states $|\varphi\rangle, XII\cdots|\varphi\rangle, ZII\cdots|\varphi\rangle, (XZ)II\cdots|\varphi\rangle$ which lie in different subspaces of (2), so that we know the error pattern we need to remove to recover $|\varphi\rangle$.

To find such a decomposition we need more qubits, i.e. a larger Hilbert space than for the 3-qubit repetition code. Remarquably, they exist.

1.3 Example: the 5-qubit code

Consider a 5-qubit Hilbert space and the following operators.

- $M_1 = XZZXI$
- $M_2 = IXZZX$
- $M_3 = XIXZZ$
- $M_4 = ZXIXZ$

These operators commute since $XZ = -ZX$, $M_iM_j = M_jM_i$, and the group S generated by (M_1, M_2, M_3, M_4) is a 16 element abelian group.

Starting from a single qubit $\alpha|0\rangle + \beta|1\rangle$, we adjoint four auxiliary qubits in the state $|0000\rangle$, and transform the resulting state to $|\varphi\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle$, with $|\psi_0\rangle = \frac{1}{4}\sum_{M\in S} M|00000\rangle$ and $|\psi_1\rangle = \frac{1}{4}\sum_{M\in S} M|11111\rangle$. For $M \in S$, $M|\varphi\rangle = |\varphi\rangle$.

Now we measure. A_{1111} is the intersection of eigenspaces of M_i with eigenvalue 1, A_{-1111} the intersection of eigenspaces of M_1 with eigenvalue -1, and M_i with eigenvalue $+1$ for $i = 2, 3, 4$, and so on, we define $A_{ijk\ell}$ to be the intersection of the eigenspaces of M_1, M_2, M_3, M_4 with eigenvalues i, j, k, ℓ respectively. Because the operators M_1, M_2, M_3, M_4 commute, they are diagonal in the same orthonormal basis, and we have $\mathcal{H} = \overset{\perp}{\bigoplus} A_{ijk\ell}$. Note that we have $|\varphi\rangle \in A_{1111}$

Definition 1.4 **Pauli errors**

The Pauli errors are $\{I, X, Y, Y\}^n \otimes \{1, -1, i, -i\}$, where $Y := iXZ$.

If we have a Pauli error E, it either commutes or anticommutes with $M \in S$. Suppose it anticommutes with M_1 for example, $EM_1 = -M_1E$. So $M_1E|\varphi\rangle = -EM_1|\varphi\rangle = -E|\varphi\rangle$, because $|\varphi\rangle$ is stabilised by any $M \in S$ and by M_1 in particular. So $E|\varphi\rangle$ belongs to the -1 eigenspace of M_1. Therefore, knowing whether E commutes or anticommutes with M_1, M_2, M_3, M_4 tells which space $A_{ijk\ell}$ the corrupted state $E|\varphi\rangle$ falls into, and conversely, knowing which space $A_{ijk\ell}$ the state $E|\varphi\rangle$ belongs to tells us whether E commutes or anticommutes with M_1, M_2, M_3, M_4.

The magic happens here:

Proposition 1.5

There is a bijection between the Pauli errors of weight 1 and the patterns $\{+1, -1\}^4$. Specifically, for every one of the 15 patterns $ijk\ell \neq 1111$, there is exactly one Pauli error E of weight 1 such that $E|\varphi\rangle \in A_{ijk\ell}$.

For example, $XIIII$ commutes with M_1, M_2, M_3, and anticommutes with M_4, so $XIIII|\varphi\rangle \in A_{111-1}$. $ZIIII$ anticommutes with M_1 and M_3 and commutes with M_2 and M_4, so $ZIIII|\varphi\rangle \in A_{-11-11}$. $YIIII$ anticommutes with M_1, M_3, M_4 and commutes with M_2, so $YIIII|\varphi\rangle \in A_{-11-1-1}$. And so on.

Summarising:

If a weight 1 error E occurs occurs on a single qubit, then measuring the resulting state $E|\varphi\rangle$ relative to the decomposition $\mathcal{H} = \overset{\perp}{\bigoplus} A_{ijk\ell}$ allows us to discover E, and since $E^2 = I$, applying E to the corrupted state allows us to recover the original state $|\varphi\rangle$ (even though we do not know it). Similarly, if a more general error of the form $\alpha I + \beta X + \gamma Z + \delta Y$ occurs on a single qubit, then applying the same measurement yields a state $E|\varphi\rangle$ with E being either the identity or a Pauli

error of weight exactly one, so E can be removed as before. We have a 1-error correcting quantum code (discovered independently by Bennet et al. and Laflamme et al. in 1996).

2 LDPC codes

2.1 Stabiliser codes

The previous code is an example of a *stabiliser code*, a space of quantum states stabilised by a group of Pauli errors called a *stabiliser group*. It is important that the stabilisers (the elements of the stabiliser group) commute. If they commute, their eigenspaces are orthogonal and we have a decomposition of the Hilbert space similar to the one above.

These codes come with a syndrome function. A syndrome is in $\{+1,-1\}^s$, with s the number of stabilisers that generate the group (the M_i), and we can measure that syndrome, which is an error pattern. The component i of the syndrome tells us if the ith operator commutes $EM_i = M_iE$ or anti-commutes $EM_i = -M_iE$ with the Pauli error pattern E.

In the real world we may not have a Pauli error, but when we measure the syndrome, we fall back on a state that is the corruption of the original state by a Pauli error.

The dimension of the code C is $\dim C = n - s = k$.

The minimal distance $d_{\min}$ is the smallest weight of an error pattern of syndrome 0 (that commutes with S) *but that is not in* S.

Contrary to the classical world, the errors in S don't hurt us. If $M \in S$, $M|\varphi\rangle = |\varphi\rangle$.

Example 2.1

In the 5-qubit code example, the dimension is 1 and the minimal distance is 3.

2.2 CSS codes

CSS (Calderbank, Schor, Steane) codes are stabiliser codes for which M_i have only I, X or only I, Z. So we can split the generators in two sets.

The matrices representing these two sets can be represented by binary matrices that must be orthogonal.

$$\begin{matrix} H_X \\ H_Z \end{matrix}\begin{bmatrix} & X & X & \\ & & & \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 1 & 1 \\ & & & \end{bmatrix} \Big)^{\perp}$$
$$\begin{bmatrix} & Z & Z & \\ & & & \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 1 & 1 \\ & & & \end{bmatrix}$$

So we have two classical codes $\mathcal{C}_X$ and $\mathcal{C}_Z$, defined by parity-check matrices H_X and H_Z respectively; and the X-distance d_X of the quantum code is the minimal weight of elements of $\mathcal{C}_X$ that are not in $\mathcal{C}_Z^{\perp}$ (i.e. not generated by rows of H_Z). Similarly, the Z-distance d_Z is defined as the minimal weight of elements of $\mathcal{C}_Z$ that are not in $\mathcal{C}_X^{\perp}$. The quantum minimum distance is the minimum of d_X and d_Z, $d_{\min} = \min(d_X, d_Z)$.

An error pattern can be decomposed as:

$$E = IIIXXXZZZYY$$
$$XXX \qquad XX$$
$$ZZZ\ ZZ$$

The following parity check matrix gives a first example of a CSS code with $k = 1$ and $d_{\min} = 3$.

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$H_X = \begin{bmatrix} X & I & I & I & X & X & X \\ I & X & I & X & I & X & X \\ I & I & X & X & X & I & X \end{bmatrix} \qquad H_Z = \begin{bmatrix} Z & I & I & I & Z & Z & Z \\ I & Z & I & Z & I & Z & Z \\ I & I & Z & Z & Z & I & Z \end{bmatrix}$$

This is the Steane code. It is the smallest 1-error correcting CSS code: it requires therefore 7 qubits instead of 5 for the 5 qubit (non CSS) code.

We have ways to tranform any stabiliser code into a CSS code, with slightly worse parameters, so people often concentrate on the simpler CSS structure.

2.3 Low Density Parity Check codes

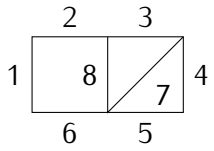
To measure whether a quantum state is in the +1 or -1 eigenspace of a stabiliser, one needs to access w qubits, where w is the weight of the stabiliser. In the quantum world, any measurement is a big deal and the larger the weight w, the more difficult it is to make the measurement reliable. To have reliable syndrome measurements, one wishes therefore for bounded weight stabilisers, represented by sparse matrices. These are Quantum LDPC (Low Density Parity-Check) codes.

We have seen an example of a classical error-correcting code that can be directly transposed into a useful quantum code. But in the LDPC case this is not straightforward, because an ordinary classical LDPC code has the property that any codeword c has a large weight. But in the CSS case we need two sparse matrices H_X and H_Z whose rows are orthogonal to each other, so we need LDPC codes that actually have many low-weight codewords: classical coding theory does not readily provide such examples.

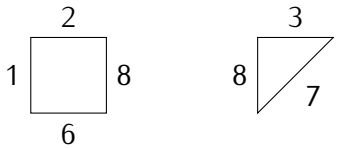
The "most LDPC" (sparsest) that we can hope for consists of matrices that have two 1 per column (matrices with weight 1 don't give good codes)

$$H_X, H_Z \begin{bmatrix} 1 & \\ 1 & \end{bmatrix}$$

They give cycle codes of graphs. Every row of the matrix is a vertex and every column is an edge between two vertices.



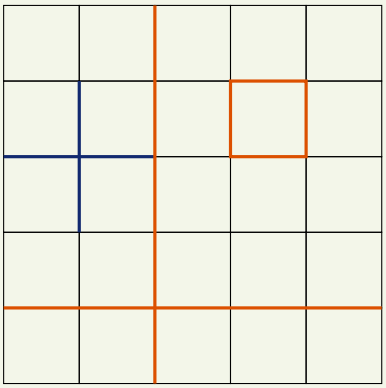
In the above example, the graph has 8 edges and several cycles, so it yields a cycle code of length 8.



For constant rate, cycle codes have $d_{\min} \leqslant \log n$. This is not very impressive, but cycle codes are still interesting for several reasons, even though they are not the best codes. In particular, complete decoding can be done in deterministic polynomial time. Complete decoding consists of always outputing a closest codeword to an input vector.

Example 2.2 The Kitaev toric code

Take a regular graph of degree 4.



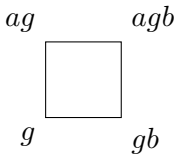
$$H_X = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & \dots & 0 \\ & & & & & & & \end{bmatrix}$$

$$H_Z = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 & \dots & \\ & & & & & & & \end{bmatrix}$$

$k = 2$, $d_{\min} \approx \sqrt{N}$

Square complexes. The Kitaev code is based upon a *square complex*.

Recent constructions of good quantum LDPC codes involve more intricate square complexes, namely *left-right Cayley complexes*. By using a group G that is not necessarily abelian, we can build a graph with vertices $g \in G$ and squares such that



where a is chosen from a set of left generators and b from a set of right generators. For example, when the group is the additive group $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, with left generators $\pm(1,0)$ and right generators $\pm(0,1)$ we recover the Kitaev square complex. For a presentation of those new codes, see the C2 talk
`https://indico.math.cnrs.fr/event/9364/attachments/4367/6474/Zemor_Gilles.pdf`