Introduction to Quantum Error Correction

Gilles Zémor

Nomade Lodge, May 2016

1 Qubits, quantum computing

1.1 Qubits

A *qubit* is a mathematical description of a particle, e.g. a photon, it is a vector of unit norm in a Hilbert space $\mathcal{H}$ of dimension 2. It is customary to give oneself a basis of this space, that is written in Dirac notation $(|0\rangle, |1\rangle)$ rather than the usual mathematical notation (e_0, e_1). A qubit is therefore a quantity expressed as

$$\alpha|0\rangle + \beta|1\rangle$$

with $|\alpha|^2 + |\beta|^2 = 1$. The physical state of n particles is described by a vector in the Hilbert space $\mathcal{H}^{\otimes n}$, which consists of all complex linear combinations of products $|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$, where $|x_i\rangle$ ranges over the two basis vectors of the i-th copy of the Hilbert space $\mathcal{H}$. Typically one uses the convention $x_i \in \{0, 1\}$ and the basis vectors of the 2^n-dimensional complex vector space $\mathcal{H}^{\otimes n}$ are written, to lighten notation as

$$|x_1\rangle|x_2\rangle \cdots |x_n\rangle \quad \text{or simply as} \quad |x_1 x_2 \ldots x_n\rangle.$$

This basis of $\mathcal{H}^{\otimes n}$ will be referred to as the *computational basis*. Quantum states are described by vectors of unit norm in $\mathcal{H}^{\otimes n}$. Quantum states are also not changed by multiplication by a complex number of modulus 1, so that strictly speaking quantum states are unit vectors of $\mathcal{H}^{\otimes n}$ modulo the multiplicative group of complex numbers of unit norm.

Unitary transformations. A quantum state $|\psi\rangle$ may be changed into another quantum state $|\psi'\rangle$ by any *unitary transformation* U of the Hilbert space $\mathcal{H}^{\otimes n}$. A unitary transformation is an operator of $\mathcal{H}^{\otimes n}$ that preserves the hermitian inner product. In other words it is a linear transformation in $\mathcal{H}^{\otimes n}$ that takes the

computational basis to any other orthonormal basis. Quantum physics does not allow any non-unitary transformation to act on n-qubit states that are perfectly isolated from the outside environment. Common and useful operators on one qubit are the Hadamard operator H and the Pauli operators X, Z whose matrices are, in the computational basis:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

One-qubit operators can be combined by tensor product to create n-qubit operators. If U_1 and U_2 are one-qubit operators then $U_1 \otimes U_2$ is naturally defined to transform $|x\rangle \otimes |y\rangle$ into $U_1|x\rangle \otimes U_2|y\rangle$. For example

$$\begin{aligned}(I \otimes H \otimes I)|000\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}(|000\rangle + |010\rangle).\end{aligned}$$

and

$$(H \otimes H)|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

Two particles that do not physically perturb each other and are individually represented by one-qubit states $|\psi\rangle$ and $|\psi'\rangle$ can be considered together in $\mathcal{H}^2$. In this case their state is naturally $|\psi\rangle \otimes |\psi'\rangle$. There are of course non-product states in $\mathcal{H}^{\otimes 2}$, and these can be obtained from a product state by applying a non-product unitary transformation. The most common 2-qubit transformation that is not a product of 1-bit transformation is the CNOT (Controlled Not) transformation that transforms the computational basis vector $|xy\rangle$ into $|x(x+y)\rangle$ for any $x, y \in \{0, 1\}$. For example, if we apply first the product unitary $H \otimes I$, and then CNOT, to the product state $|00\rangle$ we get

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

which is not a product state. two (or more) qubits, or particles, that are in a non-product states are said to be *entangled*.

Quantum measurements. A quantum measurement of a quantum state $|\psi\rangle$ is associated to a self-adjoint operator on $\mathcal{H}^{\otimes n}$ with some spectrum Λ and set of eigenspaces $(E_\lambda)_{\lambda \in \Lambda}$. Let

$$|\psi\rangle = \sum_{\lambda \in \Lambda} |\psi_\lambda\rangle$$

be the decomposition of the vector $|\psi\rangle$ into a sum of eigenvectors, $|\psi_\lambda\rangle \in E_\lambda$. The effect of the measurement is random: it randomly transforms the original

vector $|\psi\rangle$ into one of the $|\psi_\lambda\rangle$'s, with probability

$$\langle\psi_\lambda|\psi_\lambda\rangle = \||\psi_\lambda\rangle\|^2.$$

Furthermore, the associated eigenvalue λ is a visible result yielded by the measuring device, so that it becomes known in which eigenspace E_λ lives the new quantum state $\frac{1}{\langle\psi_\lambda|\psi_\lambda\rangle^{1/2}}|\psi_\lambda\rangle$.

This may seem to contradict the principle by which only unitary operations are allowed on the space $\mathcal{H}^{\otimes n}$. But this principle only applies when there is no intrusion by the environment. A quantum measurement however, *is* an intrusion by the environment.

The actual eigenvalue λ is of no practical use to us, so we may think of a measurement slightly more abstractly simply as a decomposition of $\mathcal{H}^{\otimes n}$ into an orthogonal direct sum of subspaces

$$\mathcal{H}^{\otimes n} = A_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} A_k.$$

The result of the measurement is, with probability p_i, the renormalised vector $\Pi_i|\psi\rangle$ where Π_i is the orthogonal projection onto the subspace A_i. The value of the probability p_i is the squared hermitian norm of the projected vector $\Pi_i|\psi\rangle$.

For a example, measuring a single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with respect to the orthogonal decomposition of $\mathcal{H}$ given by the computational basis $(|0\rangle, |1\rangle)$ is $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$. The measurement also tells us whether we have obtained $|0\rangle$ or $|1\rangle$. When we simply speak of measuring the qubit, it means by default with respect to the basis $(|0\rangle, |1\rangle)$.

For a 2-qubit state in $\mathcal{H}^{\otimes 2}$, measuring the first (say) qubit means measuring according to the decomposition

$$H^{\otimes 2} = A_0 \overset{\perp}{\oplus} A_1$$

where A_0 is generated by the vectors $|00\rangle$ and $|01\rangle$, while A_1 is generated by the vectors $|10\rangle$ and $|11\rangle$. If we measure the first qubit of a product state

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\alpha'_0|0\rangle + \alpha'_1|1\rangle)$$

we will get $|i\rangle \otimes (\alpha'_0|0\rangle + \alpha'_1|1\rangle)$, for $i = 0, 1$, with probability $|\alpha_i|^2$. If we measure the second qubit, we will get $|\psi\rangle \otimes |j\rangle$ with probability $|\alpha'_j|^2$, where $|\psi\rangle$ is either the original state $\alpha_0|0\rangle + \alpha_1|1\rangle$ of the first qubit if the measurement occurs *before* we measure the first qubit, or $|\psi\rangle = |i\rangle$ if the measurement occurs *after* we measure the first qubit. Our point is that measuring the first qubit does not change what is going to happen to the second qubit (and vice versa). However, if instead of starting from a product state we start from an entangled state

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

the situation is very different. Measuring the first qubit will yield $|00\rangle$ (say). But then measuring the second qubit will necessarily leave the state unchanged and also yield $|00\rangle$. The outcome $|11\rangle$ has become no longer possible. This is one of the (many) paradoxes of quantum physics.

1.2 Quantum Computation.

Let F be a function from $\{0,1\}^n$ to $\{0,1\}^n$. Suppose furthermore that F is one-to-one. Then F extends naturally into a unitary operator on $\mathcal{H}^{\otimes n}$ that takes $|x\rangle$ to $|F(x)\rangle$ for every $x \in \{0,1\}^n$. In classical computing, if we are given a circuit that computes F, then we can only feed it one input x at time, after which it will output $F(x)$. In quantum computing we can feed essentially the same circuit with an input of the form

$$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$$

and the circuit will "output"

$$\sum_{x\in\{0,1\}^n} \alpha_x |F(x)\rangle. \tag{1}$$

We can therefore think of the quantum version of the circuit as having computed *simultaneously* all values $F(x)$, $x \in \{0,1\}^n$. Preparing an input state $|\psi\rangle$ that is a superposition of all "classical" states $|x\rangle$, $x \in \{0,1\}^n$, is not very difficult: for example, starting from the state $|00\cdots0\rangle$ and applying a Hadamard operator to every qubit yields

$$\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle.$$

The real problem is whether we can extract anything useful from the output state (1) by a clever quantum measurement. It turns out that yes, in some cases the parallel computation of (1) can be exploited. We will just give a small example that gives an idea of how quantum computing can work.

Deutch's problem. This problem has a slightly artificial flavour to it, but it serves to highlight the potential of quantum computation. Suppose we are given a device, that we can think of as a black box, that computes some unknown one-bit boolean function $f : \{0,1\} \to \{0,1\}$. The only way we can learn something about what this function does is by querying the black box, i.e. feeding it some input value and observing the output. Suppose now we wish to learn whether the function f is constant on $\{0,1\}$ or not. With classical computing, there is no way we can learn this by querying the black box only once, we need to try the two different input values for f. If we are allowed to use a quantum superposition of

classical states however, we may learn whether f is constant with only *one* query. First, the black box that computes f has to be made into a *reversible* black box, i.e. a classical circuit that is a one-to-one function between inputs and outputs, in order for it to be naturally extended into a unitary transformation. For this we consider the black box that computes the 2-bit function $F : \{0,1\}^2 \to \{0,1\}^2$

$$(x, y) \mapsto (x, y + f(x))$$

which is bijective since $F^2 = I$. Note that as before, a single classical query to F

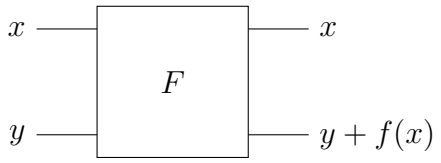

Figure 1: reversible black box that computes f

cannot determine whether f is constant on $\{0,1\}$ or not. Now consider the black box F extended to a unitary transformation. Let us feed F with the input state

$$\begin{aligned}|\psi\rangle &= H^{\otimes 2}|01\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle(|0\rangle - |1\rangle).\end{aligned}$$

The unitary F now outputs:

$$\begin{aligned}F|\psi\rangle &= \frac{1}{2}|0\rangle(|f(0)\rangle - |1 + f(0)\rangle) + \frac{1}{2}|1\rangle(|f(1)\rangle - |1 + f(1)\rangle) \\ &= \frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}(-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).\end{aligned}$$

In other words we have

$$F|\psi\rangle = \begin{cases} \pm H|0\rangle \otimes H|1\rangle & \text{if } f \text{ is constant} \\ \pm H|1\rangle \otimes H|1\rangle & \text{otherwise.} \end{cases}$$

Applying again $H^{\otimes 2}$ we therefore get

$$H^{\otimes 2}F|\psi\rangle = \begin{cases} \pm|01\rangle & \text{if } f \text{ is constant} \\ \pm|11\rangle & \text{otherwise.} \end{cases}$$

We then simply measure the first qubit. If f is constant the measurement yields $|0\rangle$ with probability 1: if f is non-constant the measurement yields $|1\rangle$ with probability 1.

2 Quantum error correction

The most natural and simple way of protecting a classical bit $b \in \{0,1\}$ from a Hamming error is to use the repetition code that encodes 0 to 000 and 1 to 111. Consider now a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. We may try a similar procedure by first appending to $|\psi\rangle$ two extra qubits in the zero state $|0\rangle$ which gives us

$$|\psi\rangle \otimes |0\rangle \otimes |0\rangle = \alpha|000\rangle + \beta|100\rangle.$$

Next, it is easy to devise a unitary transformation of $\mathcal{H}^{\otimes 3}$ that takes $|000\rangle$ to $|000\rangle$, takes $|100\rangle$ to $|111\rangle$, and which, when applied to our tensor product state, gives the encoded state

$$\alpha|000\rangle + \beta|111\rangle.$$

Now suppose an "error" occurs. In the classical case, for binary vectors, Hamming errors mean that individual bits may be flipped to their opposite value. However when we use this model we forget that the physical object underlying the zeros and ones undergoes some continuous transformation, and when we make a measurement to extract bits from this physical object, we may extract these bits wrongly, resulting in Hamming errors. In the quantum case something (somewhat) similar happens. A quantum measurement is applied to the quantum state (which in effect amounts to the syndrome computations that we shall describe below) and this quantum measurement transforms the real-world error that the quantum state is subject to into a discrete version of the error. This discrete error model affects every qubit independently, and either leaves it untouched, or applies an $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ operator to it, or applies a $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ operator, or both simultaneously, i.e. applies XZ. We therefore need to protect against two types of errors on every individual qubit, namely X-errors and Z-errors, as opposed to the unique Hamming-error type in the classical case.

Going back to our encoded state $\alpha|000\rangle + \beta|111\rangle$, suppose an X-error occurs on the second qubit (say). X-errors are very similar to Hamming errors (and are sometimes called bit-flips): indeed, an X-error on the i-th qubit acts on every vector $|x\rangle$ of the computational basis by flipping the i-th bit of x. So in our example the error gives us the state:

$$|\phi\rangle = \alpha|010\rangle + \beta|101\rangle.$$

In the classical Hamming case what would we do ? We would choose a parity-check matrix $\mathbf{H} = \left[\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right]$ (say) for the repetition code $\{(000),(111)\}$, and apply it to either (010) or (101), giving us the syndrome vector $\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ which tells us that an error has occurred on the second bit. We would then correct the error. Well, in the quantum case we can do pretty much the same thing. We use two auxiliary qubits initialised in the $|0\rangle$ state. Denoting by $\sigma(x)$ the syndrome of $x \in \mathbb{F}_2^3$

relative to the parity-check matrix $\mathbf{H}$, we have that the mapping

$$(x, 00) \mapsto (x, \sigma(x))$$

is one-to-one and can be extended into a one-to-one mapping of $\mathbb{F}_2^5$ to $\mathbb{F}_2^5$, which in turn yields a unitary transformation U of $\mathcal{H}^{\otimes 5}$. Applying U to the quantum state

$$(\alpha|010\rangle + \beta|101\rangle) \otimes |00\rangle$$

gives

$$(\alpha|010\rangle + \beta|101\rangle) \otimes |11\rangle.$$

We now measure the last two qubits: this means that we apply the quantum measurement relative to the orthogonal decomposition

$$\mathcal{H}^{\otimes 5} = A_{00} \overset{\perp}{\oplus} A_{01} \overset{\perp}{\oplus} A_{10} \overset{\perp}{\oplus} A_{11}$$

where A_{ij} is the subspace generated by the vectors $|xij\rangle$ of the computational basis, $x \in \{0,1\}^3$. This measurement gives us the syndrome value (11), from which we deduce that the X-error has occurred on the second qubit. We can now throw away the last two qubits (which does not hurt since we have a tensor product state) and we apply to our quantum state $|\phi\rangle$ an X operator on the second qubit which, since $X^2 = I$, gives us back our original state

$$\alpha|000\rangle + \beta|111\rangle.$$

Using two auxiliary qubits was something of an artifact to help us mimic multiplication by the matrix $\mathbf{H}$. We could do without the auxiliary qubits by using the decomposition of $\mathcal{H}^{\otimes 3}$

$$\mathcal{H}^{\otimes 3} = B_{00} \overset{\perp}{\oplus} B_{01} \overset{\perp}{\oplus} B_{10} \overset{\perp}{\oplus} B_{11}$$

where B_{00} is the subspace generated by $|000\rangle, |111\rangle$, B_{01} is the subspace generated by $|100\rangle, |011\rangle$, B_{10} is the subspace generated by $|001\rangle, |110\rangle$, and B_{11} is the subspace generated by $|010\rangle, |101\rangle$. Measuring relative to this decomposition also gives us the syndrome value, i.e. tells us where the X-error occurred.

Now suppose a Z-error occurred on the second qubit. This transforms the original state into

$$\alpha|000\rangle - \beta|111\rangle. \tag{2}$$

This type of error, sometimes called a "phase-flip", has no immediate equivalent in classical error-correction. The bad news is that the Z-error not only transforms the original quantum state into the different state (2) (which would also have been reached if the Z-error had been on the first or the third qubit), this time there is no measurement that will tell us that such a Z-error occurred.

So our litte "repetition" quantum code can correct one X-error but can't deal with Z-errors. If we wanted to correct Z-errors but could afford not to be bothered by X-errors, we could modify our encoding by applying a Hadamard operator H to every qubit: this would transform the quantum state $\alpha|000\rangle + \beta|111\rangle$ to

$$\alpha|+++\rangle + \beta|---\rangle$$

where

$$|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

and $|+++\rangle$ stands for $|+\rangle \otimes |+\rangle \otimes |+\rangle$, and $|---\rangle$ stands for $|-\rangle \otimes |-\rangle \otimes |-\rangle$. Now $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$. Therefore the effect of Z-errors on this encoding is exactly the same as the effect of X-errors on the original computational basis. The technique described above to correct X-errors can therefore be transposed to correct Z-errors. But this encoding suffers from the same flaw as the $\alpha|000\rangle + \beta|111\rangle$ encoding, namely it can only deal with one type of error. However this way of dealing with Z-errors suggests ways to deal with both types of errors simultaneously. The Shor 9-qubit code combines both previous encodings by encoding $\alpha|0\rangle + \beta|1\rangle$ to

$$\alpha\frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$
$$+\beta\frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle).$$

The encoded state is a complex linear combination of basis vectors of the form $|x\rangle$, with x an 9-bit binary vector belonging to the binary linear code of dimension 3 generated by

$$(111000000), (000111000), (000000111).$$

It should be clear that a syndrome-measuring technique similar to those described above will detect whether an X-error has occurred on coordinate i for any $i = 1..9$. Such a measurement will also not interfere with any possible Z-error, since Z-errors only change signs, but do not switch basis vectors of the computational basis.

Once we have removed a possible X-error by reapplying the X-operator on the relevant qubit, we are left to deal with the effect of a Z-error on the original state which can be rewritten as

$$\alpha|+\rangle|+\rangle|+\rangle + \beta|-\rangle|-\rangle|-\rangle$$

where

$$|+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle).$$

Since $Z|+\rangle = |-\rangle$, we are in a similar situation as when the state $\alpha|0\rangle + \beta|1\rangle$ was encoded by the 3-qubit state $|+++\rangle + \beta|---\rangle$. The effect of a Z-error on either the first or the second or the third qubit yields $\alpha|-++\rangle + \beta|+--\rangle$, a Z-error on either of the qubits $4, 5, 6$ gives $\alpha|+-+\rangle + \beta|-+-\rangle$, and a Z-error on qubits $6, 7$ or 8 gives $\alpha|++-\rangle + \beta|--+\rangle$. The orthogonal decomposition of the Hilbert space

$$\mathcal{H}^{\otimes 9} = E_0 \overset{\perp}{\oplus} E_1 \overset{\perp}{\oplus} E_2 \overset{\perp}{\oplus} E_3 \overset{\perp}{\oplus} F$$

where

$$\begin{aligned}
E_0 &\quad \text{is generated by} \quad |+++\rangle, |---\rangle \\
E_1 &\quad \text{is generated by} \quad |-++\rangle, |+--\rangle \\
E_2 &\quad \text{is generated by} \quad |+-+\rangle, |-+-\rangle \\
E_3 &\quad \text{is generated by} \quad |++-\rangle, |--+\rangle \\
F &= (E_0 + E_1 + E_2 + E_3)^{\perp}
\end{aligned}$$

yields a measurement that tells us exactly whether no Z-error occurred (the state is in E_0), or whether a Z-error occurred on the first, second or third block of 3 qubits (the state is in E_1, E_2, E_3 respectively). In the latter case we apply the Z-operator to either one of the qubits in the corresponding block to remove the error and recover the initial state.

3 CSS codes

We now investigate a more systematic way of encoding quantum states. Let C_1 and C_2 be two binary linear codes of length n such that $C_2 \subset C_1$. The associated CSS (Calderbank-Shor-Steane) code encodes k qubits, with $k = \dim C_1/C_2 = \dim C_1 - \dim C_2$. Its encoded states are all complex linear combinations of the form

$$|\psi\rangle = \sum_x \alpha_x |x + C_2\rangle, \quad \alpha_x \in \mathbb{C} \tag{3}$$

where we use the shorthand

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

and where x ranges over a subset of $|C_1|/|C_2|$ vectors of C_1, each one of which belongs to a distinct coset $x + C_2$ in C_1/C_2.

Before considering the error-correcting potential of this family of quantum codes, we need some preliminaries.

Let us introduce the following notation: to any binary vector $v \in \mathbb{F}_2^n$ we associate the unitary operator of $\mathcal{H}^{\otimes n}$

$$X^v = X^{v_1} \otimes X^{v_2} \otimes \cdots \otimes X^{v_n}$$

and Z^v, defined similarly. The quantities $X^u Z^v$ and $Z^u X^v$ should be understood to mean:

$$\begin{aligned} X^u Z^v &= X^{u_1} Z^{v_1} \otimes X^{u_2} Z^{v_2} \otimes \cdots \otimes X^{u_n} Z^{v_n} \\ Z^u X^v &= Z^{u_1} X^{v_1} \otimes Z^{u_2} X^{v_2} \otimes \cdots \otimes Z^{u_n} X^{v_n}. \end{aligned}$$

From $XZ = -ZX$, $HX = ZH$, $XH = HZ$, and the definition of $X^u Z^v$ and $Z^u X^v$ we have the following straightforward properties:

Lemma 1. *We have:*

(i) $X^u Z^v = (-1)^{(u\,|\,v)} Z^v X^u$,

(ii) $H^{\otimes n} X^u = Z^u H^{\otimes n}$ *and* $H^{\otimes n} Z^u = X^u H^{\otimes n}$,

(iii) for any $u, x \in \mathbb{F}_2^n$, $Z^u |x\rangle = (-1)^{(u\,|\,x)} |x\rangle$.

The next Lemma is crucial to understanding the structure of CSS codes.

Lemma 2. *For any linear code* C *in* $\mathbb{F}_2^n$*, and using the notation*

$$|C\rangle = \frac{1}{|C|^{1/2}} \sum_{x \in C} |x\rangle,$$

we have

$$H^{\otimes n} |C\rangle = |C^\perp\rangle.$$

Proof. We have, for every $y \in \mathbb{F}_2^n$,

$$\begin{aligned} H^{\otimes n} |y\rangle &= \frac{1}{2^{n/2}} \bigotimes_{i=1}^{n} (|0\rangle + (-1)^{y_i} |1\rangle) \\ &= \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{(y\,|\,x)} |x\rangle \end{aligned}$$

hence

$$\begin{aligned} H^{\otimes n}|C\rangle &= H^{\otimes n}\frac{1}{|C|^{1/2}}\sum_{y\in C}|y\rangle \\ &= \frac{1}{2^{n/2}}\frac{1}{|C|^{1/2}}\sum_{y\in C}\sum_{x\in\mathbb{F}_2^n}(-1)^{(y\,|\,x)}|x\rangle \\ &= \frac{1}{(\sqrt{2})^{n+\dim C}}\sum_{x\in\mathbb{F}_2^n}\left(\sum_{y\in C}(-1)^{(y\,|\,x)}\right)|x\rangle. \end{aligned}$$

Now any linear form which is non-zero on a binary vector space takes the values 0 and 1 an equal number of times, hence for any $x \notin C^\perp$

$$\sum_{y\in C}(-1)^{(y\,|\,x)} = 0$$

and

$$\begin{aligned} H^{\otimes n}|C\rangle &= \frac{1}{(\sqrt{2})^{n+\dim C}}\sum_{x\in C^\perp}|C||x\rangle = \frac{1}{(\sqrt{2})^{n+\dim C-2\dim C}}\sum_{x\in C^\perp}|x\rangle \\ &= \frac{1}{\sqrt{2^{n-\dim C}}}\sum_{x\in C^\perp}|x\rangle \\ H^{\otimes n}|C\rangle &= |C^\perp\rangle. \end{aligned}$$

∎

Definition 3. *If C is a linear code of $\mathbb{F}_2^n$ of dimension k, and if $\mathbf{H}$ is an $(n-k)\times n$ parity-check matrix for C, let us associate to them the quantum measurement associated to the orthogonal decomposition*

$$\mathcal{H} = \bigoplus_{s\in\mathbb{F}_2^{n-k}}^{\perp} A_s$$

where A_s is the subspace generated by all computational basis vectors $|z\rangle$, for z a binary vector of syndrome s. In other words A_s is generated by all $|z\rangle$ for z ranging over some coset $x + C$, with x of syndrome s. We call this quantum measurement the syndrome measurement *relative to C (and $\mathbf{H}$).*

Since all cosets modulo C are disjoint, the associated subspaces A_s of the Hilbert space are orthogonal. Note in particular that the effect of a pattern X^e of X-errors on a state $|\psi\rangle$ in A_0 takes it into the subspace A_s where s is the syndrome of the binary vector e. Note also that Z-errors applied to states within a subspace A_s may modify the state but leave it within A_s.

Let us now consider the action of a mixed pattern of X-errors and Z-errors on a state $|\psi\rangle$ given by (3). This yields a state of the form

$$X^e Z^f |\psi\rangle = \sum_{x \in C_1/C_2} \alpha_x X^e Z^f |x + C_2\rangle \tag{4}$$

where, abusing notation, we identify the cosets of C_1/C_2 with some subset of representatives in C_1. As just discussed above, we may, without modifying the quantum state, measure the syndrome of the binary n-tuple e relative to some parity-check matrix of C_1, since the original state $|\psi\rangle$ is in the subspace A_0 associated to C_1. If we suppose that the classical binary code C_1 has the ability to recover the binary word e from its syndrome, then we may apply the unitary transformation X^e to the quantum state (4) to erase the effect of the X-errors on the original state $|\psi\rangle$ and obtain

$$Z^f |\psi\rangle = \sum_{x \in C_1/C_2} \alpha_x Z^f |x + C_2\rangle = \sum_x \alpha_x Z^f X^x |C_2\rangle.$$

To recover the original state we now only need to extract the binary pattern f from the modified quantum state. To do this we first apply the Hadamard transform $H^{\otimes n}$. We get, applying property (ii) of Lemma 1 and Lemma 2:

$$\begin{aligned} H^{\otimes n} Z^f |\psi\rangle &= \sum_x \alpha_x X^f Z^x H^{\otimes n} |C_2\rangle \\ &= \sum_x \alpha_x X^f Z^x |C_2^\perp\rangle. \end{aligned}$$

Now we see that, by the same argument that followed Definition 3, that the quantum measurement relative to the code $C_2^\perp$ will not modify the quantum state and will yield the syndrome for the code $C_2^\perp$ of the binary vector f. If it is possible to recover the binary error f from its syndrome, then we may reapply the Hadamard transform $H^{\otimes n}$ to the present quantum state $H^{\otimes n} Z^f |\psi\rangle$, which gives back, since $H^2 = I$, the modified state $Z^f |\psi\rangle$. Finally, applying Z^f yields the original quantum state $|\psi\rangle$.

We have just proved:

Theorem 4. *Let C_1 and C_2 be two binary linear codes such that $C_2 \subset C_1$. If e is a binary error pattern that can be recovered from its syndrome by the code C_1, and if f is a binary error pattern that can be recovered from its syndrome by the binary code $C_2^\perp$, then the quantum error pattern $X^e Z^f$ can be corrected by the CSS quantum code associated to the pair of binary codes (C_1, C_2).*

Example: the Steane code. Take C_1 to be the $[7, 4, 3]$ Hamming code and $C_2 = C_1^\perp$ which happens to be included in C_1. Both C_1 and C_2 can correct an arbitrary Hamming error, therefore the associated CSS code can correct an arbitrary X-error and an arbitrary Z-error (even if they occur simultaneously).

Stabilising a CSS code. Let us make some remarks that will pave the way for a more general class of quantum error correcting codes.

Let $\mathbf{H}_X$ be a parity-check matrix of C_1 and let $\mathbf{H}_Z$ be a parity-check matrix of $C_2^\perp$. The condition $C_2 \subset C_1$ is equivalent to saying that the binary vector space generated by the rows of $\mathbf{H}_X$ and the binary vector space generated by the rows of $\mathbf{H}_Z$ are orthogonal in $\mathbb{F}_2^n$. A CSS code can thus be defined by a such a pair $(\mathbf{H}_X, \mathbf{H}_Z)$ of mutually orthogonal parity-check matrices, and the associated quantum code has the property that for any pattern of errors $X^e Z^f$, the syndromes $\mathbf{H}_X e^T$ and $\mathbf{H}_Z f^T$ can be computed. This equivalent way of presenting a CSS code highlights the symmetrical roles of the X-error correction, provided by $\mathbf{H}_X$, and the Z-error correction, provided by $\mathbf{H}_Z$. In particular if we have a code C_1 such that $C_1^\perp \subset C_1$, then we can take $\mathbf{H}_X = \mathbf{H}_Z = \mathbf{H}$, were $\mathbf{H}$ is a parity-check matrix of C_1. The Steane code is an example of a CSS code obtained in this way.

Now let us make the following remark. Let e be any binary vector belonging to C_2, i.e. generated by the rows of $\mathbf{H}_Z$. Then clearly $X^e|x + C_2\rangle = |e + x + C_2\rangle = |x + C_2\rangle$, for any binary vector x. In particular the operator X^e *stabilises* any quantum state $|\psi\rangle$ of the form (3), i.e. leaves it invariant. Similarly, suppose $f \in \mathbb{C}_1^\perp$, equivalently f is generated by the rows of $\mathbf{H}_X$. Then, from property (iii) of Lemma 1,

$$Z^f|y\rangle = (-1)^{(f\,|\,y)}|y\rangle$$

for any $y \in \mathbb{F}_2^n$, hence, for any $x \in C_1$ we have that every binary vector y in the coset $x + C_2$ is in C_1 and $(f\,|\,y) = 0$, which implies

$$Z^f|x + C_2\rangle = |x + C_2\rangle.$$

Therefore $Z^f|\psi\rangle = |\psi\rangle$ for any quantum state $|\psi\rangle$ of the form (3).

We have just noticed that for $e \in C_2$ and $f \in C_1^\perp$, any quantum error pattern of the form $X^e Z^f$ stabilises the quantum states of the quantum CSS code. Furthermore, since e and f are orthogonal vectors in $\mathbb{F}_2^n$, property (i) of Lemma 1, implies

$$X^e Z^f = (-1)^{(e\,|\,f)} Z^f X^e = Z^f X^e.$$

In particular, any two stabilising patterns $X^e Z^f$ and $X^{e'} Z^{f'}$ for $e, e' \in C_2$ and $f, f' \in C_1^\perp$, commute. Therefore, the set of stabilising patterns $X^e Z^f$ form an *abelian* group isomorphic to $C_2 \times C_1^\perp$. It is natural to ask whether the set of quantum states stabilised by this group of operators is exactly the set quantum states (3). It turns out the answer is yes, and that more general quantum codes can be defined as the subspace of quantum states stabilised by some abelian subgroup of the group of error patterns of the form $X^e Z^f$, This is the object of the next section.

4 Stabiliser Codes

Let us start with an example of a non-CSS quantum code. Consider the following four operators on $\mathcal{H}^{\otimes 5}$:

$$\begin{aligned} M_1 &= X \otimes Z \otimes Z \otimes X \otimes I \\ M_2 &= I \otimes X \otimes Z \otimes Z \otimes X \\ M_3 &= X \otimes I \otimes X \otimes Z \otimes Z \\ M_4 &= Z \otimes X \otimes I \otimes X \otimes Z \end{aligned}$$

It is easily checked that M_1, M_2, M_3, M_4 all commute, so that they generate an abelian group $\mathbb{S}$ of order 16. Consider now the subspace C of states of $\mathcal{H}^{\otimes 5}$ that are stabilised by $\mathbb{S}$. The space C is non-empty, indeed it contains all complex linear combinations

$$\alpha_0|\psi_0\rangle + \alpha_1|\psi_1\rangle$$

where

$$\begin{aligned} |\psi_0\rangle &= \sum_{M \in S} M|00000\rangle \\ |\psi_1\rangle &= \sum_{M \in S} M|11111\rangle. \end{aligned}$$

That $|\psi_0\rangle$ and $|\psi_1\rangle$ are stabilised by $\mathbb{S}$ is self-evident: furthermore we notice that $|\psi_0\rangle$ is a linear combination of basis vectors $|x\rangle$ with x of even weight and $|\psi_1\rangle$ is a linear combination of basis vectors $|x\rangle$ with x of odd weight, so that $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal, and in particular linearly independent. That the space of states stabilised by $\mathbb{S}$ is exactly the space generated by $|\psi_0\rangle$ and $|\psi_1\rangle$ will become clear later on, see Theorem 8.

Now let $E = X^e Z^f$ be any quantum error pattern. Define the binary 4-tuple $\sigma(E) = s = (s_1, s_2, s_3, s_4)$ by

$$s_i = \begin{cases} 0 & \text{if} \quad EM_i = \quad M_i E \\ 1 & \text{if} \quad EM_i = -M_i E \end{cases}$$

for $i = 1, 2, 3, 4$. Now we notice, by exhaustively trying all 15 cases, that the function σ restricted to the 15 error patterns of weight 1, by which we mean the patterns of the form X^e, or Z^e, or $X^e Z^e$ with e a binary 5-tuple of Hamming weight 1, is in one-to-one correspondence with $\mathbb{F}_2^4 \setminus (0000)$. This means that if we could somehow find a quantum measurement that will extract $\sigma(E)$ from $E(\alpha_0|\psi_0\rangle + \alpha_1|\psi_1\rangle)$, then we can uncover any error pattern E of weight 1 that has been applied to the encoded quantum state, and remove it by applying E^{-1}.

It turns out that yes, such a quantum measurement exists. The function σ will be called a *syndrome* function. We now proceed to showing in all generality how syndromes can be measured. First we define general stabiliser groups.

The group of Pauli errors $\mathbb{G}_n$. The set of operators of $\mathcal{H}^{\otimes n}$ of the form $X^e Z^f$ forms a multiplicative group. We augment this group slightly by allowing multiplication by the complex number i, so that we also allow operators of the form $iX^e Z^f$. This augmented set forms a group denoted by $\mathbb{G}_n$ and is usually referred to as the Pauli group on n qubits. Strictly speaking, it makes no difference to a quantum state whether we apply to it an operator E or the operator iE, because quantum states are really defined modulo multiplication by complex numbers of modulus 1. The error operator XZ acting on one qubit can just as well be thought of as $ZX = -XZ$, or iXZ. However it will be technically helpful to define $Y = iXZ$ and distinguish it from XZ, because we have in particular $Y^2 = I$, while $(XZ)^2 = -I$. the usefulness of this distinction will be apparent shortly. We have $\mathbb{G}_n \simeq \{\pm 1, \pm i\} \times \{I, X, Y, Z\}^n$.

Definition 5. *A subgroup $\mathbb{S}$ of $\mathbb{G}_n$ is said to be admissible if $-1 \notin \mathbb{S}$.*

Remark: an admissible subgroup is abelian. Indeed, any two elements of $\mathbb{G}_n$ either commute or anticommute, meaning $EF = FE$ or $EF = -FE$. Also, for any $E \in \mathbb{G}_n$, $E^2 = \pm 1$, so if E, F belong to an admissible subgroup, then $E^2 = F^2 = 1$, and $EF = -FE$ implies $EFEF = -EF^2E = -1$, therefore there are no anticommuting pairs of elements in an admissible subgroup.

Definition 6. *A stabiliser code is the set of quantum states stabilised by an admissible subgroup of $\mathbb{G}_n$.*

Syndrome function. Let S be an admissible subgroup of $\mathbb{G}_n$ and let $\mathcal{C}$ be the associated stabiliser code. Let $M_1, M_2, \ldots, M_r$ be independent generators of $\mathbb{S}$: we have therefore $|\mathbb{S}| = 2^r$. We define the syndrome function

$$\begin{aligned} \sigma : \quad & \mathbb{G}_n \to \{0,1\}^r \\ & E \mapsto \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_r \end{pmatrix} \end{aligned}$$

with

$$s_i = \begin{cases} 0 & \text{if} \quad EM_i = \quad M_i E \\ 1 & \text{if} \quad EM_i = -M_i E \end{cases}$$

and proceed to show that, for any $|\psi\rangle \in \mathcal{C}$, the syndrome $\sigma(E)$ can be extracted from the state $E|\psi\rangle$ without modifying it.

For any $s \in \{0,1\}^r$, define the subspace of $\mathcal{H}^{\otimes n}$

$$\mathcal{C}(s) = \{|\psi\rangle,\ M_i|\psi\rangle = (-1)^{s_i}|\psi\rangle \text{ for } i = 1, \ldots r\}.$$

In particular $\mathcal{C}(0) = \mathcal{C}$. The following proposition shows that there exists a quantum measurement that extracts the syndrome.

Proposition 7. *The family of subspaces $(\mathcal{C}(s))_{s\in\{0,1\}^r}$ satisfies the following properties:*

1. *For any $E \in \mathbb{G}_n$ and any $|\psi\rangle \in \mathcal{C}$, we have $E|\psi\rangle \in \mathcal{C}(\sigma(E))$.*
2. *The Hilbert space $\mathcal{H}^{\otimes n}$ decomposes into the orthogonal direct sum:*

$$\mathcal{H}^{\otimes n} = \bigoplus_{s\in\{0,1\}^r}^{\perp} \mathcal{C}(s). \tag{5}$$

Proof. Let $s_i = \sigma(E)_i$. We have $M_i E|\psi\rangle = (-1)^{s_i} E M_i|\psi\rangle$ by definition of s_i, and by definition of $\mathcal{C}$ we have $M_i|\psi\rangle = |\psi\rangle$, hence $M_i E|\psi\rangle = (-1)^{s_i} E|\psi\rangle$ which proves point 1. We now prove point 2. Since $-1 \notin \mathbb{S}$ by definition of an admissible subgroup, we have $M_i^2 = I$ for any $i = 1 \dots r$. Therefore the unitary operator M_i has eigenvalues 1 and -1. Denote by $\mathcal{E}_1(M_i)$ and $\mathcal{E}_{-1}(M_i)$ the corresponding eigenspaces of M_i. Since the operators M_i commute, there is an orthogonal basis in which all the M_i are simultaneously diagonal. This implies in particular that we can write

$$\begin{aligned}
\mathcal{H}^{\otimes n} &= \mathcal{E}_1(M_1) \overset{\perp}{\oplus} \mathcal{E}_{-1}(M_1) \\
&= \mathcal{E}_1(M_1) \cap \mathcal{E}_1(M_2) \overset{\perp}{\oplus} \mathcal{E}_1(M_1) \cap \mathcal{E}_{-1}(M_2) \\
&\quad \overset{\perp}{\oplus} \mathcal{E}_{-1}(M_1) \cap \mathcal{E}_1(M_2) \overset{\perp}{\oplus} \mathcal{E}_{-1}(M_1) \cap \mathcal{E}_{-1}(M_2) \\
&\vdots \\
&= \bigoplus_{s\in\{0,1\}^r}^{\perp} \left(\bigcap_{i=1}^{r} \mathcal{E}_{(-1)^{s_i}}(M_i) \right)
\end{aligned}$$

and noticing that

$$\mathcal{C}(s) = \bigcap_{i=1}^{r} \mathcal{E}_{(-1)^{s_i}}(M_i)$$

proves point 2. ∎

Theorem 8. *If $\mathbb{S}$ is an admissible group with $|\mathbb{S}| = 2^r$, then the associated stabiliser code $\mathcal{C}$ has dimension $\dim_{\mathbb{C}} \mathcal{C} = 2^{n-r}$.*

Proof. It suffices to show that all spaces $\mathcal{C}(s)$ have the same dimension, since applying the decomposition (5) will then allow us to conclude. The first lines of the proof of Proposition 7 show that if $E \in \mathbb{G}_n$ has syndrome s, then the mapping $|\psi\rangle \mapsto E|\psi\rangle$ is one-to-one from $\mathcal{C}$ to $\mathcal{C}(s)$. It suffices therefore to show that for any $s \in \mathbb{F}_2^n$, there exists a Pauli error pattern E of syndrome $\sigma(E) = s$. By linearity of the syndrome function σ, it suffices to show that for any $i = 1 \dots r$,

there exists $E \in \mathbb{G}_n$ such that $\sigma(E)_i = 1$ and $\sigma(E)_j = 0$ for $j \neq i$. This last fact can be shown by an orthogonality argument. Error patterns of the form $X^e Z^f$ are clearly in one-to-one correspondence with couples $(e, f) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. Consider the bilinear form b:

$$\begin{aligned} (\mathbb{F}_2^n \times \mathbb{F}_2^n)^2 &\to \mathbb{F}_2 \\ ((e, f), (e', f')) &\mapsto (e \,|\, f') + (e' \,|\, f)\,. \end{aligned}$$

Property (i) of Lemma 1 easily shows that $X^e Z^f$ and $X^{e'} Z^{f'}$ commute if and only if $b((e, f), (e', f')) = 0$, i.e. (e, f) and (e', f') are orthogonal with respect to b.

Let us consider Pauli errors modulo $\{\pm 1, \pm i\}$, since multiplication by these elements does not change commutation/anticommutation properties, and use the idenfication

$$\mathbb{G}_n / \{\pm 1, \pm i\} \xrightarrow{\sim} \mathbb{F}_2^n \times \mathbb{F}_2^n$$

so that we allow ourselves to write $M \perp_b N$ for $M, N \in \mathbb{G}_n$. Let $\mathbb{S}_i$ be the subgroup of $\mathbb{S}$ generated by $\{M_1, \ldots, M_r\} \setminus \{M_i\}$. We have $\mathbb{S}_i \subsetneq \mathbb{S}$, and since the bilinear form b is non-degenerate, we have $\mathbb{S}^{\perp_b} \subsetneq \mathbb{S}_i^{\perp_b}$. Any element E in $\mathbb{S}_i^{\perp_b} \setminus \mathbb{S}^{\perp_b}$ has the required syndrome $\sigma(E)$. ∎

Theorem 8 shows in particular that if $\mathbb{S}$ is an admissible group and $\mathcal{C}$ is the associated stabiliser code, then $\mathbb{S}$ is uniquely determined (modulo $\{\pm 1, \pm i\}$) and we may speak of the stabiliser group of $\mathcal{C}$.

Minimum distance. The minimum distance d of a stabiliser code is defined to be the weight (number of non-identity symbols of an n-tuple in $\{I, X, Y, Z\}^n$) of an n-Pauli group element E that has zero syndrome, $\sigma(E) = 0$, but does not belong to the stabiliser group $\mathbb{S}$.

Theorem 9. *If $\mathcal{C}$ is a quantum stabiliser code and a state $|\psi\rangle \in \mathcal{C}$ is corrupted by an error E of weight $t < d/2$, then the state $|\psi\rangle$ can be recovered.*

Proof. As Proposition 7 and the discussion before it has shown, we can recover the syndrome $s = \sigma(E)$ from the corrupted state $E|\psi\rangle$. We then look for the element $E' \in \mathbb{G}_n$ of smallest weight such that $\sigma(E') = s$. Since $\mathbb{G}_n$ is finite, this is always possible, and there is nothing quantum about this computation. Exhaustive search may be unrealistic however, and we may need a reasonable low-complexity algorithm that will come with the stabiliser group for this task, but this is a purely classical computing issue (although an important one nonetheless) that we ignore it for the moment. Now we have $\sigma(E'E) = \sigma(E') + \sigma(E) = 0$, but since the weight t' of E' satisfies $t' \leqslant t < d/2$, and since the weight of $E'E$ is at most $t + t' < d$ it must be that $E'E \in \mathbb{S}$, meaning in particular that $E'E$ stabilises the quantum state represented by $|\psi\rangle$. So we can recover the original quantum state $|\psi\rangle$ by applying E' to $E|\psi\rangle$. ∎

Since CSS codes are instances of stabiliser codes, Theorem 9 applies in particular to them. We note that the error-correcting potential given by Theorem 9 is stronger than that given by Theorem 4. The quantum CSS code of the next section gives a strong illustration of this.

Parameters of a quantum code. The parameters of a quantum stabiliser code are usually denoted by $[[n, k, d]]$. The integer n refers to the length or the number of qubits, k refers to the code "dimension", which means that the dimension over $\mathbb{C}$ of $\mathcal{C}$ is 2^k, and d refers to the minimum distance as defined just before Theorem 9.

5 Kitaev's toric code

Kitaev's toric code (or family of codes) has the specific feature that its stabiliser group is generated by low-weight elements of $\mathbb{G}_n$, specifically elements of weight 4. This is a desirable feature of a quantum code that we do not attempt to motivate properly here but it makes these codes potentially easier to implement and is relevant to quantum aspects of computational complexity. The Kitaev code is a CSS code. As such, its stabiliser group is generated by a set of elements of $\mathbb{G}_n$ that can be partitioned into two sets. The first of these sets is made up of error patterns of the form Z^e, that is in one-to-one correspondence with rows e of a binary matrix that we call $\mathbf{H}_X$ (because it is used to correct X-errors). Similarly, the second of these sets corresponds to the rows of a matrix named $\mathbf{H}_Z$. The matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ were introduced at the end of Section 3.

To define the matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ we identify their column coordinates with the set of edges of a graph $\mathbf{T} = (V, E)$, represented below, that is the Cayley graph of the additive group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with generators $(\pm 1, 0)$ and $(0, \pm 1)$. This is a 4-regular graph that tiles a 2-dimensional torus – hence the name 'toric code'. The graph $\mathbf{T}$ has $|V| = m^2$ vertices and $|E| = n = 2m^2$ edges.

The matrix $\mathbf{H}_X$ is defined as the vertex-edge incidence matrix of the graph $\mathbf{T}$ and its rows represent elementary cocycles of the graph. In other words, every vertex (x, y) gives rise to a row of $\mathbf{H}_X$ that is a binary vector of weight 4, and whose 1-coordinates are indexed by the edges that connect (x, y) to $(x + 1, y), (x, y + 1), (x - 1, y), (x, y - 1)$. The rows of the matrix $\mathbf{H}_Z$ correspond similarly to elementary cycles, or faces of the graph, meaning all 4-cycles of the form $(x, y) - (x, y + 1) - (x + 1, y + 1) - (x + 1, y) - (x, y)$.

We see that any elementary cocycle has an even (0 or 2) number of edges in common with a face, which means that every row of $\mathbf{H}_X$ is orthogonal to every row of $\mathbf{H}_Z$, which is exactly the property we need for $\mathbf{H}_X$ and $\mathbf{H}_Z$ to define a quantum CSS code.

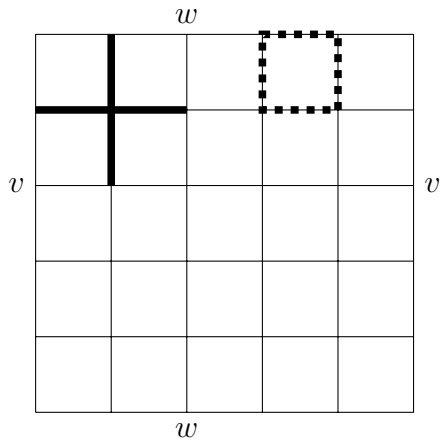

Figure 2: the torus: identify opposing sides of the grid to make v and w into single vertices. A row vector of $\mathbf{H}_X$ ($\mathbf{H}_Z$) is represented by the thick (dashed) edges.

Poincaré duality. If we associate to every face of $\mathbf{T}$ a vertex, and connect two of these vertices whenever the corresponding faces have an edge in common, we obtain the *dual graph* $\mathbf{T}^*$, as represented on Figure 3.

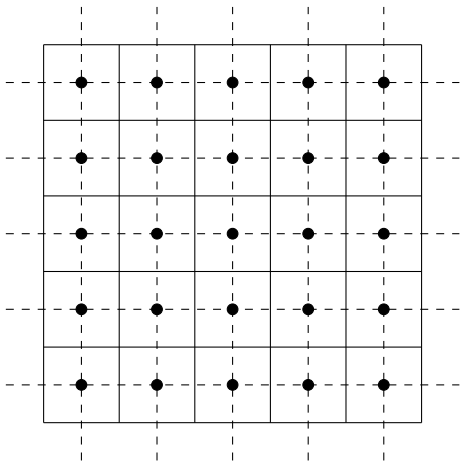

Figure 3: The dual graph $\mathbf{T}^*$

The classical binary code defined by the parity-check matrix $\mathbf{H}_X$ is called the *cycle code* (or cycle space outside the coding theory context) of the graph $\mathbf{T}$. We see that the binary code defined by the parity-check matrix $\mathbf{H}_Z$ is the cycle code of the *dual graph* $\mathbf{T}^*$. Since the graph $\mathbf{T}^*$ is isomorphic to $\mathbf{T}$, we have that $\mathbf{H}_X$ and $\mathbf{H}_Z$ are associated to equivalent classical codes, and more generally that the quantum CSS code defined by $(\mathbf{H}_X, \mathbf{H}_Z)$ will correct exactly the same set of X-error patterns as that of Z-error patterns.

Code dimension. Since every column of $\mathbf{H}_X$ has weight 2, the sum of all the rows of $\mathbf{H}_X$ is 0. It can be shown that the dimension of the row space of $\mathbf{H}_X$ is exactly $m^2 - 1$. By duality, the dimension of the row space of $\mathbf{H}_Z$ must also be $m^2 - 1$, and we get that the dimension of the stabiliser group is $2m^2 - 2 = n - 2$, which means that the dimension of the quantum code is $k = 2$. The Kitaev code protects two qubits.

Minimum distance. The classical code defined by the parity-check matrix $\mathbf{H}_X$ is a very poor code. Its Hamming minimum distance is 4, since it contains rows of $\mathbf{H}_Z$ among its codewords. The quantum minimum distance is better however. Indeed, this is given by the smallest length of a cycle that cannot be expressed as a sum of faces. This is seen to be $d = m = \sqrt{n/2}$ (see Figure 4).

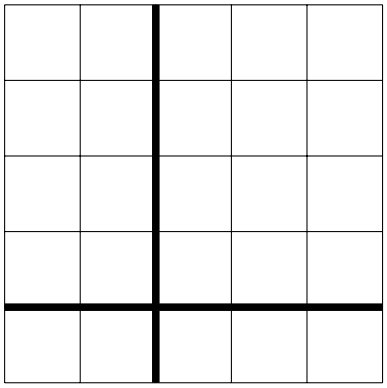

Figure 4: Minimal cycles that are not sums of faces

Decoding. Suppose we want to decode an X-error pattern. By duality we will be able to decode Z-errors in exactly the same way. The X-error gives rise to a binary syndrome $s \in \mathbb{F}_2^V$ for the parity-check matrix $\mathbf{H}_X$, and the decoding problem consists exactly of finding a minimum weight binary vector e that fits this syndrome, i.e. such that $\sigma(e) = \mathbf{H}_X e^T = s$. The set of syndrome coordinates is in one-to-one correspondence with the set V of vertices of $\mathbf{T}$, and the syndrome vector s is the characteristic vector of a subset of vertices W. The decoding problem consists of finding a minimum-cardinality set of edges that is equal to an edge-disjoint union of paths whose endpoints make up a partition of W into pairs of vertices. An example is illustrated in Figure 5.

How to efficiently find such a minimal weight partition of the "syndrome set" W is a non-trivial task. It can be done by first computing all minimum distances between pairs of vertices of W. This gives rise to a weighted complete graph on the vertex set W. Then one applies Edmonds "Blossom" algorithm which finds a minimum weight matching for this graph.

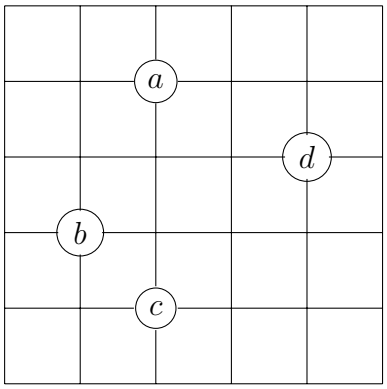

Figure 5: An example of the decoding problem. Vertex a should be paired with d to yield a weight 5 error pattern made up of one path of length 3 from a to d and a length 2 path from b to c. Other pairings of $\{a, b, c, d\}$ yield error patterns of greater weight.

References

[1] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Info. Theor.*, 44(4), 1369–1387, 1998.

[2] J. Edmonds, Paths, trees, and flowers. *Canad. J. Math.* 17: pp. 449–467, 1965.

[3] D. Gottesman. *Stabilizer codes and quantum error correction.* PhD thesis, California Institute of Technology, Pasadena, CA, 1997.

[4] A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi, *Classical and Quantum Computation*, AMS, 2002.

[5] Raymond Laflamme, Cesar Miquel, Juan Pablo Paz, and Wojciech Hubert Zurek, Perfect Quantum Error Correcting Code *Phys. Rev. Lett.* 77, 1996.

[6] John Preskill. Lecture notes, *Quantum error correction.* `http://www.theory.caltech.edu/people/preskill/ph229/notes/chap7.pdf`

[7] John Watrous's Lecture Notes, `https://cs.uwaterloo.ca/~watrous/LectureNotes.html`