QUANTUM COMPUTATION AND QUANTUM ERROR CORRECTION: THE THEORETICAL MINIMUM⋆

⋆WITH ANSWERS AND OTHER EXTRAS IN THE FOOTNOTES

MARK WILDON

Abstract. These notes introduce quantum computation and quantum error correction, emphasising the importance of stabilisers and the mathematical foundations in basic Lie theory. We begin by using the double cover map $\mathrm{SU}_2 \to \mathrm{SO}_3(\mathbb{R})$ to illustrate the distinction between states and measurements for a single qubit. We then discuss entanglement and CNOT gates, the Deutsch–Jozsa Problem, and finally quantum error correction, using the Steane $[[7,1,3]]$-code as the main example. The necessary background physics of unitary evolution and Born rule measurements is developed as needed. The circuit model is used throughout.

Introduction. Maybe you know that atoms bond together into molecules by sharing pairs of electrons. In quantum language, electrons are qubits, or elements of 2-dimensional Hilbert space, and one type of bond is the Bell pair made by applying a CNOT gate with control qubit $|+\rangle$ to a target qubit $|0\rangle$ (see §2.1). In this article we use controlled gates, most importantly the CNOT gate, to prove that quantum computers are strictly more powerful than classical computers. We introduce the key idea of 'measuring a stabiliser' and show how it can be used to implement quantum error correction, making quantum computation a practical possibility.[1]

Outline: §1, §2, §3, §4 deal respectively with one qubit (basics), two qubits (CNOT gates, entanglement), many qubits (quantum computing, including the Quantum Discrete Fourier Transform for Boolean functions) and 'too many' qubits (quantum error correction).

1. One qubit

1.1. **The absolute minimum.** A qubit is an element of 2-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$. We fix the orthonormal basis $|0\rangle$, $|1\rangle$ of $\mathcal{H}$. Thus

$$\mathcal{H} = \big\{ \alpha|0\rangle + \beta|1\rangle : \alpha, \beta \in \mathbb{C} \big\}$$

and $\langle 0|0\rangle = \langle 1|1\rangle = 1$, $\langle 0|1\rangle = \langle 1|0\rangle = 0$.

Date: February 2026, *Email for comments:* `mark.wildon@bristol.ac.uk`.

[1]**Lie:** the early parts of these notes are crawling with ~~lies~~ deliberate oversimplifications, the worst of which are mentioned in numbered footnotes like this. I hope you will be impressed by the number so far: elements of Hilbert space proportional by a non-zero scalar define the same physical state; qubits are not necessarily electrons; a more typical bond is the spin singlet state $\frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$, which is the Bell pair $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ with the XZ-operator applied (see Exercise 2.8); quantum computers are only proved to be more powerful than classical computers *relative to an oracle*; error correction only works if the raw qubits are not *too* error prone.

Remark 1.1. Do not be scared by the ket notation. As a rough guide, symbols of the same type, such as '00' and '01' define orthonormal kets in the same basis, while symbols of different types, such as '0' and '+', define kets in different bases and generally are not orthogonal. For instance the inner product of $|0\rangle$ and $|+\rangle$ is given by flipping $|0\rangle$ so that it becomes $\langle 0|$ and then putting it next to $|+\rangle$, getting $\langle 0|+\rangle$, which is of course $\frac{1}{\sqrt{2}}$. Since bras such as $\langle 0|$ are elements of the dual space $\mathcal{H}^\star$, our inner product must be defined so that the conjugation is on the left-hand side: $\langle \alpha v|\beta w\rangle = \overline{\alpha}\beta \langle v|w\rangle$.[2]

Quantum computers work by applying unitary linear maps to $\mathcal{H}$ and its tensor powers. These unitary linear maps are called *gates*.[3] For instance, the *Z-gate* and *X-gate* act on the single qubit space $\mathcal{H}$ and have matrices

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

in the basis $|0\rangle$, $|1\rangle$. Observe that $|0\rangle$ is a $+1$-eigenvector of Z and $|1\rangle$ is a -1-eigenvector of Z. For this reason, we call $|0\rangle, |1\rangle$ the *Z-basis* of $\mathcal{H}$. Similarly

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

form an orthonormal basis of $\mathcal{H}$ of X-eigenvectors, with eigenvalues $+1$ and -1; this is the *X-basis*. The X-gate is the analogue of the classical NOT gate, flipping between $|0\rangle$ and $|1\rangle$, while the Z-gate, which introduces a phase from the minus sign in $Z|1\rangle = -|1\rangle$, has no analogue in classical computing.

The Z- and X-bases are switched by the unitary *Hadamard* gate

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Note that $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$, and $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$. Thus H has order 2.

Definition 1.2 (Z-basis measurement)**.** Let $\alpha|0\rangle + \beta|1\rangle$ be a qubit normalized so that $|\alpha|^2 + |\beta|^2 = 1$. *Measuring* $\alpha|0\rangle + \beta|1\rangle$ in the Z-basis projects it to $|0\rangle$ with probability $|\alpha|^2$ and to $|1\rangle$ with probability $|\beta|^2$. The measurement result is 0 or 1, respectively.

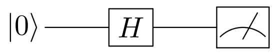
[2]**Aside:** physicists will put anything and everything into a ket. For instance they like to write $|x\rangle$ for the state 'the particle is certainly at position $x \in \mathbb{R}$', and will then happily apply an operator to this eigenstate to extract the eigenvalue x. Sometimes this operator is also denoted x, although it should be admitted that $\widehat{x}$ is more common. Thus $\widehat{x}|x\rangle = x|x\rangle$ is not a tautological string of barely meaningful symbols, but instead a deep physical truth about measurement of quantum states. Worse still, in the continuous setting, $|x\rangle$ is not really defined at all, since it would have to be some kind of Dirac delta 'function', and so not a member of any reasonable Hilbert space. None of this matters.

[3]**Lie:** we will get to measurement shortly. This *circuit model* is not the only model for quantum computation, but all reasonable models define the same computational class BQP. See §3.10 for more on BQP, footnote 36 for the Solovay–Kitaev Theorem and §3.11 for why gates are unitary.

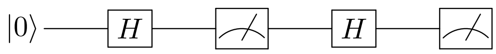
This is a special case of the *Born rule*. Note that we need normalized states in order for the probabilities as defined to sum to 1. Please pause for a moment to note that *measurement changes the state*. This already shows that *states are not the same as measurement*.[4] This is one of the three basic ways in which quantum physics differs from classical physics. (The other two are superposition and entanglement; all three are critical to quantum computation.) We will see in Theorem 3.6 and §4.4 how this 'collapse of the wave function on measurement' is exploited in quantum computation and in quantum error correction.

After an act of measurement, you learn the result: this is a classical bit 0 or 1, depending on whether the new quantum state is $|0\rangle$ or $|1\rangle$. In the computational setting, imagine a wire connecting the quantum computer to an ordinary classical computer that carries all these measurement results. As a quick exercise, what does X-basis measurement do?[5] What happens if you measure the qubit $|0\rangle$ in the X-basis and then in the Z-basis?[6] Well done, now you do not have to read the rest of this section, which is by far the hardest part of these notes. Please skip to §2.

1.2. **The Stern–Gerlach experiment*****.** Subsections marked $\star$ should be skipped. Seriously, haven't you been warned enough? The diagram below show the quantum circuit abstraction of the Stern–Gerlach experiment, in which a spin up qubit (mathematically $|0\rangle$) is put through a splitter (mathematically the Hadamard gate H). Its spin is then measured by a gadget implementing the Z-basis measurement in Definition 1.2, as shown by the meter. Since just before measurement the qubit is in the plus state $\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$, Definition 1.2 implies that the experimental results show an even split between measurements of 0 and 1.



Consistent with Definition 1.2, exactly the same statistics are observed if we instead start with spin down qubits (mathematically $|1\rangle$) which are transformed by the splitter to the minus state $\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$. Now suppose that we put the measured qubit through a second splitter, and measure again, as shown below



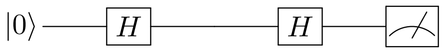
Again it follows easily from Definition 1.2 that both measurements give an even split between $|0\rangle$ and $|1\rangle$. But now suppose we do not observe the qubit

[4]**Isn't this obvious?** Mathematically we already know states are not measurements, because states are elements of $\mathcal{H}$ (or its tensor powers) and measurements are certain projections. But the emphasis is deserved because it is tempting to relapse into a classical world that elides this 'type level' distinction. I can imagine a first lecture on classical physics that begins 'Physics is about physical states, i.e. what we can measure . . . '.

[5]**Answer:** it projects to $|+\rangle$ and $|-\rangle$ and after measurement you learn $+$ if the new state is $|+\rangle$ and $-$ if the new state is $|-\rangle$.

[6]**Answer:** the X-basis measurement gives $|+\rangle$ and $|-\rangle$ with equal probability (and you learn which); the Z-basis measurement then gives $|0\rangle$ and $|1\rangle$ again with equal probability (and again you learn which).

in between the two splitters, so the relevant circuit is now



What now are the experimental results? Correct: because $H^2 = I$, we always measure $|0\rangle$. The Stern–Gerlach experiment shows that a *superposition*, such as the plus state $\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ of the unmeasured qubit between the two splitters, is not 'secretly' either $|0\rangle$ or $|1\rangle$ — since if so, the final experimental results would show the same even split between $|0\rangle$ and $|1\rangle$ — but a *different physical state*. This contradicts classical physics. Note we needed only a single qubit and a 2-dimensional Hilbert space to do all this: no continuous wave functions or double-slit experiments were required![7]

1.3. **Measuring spin in any direction*.** For this subsection we shall suppose that qubits are particles such as electrons which have a *spin*, namely an axis in $\mathbb{R}^3$ and a spin magnitude, either $+\frac{1}{2}$ or $-\frac{1}{2}$. In this case the Stern–Gerlach measuring apparatus is a pair of magnets. To measure spin about the axis in the direction of the normalized vector $\widehat{\mathbf{n}} \in \mathbb{R}^3$, you orient the pair in the direction of $\widehat{\mathbf{n}}$, and observe whether the particle is pulled in the direction $\widehat{\mathbf{n}}$ 'forwards', indicating spin $+\frac{1}{2}$, or in the direction $-\widehat{\mathbf{n}}$ 'backwards', indicating spin $-\frac{1}{2}$.[8]

Measurement in a rotated direction. Measurement in direction $\widehat{\mathbf{z}}$ is observed experimentally to result in 'up', $+1$, 'forward' on particles in state $|0\rangle$ and 'down', -1, 'backward' on particles in state $|1\rangle$. (We may take this as the *definition* of 'spin up' and 'spin down', and ignore that the correct quantized unit is $\hbar/2$.) Recall that the Z-matrix has 1-eigenvector $|0\rangle$, and -1-eigenvector $|1\rangle$ forming the Z-basis. If we rotate the apparatus by a small

[7]**Reference:** see [11] for a rigorous introduction to quantum computation, written for the lay reader that, no coincidence, continues along these lines. For more quantum circuit abstractions of important physics experiments, including a fascinating discussion of Wigner's Friend, see Maria Violaris' videos: `https://www.youtube.com/watch?v=TMBK88Mpg5U`.

[8]**Physical details:** the Stern–Gerlach experiment is typically performed with silver atoms because they are easier to manage in the laboratory than electrons (cathode rays). The reason silver is an acceptable substitute is that silver has atomic number $47 = 2+8+8+18+10+1$, filling up the $1s, 2s, 2p, 3s, 3p, 3d, 4s, 4p, 4d$ shells, leaving one electron all on its own in the outermost $5s$ shell. (This is an exception to the Aufbau rule, that predicts $\ldots 4d^9 5s^2$: the configuration adopted by silver is lower energy.) Because all the inner electrons resonate with each other, the magnetic properties of silver are dominated by the spin of this single outer electron. To measure spin in direction $\widehat{\mathbf{z}}$, take a strong top magnet and a weaker bottom magnet, making a magnetic field oriented in the $\widehat{\mathbf{z}}$ direction. Spin $\frac{1}{2}$ particles entering the field align their spin with the $\widehat{\mathbf{z}}$ direction, and because the field is inhomogeneous, particles with spin $+\frac{1}{2}$ are pulled up ('forward', project to $|0\rangle$, measure 0) and particles with spin $-\frac{1}{2}$ are pulled down ('backwards', project to $|1\rangle$, measure 1). The deflection is quantized, and is always a multiple by $+1, -1, +2, -2$ etc, of a minimum deflection; this minimum deflection is determined by Planck's constant and the magnetic field strength. (For silver atoms, there are no excited states and only two deflections are observed, one up and one down.) This is already not consistent with classical physics, which says that there should exist particles with spin very weakly aligned in the $\widehat{\mathbf{z}}$ direction that are deflected up by a very small but non-zero amount.

angle ϑ about the y-axis, so that it now points in the direction $\cos\vartheta\,\widehat{\mathbf{z}}+\sin\vartheta\,\widehat{\mathbf{x}}$, then the Z matrix 'rotates' to

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$R = \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{pmatrix} = (\cos\vartheta)Z + (\sin\vartheta)X$$

Note that R is still a Hermitian matrix and from the determinant and trace, you can see it still has eigenvalues $+1$ and -1; moreover it shows the only way to evolve Z by a one-parameter subgroup so that when $\vartheta = \frac{\pi}{2}$ it becomes X.[9] The calculations

$$\begin{pmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{pmatrix}\begin{pmatrix} \cos\frac{\vartheta}{2} \\ \sin\frac{\vartheta}{2} \end{pmatrix} = \begin{pmatrix} \cos\vartheta\cos\frac{\vartheta}{2} + \sin\vartheta\sin\frac{\vartheta}{2} \\ \sin\vartheta\cos\frac{\vartheta}{2} - \cos\vartheta\sin\frac{\vartheta}{2} \end{pmatrix} = \begin{pmatrix} \cos\frac{\vartheta}{2} \\ \sin\frac{\vartheta}{2} \end{pmatrix}$$

$$\begin{pmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{pmatrix}\begin{pmatrix} \sin\frac{\vartheta}{2} \\ -\cos\frac{\vartheta}{2} \end{pmatrix} = \begin{pmatrix} \cos\vartheta\sin\frac{\vartheta}{2} - \sin\vartheta\cos\frac{\vartheta}{2} \\ \sin\vartheta\sin\frac{\vartheta}{2} + \cos\vartheta\cos\frac{\vartheta}{2} \end{pmatrix} = \begin{pmatrix} -\sin\frac{\vartheta}{2} \\ \cos\frac{\vartheta}{2} \end{pmatrix}$$

show that R has eigenvector $\cos\frac{\vartheta}{2}\left|0\right\rangle + \sin\frac{\vartheta}{2}\left|1\right\rangle$ with eigenvalue 1 and eigenvector $-\sin\frac{\vartheta}{2}\left|0\right\rangle + \cos\frac{\vartheta}{2}\left|1\right\rangle$ with eigenvalue -1. These are eigenstates that are the two possible results of measurement in the direction $\cos\vartheta\,\widehat{\mathbf{z}}+\sin\vartheta\,\widehat{\mathbf{x}}$. By the Born rule, starting with $\left|0\right\rangle$, the probability of measuring $+1$ 'forwards' and -1 'backwards' are

$$\left|\cos\tfrac{\vartheta}{2}\left\langle 0|0\right\rangle + \sin\tfrac{\vartheta}{2}\left\langle 1|0\right\rangle\right|^2 = \cos^2\tfrac{\vartheta}{2}, \quad \left|-\sin\tfrac{\vartheta}{2}\left\langle 0|0\right\rangle + \cos\tfrac{\vartheta}{2}\left\langle 1|0\right\rangle\right|^2 = \sin^2\tfrac{\vartheta}{2},$$

respectively. This is both a theoretical prediction and an experimental fact.

From Stern–Gerlach to $\mathrm{SU}_2 \to \mathrm{SO}_3(\mathbb{R})$. Imagine rotating the apparatus very slowly, and repeatedly performing measurements. Occasionally, we'll be unlucky and measure 'backwards', in which case we start again, but we can safely assume that all measurements are 'forwards'.[10]

Exercise 1.3. Suppose we rotate the apparatus in total by an angle ϑ. What is the new quantum state? What unitary operator U corresponds to this evolution of the starting state $\left|0\right\rangle$? What is the conjugate of Z by this U? Go on to discover the double cover $\mathrm{SU}_2 \to \mathrm{SO}_3(\mathbb{R})$ and interpret everything so far with Lie algebras.[11]

---

[9] **Aside:** the author has thought about variations of this argument for over four years and still cannot decide whether this is (a) a correct, physically motivated argument using the isotropy of space, that shows that the Pauli matrices behave like 'vectors' in that measurement in direction $\cos\vartheta\,\widehat{\mathbf{z}} + \sin\vartheta\,\widehat{\mathbf{x}}$ corresponds to the Hermitian matrix $\cos\vartheta Z + \sin\vartheta X$ *or* (b) a complete cheat.

[10] **Not a lie:** by the Born rule, the probability of a 'backwards' measurement after a rotation by $\frac{\vartheta}{N}$ is $\sin^2\frac{\vartheta}{N}$ which is at most $\frac{\vartheta^2}{N^2}$ and so by a union bound the probability of a 'backwards' measurement in N steps is at most ϑ^2/N. Thus by rotating sufficiently slowly (not forgetting to measure after each tiny rotation) we can make the chance of a 'backwards' measurement — corresponding in other settings to a dissipation of the quantum state — arbitrarily small.

[11] **Answer:** the new quantum state is the eigenstate $\cos\frac{\vartheta}{2}\left|0\right\rangle + \sin\frac{\vartheta}{2}\left|1\right\rangle$ above and

$$U = \begin{pmatrix} \cos\frac{\vartheta}{2} & -\sin\frac{\vartheta}{2} \\ \sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{pmatrix}.$$

The previous exercise is, as far as the author has been able to understand, what physicists mean when they say that the symmetry group of a qubit is SU_2 or, rephrased, that a qubit 'is' a vector in the standard representation of SU_2. At the next level up there is the standard representation $\mathcal{K}$ of SU_3, in which the canonical basis vectors label the up, down and strange flavours

---

Calculation shows that

$$\begin{aligned} UZU^{-1} &= \begin{pmatrix} \cos\frac{\vartheta}{2} & -\sin\frac{\vartheta}{2} \\ \sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\frac{\vartheta}{2} & \sin\frac{\vartheta}{2} \\ -\sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{pmatrix} \\ &= \begin{pmatrix} \cos\frac{\vartheta}{2} & \sin\frac{\vartheta}{2} \\ \sin\frac{\vartheta}{2} & -\cos\frac{\vartheta}{2} \end{pmatrix} \begin{pmatrix} \cos\frac{\vartheta}{2} & \sin\frac{\vartheta}{2} \\ -\sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\frac{\vartheta}{2} - \sin^2\frac{\vartheta}{2} & 2\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2} \\ 2\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2} & \sin^2\frac{\vartheta}{2} - \cos^2\frac{\vartheta}{2} \end{pmatrix} \\ &= \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{pmatrix} \end{aligned}$$

Thus when a quantum state transforms by U, physical measurements (i.e. Hermitian matrices) transform by conjugation by U, and the calculation above shows that measurement in the $\widehat{\mathbf{z}}$ direction transforms to measurement in the $\cos\vartheta\,\widehat{\mathbf{z}} + \sin\vartheta\,\widehat{\mathbf{x}}$ direction. (We agreed this was the correct physical interpretation of the final matrix, which is R from earlier: see footnote 8.) More mathematically, quantum states transform by the natural representation of SU_2 and measurements transform by the adjoint representation of SU_2, acting by conjugacy on Hermitian matrices.

We carry on to do the calculations needed for §1.4. Restricting the adjoint action of SU_2 to the subspace $\langle X, Y, Z\rangle$ of 2×2 complex matrices spanned by the Pauli matrices, we get the double cover $\mathrm{SU}_2 \to \mathrm{SO}_3(\mathbb{R})$. The image is in the orthogonal group $\mathrm{SO}_3(\mathbb{R})$ because conjugation preserves the inner product on $\langle Z, X, Y\rangle_{\mathbb{R}}$ defined by $(P,Q) = \frac{1}{2}\operatorname{tr} PQ$ having Z, X, Y as an orthonormal basis. The more general version of the calculation above needs U defined so that $U|0\rangle = \alpha|0\rangle + \beta|1\rangle$, for arbitrary $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$. To make U unitary we take $U = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}$ and then

$$UZU^{-1} = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} Z \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} \alpha & \overline{\beta} \\ \beta & -\overline{\alpha} \end{pmatrix} \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} |\alpha^2| - |\beta|^2 & 2\alpha\overline{\beta} \\ 2\overline{\alpha}\beta & -|\alpha|^2 + |\beta|^2 \end{pmatrix}$$

shows that $UZU^{-1} = a_Z Z + a_X X + a_Y Y$ where $a_Z = |\alpha|^2 - |\beta|^2$, $a_X = 2\operatorname{Re}\alpha\overline{\beta}$ and $a_Y = -2\operatorname{Im}\alpha\overline{\beta}$. Since Z has $|0\rangle$ as its 1-eigenstate, the conjugate UZU^{-1} has $U\,|0\rangle = \alpha|0\rangle + \beta|1\rangle$ as its 1-eigenstate. Thus, in the measurement representation, $\widehat{\mathbf{z}} \mapsto a_Z\,\widehat{\mathbf{z}} + a_X\,\widehat{\mathbf{x}} + a_Y\,\widehat{\mathbf{y}}$. Similar calculations conjugating the Pauli X and $Y = iXZ$ matrices show that

$$UXU^{-1} = \begin{pmatrix} -\overline{\beta} & \alpha \\ \overline{\alpha} & \beta \end{pmatrix} \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} -2\operatorname{Re}\alpha\beta & \alpha^2 - \overline{\beta}^2 \\ \overline{\alpha}^2 - \beta^2 & 2\operatorname{Re}\alpha\beta \end{pmatrix}$$

$$UYU^{-1} = \begin{pmatrix} -i\overline{\beta} & -i\alpha \\ i\overline{\alpha} & -i\beta \end{pmatrix} \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} -2\operatorname{Im}\alpha\beta & -i(\alpha^2 + \overline{\beta}^2) \\ i(\alpha^2 + \overline{\beta}^2) & 2\operatorname{Im}\alpha\beta \end{pmatrix}$$

and so, using the coefficients of Z, X, Y as the column of the matrix, we get the explicit double-cover map

$$\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \mapsto \begin{pmatrix} |\alpha|^2 - |\beta|^2 & -2\operatorname{Re}\alpha\beta & -2\operatorname{Im}\alpha\beta \\ 2\operatorname{Re}\alpha\overline{\beta} & \operatorname{Re}(\alpha^2 - \overline{\beta}^2) & \operatorname{Im}(\alpha^2 + \overline{\beta}^2) \\ -2\operatorname{Im}\alpha\overline{\beta} & -\operatorname{Im}(\alpha^2 - \overline{\beta}^2) & \operatorname{Re}(\alpha^2 + \overline{\beta}^2) \end{pmatrix}$$

A corollary is the Lie algebra isomorphism $\mathsf{su}_2 \cong \mathsf{so}_3(\mathbb{R})$. It is arguably more elegant to bring in the Lie algebra earlier and restrict the adjoint action instead to $\langle iZ, iX, iY\rangle$. We then get SU_2 acting by conjugacy on its Lie algebra su_2 of anti-Hermitian matrices M such that $M = -\overline{M}^t$; an explicit isomorphism $\mathrm{SU}_2(\mathbb{R}) \cong (\mathbb{R}^3, \wedge)$ is then defined on this basis by $-\frac{iX}{2} \mapsto \widehat{\mathbf{x}}$, $-\frac{iY}{2} \mapsto \widehat{\mathbf{y}}$, $-\frac{iZ}{2} \mapsto \widehat{\mathbf{z}}$. In turn an isomorphism $(\mathbb{R}^3, \wedge) \cong \mathsf{so}_3(\mathbb{R})$ is of quarks and general elements represent superpositions of these flavour states. The 27-dimensional tensor product $\mathcal{K} \otimes \mathcal{K} \otimes \mathcal{K}$ decomposes into irreducible subrepresentations that partition baryons made from the up, down and strange quarks. For instance the proton and neutron 'live' in the same irreducible 8-dimensional representation: this is the famous Gell-Mann eightfold way. Be warned that if you search on the web, you are very likely to find this, rather than the simpler SU_2 symmetry group relevant to a spinor qubit.

Exercise 1.4. Suppose that the measurement apparatus is rotated slowly by a full turn, about the $\widehat{\mathbf{y}}$-axis as usual, measuring as usual after each small rotation. What is the new quantum state? Interpret this as paths in SU_2 and $\mathrm{SO}_3(\mathbb{R})$.[12]

1.4. **Summary: the Bloch sphere*.** Generalizing Exercise 1.4, it follows from the explicit double cover map in footnote 11 that the image of the one-parameter subgroup

$$\vartheta \mapsto \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix} \in \mathrm{SU}_2$$

under the double cover map is the one-parameter subgroup

$$\vartheta \mapsto \begin{pmatrix} \cos 2\vartheta & \sin 2\vartheta & 0 \\ -\sin 2\vartheta & \cos 2\vartheta & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SO}_3(\mathbb{R}).$$

For example, as seen in Exercise 1.4, a trip along the path defined by $0 \le \vartheta \le \pi$ in $\mathrm{SU}_2(\mathbb{R})$, which overall flips the phase of the qubit, becomes a closed loop in $\mathrm{SO}_3(\mathbb{R})$; this corresponds to the unobservability of global phase. Going the other way, by varying the axis of rotation in $\mathrm{SO}_3(\mathbb{R})$ (the spin axis that we can measure) we can trace out any path we like in SU_2, or equivalently, move the starting qubit $|0\rangle$ to an arbitrary $\alpha|0\rangle + \beta|1\rangle$. Since elements of $\mathrm{SO}_3(\mathbb{R})$ are rotations, acting on the 2-sphere, this implies that we should be able to visualize states (up to phase) as points on the 2-sphere. This is the *Bloch sphere* model, shown in Figure 1.

---

given by mapping $\widehat{\mathbf{n}}$ to the generator of the infinitesimal rotation with axis $\widehat{\mathbf{n}}$. In our chosen basis,

$$-\tfrac{iZ}{2} \mapsto \begin{pmatrix} 0 & \cdot & \cdot \\ \cdot & 0 & -1 \\ \cdot & 1 & 0 \end{pmatrix}, \quad -\tfrac{iX}{2} \mapsto \begin{pmatrix} 0 & \cdot & 1 \\ \cdot & 0 & \cdot \\ -1 & \cdot & 0 \end{pmatrix}, \quad -\tfrac{iY}{2} \mapsto \begin{pmatrix} 0 & -1 & \cdot \\ 1 & 0 & \cdot \\ \cdot & \cdot & 0 \end{pmatrix}$$

See §3.11 for why anti-Hermitian matrices are natural in this context.

[12]**Answer:** the final state is not the starting state $|0\rangle$ but instead $-|0\rangle$, which differs by an unobservable global phase. Particles with this property are called *spinors*. Thus in $\mathrm{SO}_3(\mathbb{R})$ we made a full circuit (visiting all rotations about the $\widehat{\mathbf{y}}$-axis by angles between 0 and 2π) but in SU_2 we travelled only from I to the antipodal point $-I$. This is consistent with the double cover because U and $-U$ have the same image in $\mathrm{SO}_3(\mathbb{R})$; in fact the kernel of the double cover homomorphism is the subgroup $\{I, -I\}$. While the global phase in $-|0\rangle$ is unobservable, if the rotated qubit is entangled in a Bell pair (see §2), the phase difference between rotated and unrotated qubits can be measured experimentally.

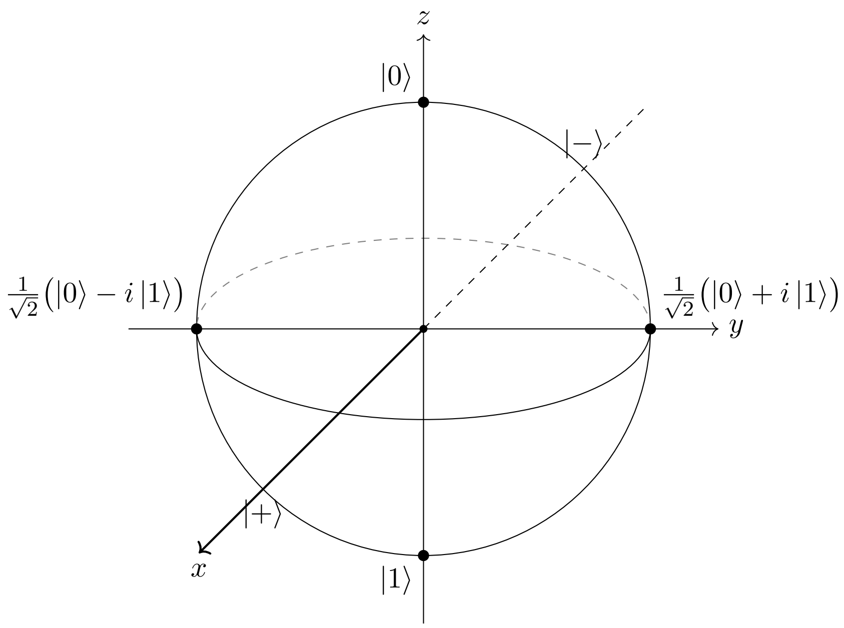


FIGURE 1. The Bloch sphere showing the Z-basis $|0\rangle$, $|1\rangle$, the X-basis $|+\rangle$, $|-\rangle$ and the normalized eigenvectors of $Y = iXZ$.

Exercise 1.5. Check that a normalized qubit, up to phase, has two free parameters, and so the 2-dimensional Bloch sphere has the right dimension.[13]

By the angle doubling remark above, *orthogonal* quantum states, such as the Z-eigenvectors $|0\rangle$ and $|1\rangle$ correspond to *antipodal* points on the Bloch sphere.

$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Exercise 1.6. Check that the Pauli Y matrix defined by $Y = iXZ$, as shown in the margin, has eigenvectors as shown on the y-axis of the Bloch sphere.[14]

For our explicit double cover map, the map from normalized qubits to points on the Bloch sphere is

$$\begin{aligned}\alpha|0\rangle + \beta|1\rangle &= \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} |0\rangle \\ &\mapsto \begin{pmatrix} |\alpha|^2 - |\beta|^2 & -2\operatorname{Re}\alpha\beta & -2\operatorname{Im}\alpha\beta \\ 2\operatorname{Re}\alpha\overline{\beta} & \operatorname{Re}(\alpha^2 - \overline{\beta}^2) & \operatorname{Im}(\alpha^2 + \overline{\beta}^2) \\ -2\operatorname{Im}\alpha\overline{\beta} & -\operatorname{Im}(\alpha^2 - \overline{\beta}^2) & \operatorname{Re}(\alpha^2 + \overline{\beta}^2) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} |\alpha|^2 - |\beta|^2 \\ 2\operatorname{Re}\alpha\overline{\beta} \\ -2\operatorname{Im}\alpha\overline{\beta} \end{pmatrix}.\end{aligned}$$

[13]**Solution:** a general normalized qubit is $\alpha|0\rangle + \beta|1\rangle$ where $|\alpha|^2 + |\beta|^2 = 1$. Working up to phase we can multiply through by $e^{-i\vartheta}$ where ϑ is the argument of α, to reduce to the case where α is real. So the state is $c\,|0\rangle + (d+ie)\,|1\rangle$ where $c^2+d^2+e^2 = 1$, matching points on the 2-sphere.

[14]**Solution:** after multiplying through by the normalization factor $\frac{1}{\sqrt{2}}$ we have

$$Y\big(|0\rangle \pm i\,|1\rangle\big) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \pm i \end{pmatrix} = \begin{pmatrix} \pm 1 \\ i \end{pmatrix} = \pm \begin{pmatrix} 1 \\ \pm i \end{pmatrix} = \pm\big(|0\rangle \pm i\,|1\rangle\big).$$

Note that the axes are ordered (z, x, y). This is a reformulation of the remark in footnote 11 that in the measurement representation $\widehat{\mathbf{z}} \mapsto a_Z \widehat{\mathbf{z}} + a_X \widehat{\mathbf{x}} + a_Y \widehat{\mathbf{y}}$, where $a_Z = |\alpha|^2 - |\beta|^2$, $a_X = 2\,\mathrm{Re}\,\alpha\overline{\beta}$, $a_Y = -2\,\mathrm{Im}\,\alpha\overline{\beta}$. In the same footnote, we saw that since Z has eigenbasis $|0\rangle$, $|1\rangle$, the conjugate

$$\begin{aligned} UZU^{-1} &= \big(|\alpha|^2 - |\beta|^2\big) Z + 2\,\mathrm{Re}\,\alpha\overline{\beta} X - 2\,\mathrm{Im}\,\alpha\overline{\beta} Y \\ &= a_Z Z + a_X X + a_Y Y \end{aligned}$$

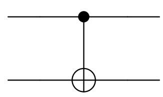
has $\alpha|0\rangle + \beta|1\rangle$ as a 1-eigenvector. (And, from the second column of U, $-\overline{\beta}\,|0\rangle + \overline{\alpha}\,|1\rangle$ spans its orthogonal complement in $\mathcal{H}$ and is a -1-eigenvector.) Thus qubits transform by SU_2 whereas physical measurements — thought of either as Hermitian matrices as immediately above, or directions of our measuring apparatus in $\mathbb{R}^3$ — transform by the image $\mathrm{SO}_3(\mathbb{R})$ of SU_2 under the double cover map; this is the adjoint representation of SU_2. In particular by taking $\alpha = \frac{1}{\sqrt{2}}$, $\beta = \frac{i}{\sqrt{2}}$ and noting that $a_Z = 0$, $a_X = 0$ and $a_Y = \frac{1}{2}$, we get an alternative solution to Exercise 1.6. For more on the Bloch sphere see [9, page 15].

2. Two qubits and the copy rules

2.1. **Two qubits.** The correct way to model two qubits is by the tensor product $\mathcal{H} \otimes \mathcal{H}$ where, as always in these notes, the tensor product is over $\mathbb{C}$. Experience shows that it works very well to take as the *definition* of $\mathcal{H} \otimes \mathcal{H}$ that it is the vector space spanned by the symbols $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$, which we quickly rewrite as either $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, $|1\rangle|1\rangle$, or, particularly when more than two qubits (see §3.1) are involved, as $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. This is the *Z-basis* of $\mathcal{H} \otimes \mathcal{H}$ of eigenvectors for $Z \otimes Z$.[15]

CNOT gates. By far the most important 2-qubit gate is the CNOT gate. The inputs to the CNOT gate are a *control* qubit and a *target qubit.* Its matrix in the basis $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, $|1\rangle|1\rangle$, supposing that the first qubit is the control qubit and the second qubit is the target qubit, is

$$\mathrm{CNOT} = \begin{array}{c} \begin{matrix} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$



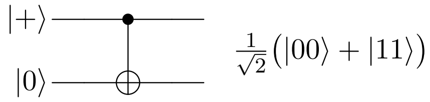
The circuit diagram for CNOT is shown right above, with the usual convention that the first qubit is on the top wire. Given any $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathcal{H}$, we have

$$\begin{aligned} \mathrm{CNOT}\,|0\rangle|\psi\rangle &= \mathrm{CNOT}\big(\alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle\big) = \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle = |0\rangle|\psi\rangle\,, \\ \mathrm{CNOT}\,|1\rangle|\psi\rangle &= \mathrm{CNOT}\big(\alpha|1\rangle|0\rangle + \beta|1\rangle|1\rangle\big) = \alpha|1\rangle|1\rangle + \beta|1\rangle|0\rangle = |1\rangle X\,|\psi\rangle\,. \end{aligned}$$

[15]**Maths:** of course if you prefer a more high-brow definition of the tensor product, then you are very welcome to it. It might seem that omitting the tensor product sign in $|0\rangle|1\rangle$ would create an ambiguity with symmetric powers, but, unlike most things, this has never confused the author.

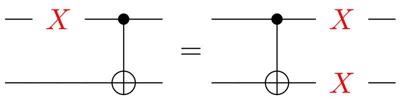
Thus one often says that CNOT 'flips the target qubit if the control qubit is set'.[16] In the setup of Definition 3.3, CNOT is a controlled NOT gate.

Exercise 2.1. Show that CNOT $|+\rangle\,|0\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ as shown diagrammatically below.

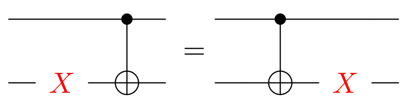


The output is known as the *Bell state*. Is there a meaningful way to label the two output wires separately, as we did for the input wires?[17]

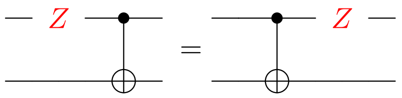
2.2. **The copy rules.** Here are the diagrammatic copy rules for conjugating faults past CNOT gates. The equivalent algebra is below.



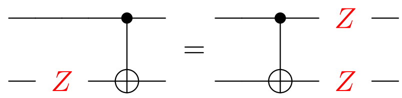
$\mathrm{CNOT}(X\otimes I) = (X\otimes X)\,\mathrm{CNOT}$



$\mathrm{CNOT}(I\otimes X) = (I\otimes X)\,\mathrm{CNOT}$



$\mathrm{CNOT}(Z\otimes I) = (Z\otimes I)\,\mathrm{CNOT}$



$\mathrm{CNOT}(I\otimes Z) = (Z\otimes Z)\,\mathrm{CNOT}$

Exercise 2.2. Prove the copy rules.[18]

In the context of quantum error correction, we often imagine the incoming X- or Z- as an X-fault or Z-fault thrown by a quantum glitch somewhere in the circuit. The copy rules then become rules for fault propagation.

---

[16]**Misleading:** in practice the control qubit is very often not $|0\rangle$ or $|1\rangle$ but instead the superposition $|+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$, and so this 'classical' account of what CNOT does makes no sense. Still it seems to work for everyone.

[17]**Solution:** by linearity,

$$\mathrm{CNOT}\,|+\rangle\,|0\rangle = \mathrm{CNOT}\,\tfrac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)\,|0\rangle = \tfrac{1}{\sqrt{2}}\,\mathrm{CNOT}\,|00\rangle + \tfrac{1}{\sqrt{2}}\,\mathrm{CNOT}\,|10\rangle = \tfrac{1}{\sqrt{2}}\,|00\rangle + \tfrac{1}{\sqrt{2}}\,|11\rangle$$

as required. No: since the Bell state does not factor as a tensor product $|\phi\rangle \otimes |\psi\rangle$ the wires cannot be labelled separately. In fact the Bell state is in a precise sense, maximally entangled. See §2.3 for an application of this entanglement.

[18]**Not a solution:** sorry, this really is something everyone should do once in their life. If you find the algebra isn't working for you, please check that you are composing maps from right-to-left; note this is the opposite direction to circuit diagrams, but consistent with matrices acting on column vectors and usual mathematical practice. (Although with a double dose of potential confusion, this might not matter because CNOT is self-inverse.) Another way to go wrong is to be inconsistent in the order of qubits. For instance the matrices for $X \otimes I$ and $I \otimes X$ are, with our usual order $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ for the basis,

$$\begin{pmatrix} 0 & \cdot & 1 & \cdot \\ \cdot & 0 & \cdot & 1 \\ 1 & \cdot & 0 & \cdot \\ \cdot & 1 & \cdot & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & \cdot & \cdot \\ 1 & 0 & \cdot & \cdot \\ \cdot & \cdot & 0 & 1 \\ \cdot & \cdot & 1 & 0 \end{pmatrix}.$$

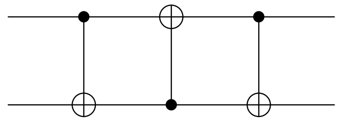
As a visual guide, $\cdot$ denotes a 0 from the tensor product factorization, which puts a 0 in the positions corresponding to the zeros of X; these are marked $\cdot$ in the margin.

Remark 2.3. From the classical point of view that CNOT is an operation performed on the target qubit, it may seem very unintuitive that a Z-fault on the target qubit should copy up to the control qubit: well, that's entanglement for you. This becomes a recurring theme in quantum error correction: faults on ancilla states copy up to the target state. See Exercise 4.10 for an example of this.

Any circuit involving only CNOT and Hadamard gates (and a few other gates we haven't defined) is characterized by its conjugation action on X- and Z-faults.[19] That is, *how the circuit propagates incoming X- and Z-faults determines it completely.* This makes the copy rules enormously powerful.

Exercise 2.4. The SWAP gate is defined on $\mathcal{H} \otimes \mathcal{H}$ in a basis independent way by $\mathrm{SWAP}\,|\phi\rangle\,|\psi\rangle = |\psi\rangle\,|\phi\rangle$. Its Z-basis matrix is shown below, with a circuit implementing SWAP to the right.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



Prove this by pushing faults through the three CNOT gates using the copy rules. Equivalently, using indices to denote control and targets in CNOTs, prove that $\mathrm{SWAP} = \mathrm{CNOT}_{12}\,\mathrm{CNOT}_{21}\,\mathrm{CNOT}_{12}$.[20]

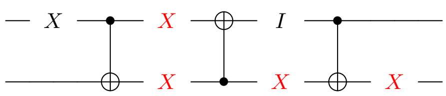
Exercise 2.5. Use fault pushing to give an alternative solution to Exercise 2.1. [*Hint:* the stabiliser group of $|+\rangle\,|0\rangle$ is generated by $X \otimes I$ and $I \otimes Z$. Push these faults through to get the stabiliser group of the output state.][21]

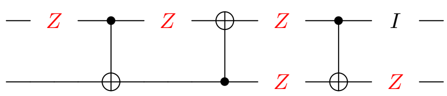
$X = \begin{pmatrix} \cdot & 1 \\ 1 & \cdot \end{pmatrix}$

---

[19]**Sketch proof:** all these gates lie in the Clifford group and so are determined, up to phase, by their conjugacy action on tensor products of the Pauli X and Z operators. But H and CNOT do not introduce any phases, so this 'up to' is irrelevant. For example, CNOT is the unique phaseless 2 qubit gate satisfying the copy rules above, which restated as conjugations are $\mathrm{CNOT}(X \otimes I)\,\mathrm{CNOT}^{-1} = X \otimes X$, and so on. □ The characterization extends to circuits using the single qubit X, Y and Z gates if one allows for a global phase of ± 1, and to general Clifford circuits, including the S-gate, allowing for ± 1 and $\pm i$.

[20]**Solution**: the diagrams below shows that $\mathrm{SWAP}(X \otimes I) = (I \otimes X)\,\mathrm{SWAP}$ and $\mathrm{SWAP}(Z \otimes I) = (I \otimes Z)\,\mathrm{SWAP}$.



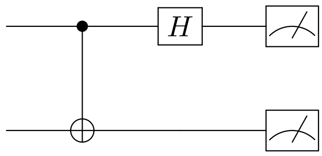


Here I is used to denote the place where two X- or two Z-faults cancel. Very similarly, or algebraically by composing on the left and right with SWAP, we have $(X \otimes I)\,\mathrm{SWAP} = \mathrm{SWAP}(I \otimes X)$ and $(Z \otimes I)\,\mathrm{SWAP} = \mathrm{SWAP}(I \otimes Z)$. By the Clifford characterization, since the putative SWAP gate does the correct thing on X- and Z-faults, and is phaseless, it is SWAP. It is interesting to compare this circuit with the way to swap two variables in a classical computer without using extra scratch space: in C, using the XOR operator `^`, this is `x = x^y; y = x^y; x = x^y;`

[21]**Solution:** the 'non-pass-through' copy rules are precisely the statements that $\mathrm{CNOT}(X \otimes I) = (X \otimes X)\,\mathrm{CNOT}$ and $\mathrm{CNOT}(I \otimes Z) = (Z \otimes Z)\,\mathrm{CNOT}$. Hence, writing $|\Phi\rangle$ for the output of the circuit in Exercise 2.1,

$$|\Phi\rangle = \mathrm{CNOT}\,|+\rangle\,|0\rangle = \mathrm{CNOT}(X \otimes I)\,|+\rangle\,|0\rangle = (X \otimes X)\,\mathrm{CNOT}\,|+\rangle\,|0\rangle = (X \otimes X)\,|\Phi\rangle$$

2.3. **Superdense encoding: entanglement as a resource*.** Dual to the Bell state preparation circuit in Exercise 2.1 there is the measurement circuit below.



Here H denotes the Hadamard gate and, as usual, meters denote Z-basis measurement on each qubit. For this subsection, the simple single qubit definition of measurement (Definition 1.2) can be applied to each qubit in turn.[22] Let $|\Phi\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ denote the Bell state. Since $(X \otimes I)|\Phi\rangle = (I \otimes X)|\Phi\rangle$ we can write $X|\Phi\rangle$ without ambiguity to mean 'there is an X-error on the Bell state'. The table below showing the measurement results for both top and bottom measurements (using Definition 1.2 to define measurement on a single qubit) on the four Bell basis states.

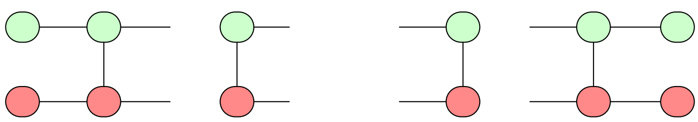
State	In Z-basis	After CNOT	After H	Top	Bottom
$\|\Phi\rangle$	$\frac{1}{\sqrt{2}}\big(\|00\rangle + \|11\rangle\big)$	$\|+\rangle\|0\rangle$	$\|0\rangle\|0\rangle$	0	0
$X\|\Phi\rangle$	$\frac{1}{\sqrt{2}}\big(\|01\rangle + \|10\rangle\big)$	$\|+\rangle\|1\rangle$	$\|0\rangle\|1\rangle$	0	1
$Z\|\Phi\rangle$	$\frac{1}{\sqrt{2}}\big(\|00\rangle - \|11\rangle\big)$	$\|-\rangle\|0\rangle$	$\|1\rangle\|0\rangle$	1	0
$XZ\|\Phi\rangle$	$\frac{1}{\sqrt{2}}\big(\|01\rangle - \|10\rangle\big)$	$\|-\rangle\|1\rangle$	$\|1\rangle\|1\rangle$	1	1

Again let us observe the traditional pause to remember that *measurement changes the state*. For example, since $(H \otimes I)\,\mathrm{CNOT}\,|10\rangle = H\,|11\rangle = |-\rangle\,|1\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |11\rangle\big)$, measuring $|11\rangle$ by the Bell basis gadget reports $(0,1)$ and $(1,1)$ with equal probability; the final states are $|01\rangle$ and $|11\rangle$ respectively.[23]

$$|\Phi\rangle = \mathrm{CNOT}\,|+\rangle\,|0\rangle = \mathrm{CNOT}(I \otimes Z)\,|+\rangle\,|0\rangle = (I \otimes Z)\,\mathrm{CNOT}\,|+\rangle\,|0\rangle = (Z \otimes Z)\,|\Phi\rangle$$

showing that $|\Phi\rangle$ has stabiliser group containing $X \otimes X$ and $Z \otimes Z$. By reversibility, this is the full stabiliser group. The unique state with this stabiliser group is the Bell state, so the state made by the circuit is $|\Phi\rangle$. In this case the fault pushing solution is more fuss than a direct calculation, but in the context of the larger ancilla states needed in quantum error correction, the method of stabiliser subgroups becomes very powerful.

[22]**More elegant:** the author would rather think of the top line as measurement in the X-basis: compare the two circuits at the end of §3.7. This makes the duality more obvious: preparation of $|+\rangle$ dualizes to measurement in the X-basis; preparation of $|0\rangle$ dualizes to measurement in the Z-basis. In the ZX-calculus [14], the symmetry is complete: the diagrams for Bell state preparation and Bell measurement are shown far left and right below, and their fused versions in the middle. By a further simplification these become the 'cup' and 'cap' operators from string-diagram calculus. None of this matters, but you might enjoy contemplating it, and possibly even being paid to do so.



[23]**Pitfall:** since the final states are not in the Bell basis, it would be dangerously loose to describe our gadget as 'measuring in the Bell basis'; instead this is done by projecting

Exercise 2.6. Suppose that Alice and Bob share a Bell pair. Show that Alice can transmit two classical bits of information to Bob by applying suitable Pauli operators to the qubit in her possession and then sending this single qubit to Bob.[24]

Superdense encoding is perhaps only surprising if you think that a qubit is an ordinary classical bit in disguise and overlook that entanglement is a vital resource in quantum communication. A much more striking application of Bell state preparation and measurement is quantum teleportation, but this is beyond the scope of this section because it needs three qubits.[25]

2.4. **The failure of spin polarisation*.** Spin polarisation is the principle that any single qubit[26] has a well-defined spin in some direction $\widehat{\mathbf{n}}$ in $\mathbb{R}^3$. We proved it in Exercise 1.3 by showing that the normalized state $\alpha|0\rangle + \beta|1\rangle$ is an eigenstate of $n_Z Z + n_X X + n_Y Y$ for suitable $(n_Z, n_X, n_Y) \in \mathbb{R}^3$. That this exercise is non-trivial should perhaps warn us that this principle is not

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

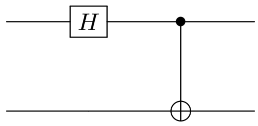
$$Y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

---

directly to this basis. In our example,

$$|10\rangle = \tfrac{1}{2}\big(|01\rangle + |10\rangle\big) - \tfrac{1}{2}\big(|01\rangle - |10\rangle\big) = \tfrac{1}{\sqrt{2}} X\,|\Phi\rangle + \tfrac{1}{\sqrt{2}} XZ\,|\Phi\rangle$$

and so $\langle \beta X|10\rangle = \frac{1}{\sqrt{2}}$, $\langle \beta XZ|10\rangle = \frac{1}{\sqrt{2}}$, and $\langle \beta|10\rangle = \langle \beta Z|10\rangle = 0$. Therefore projection of $|10\rangle$ to the Bell basis gives $|X\beta\rangle$ and $|XZ\beta\rangle$ with equal probability, corresponding to the measurement results $(1,0)$ and $(1,1)$ reported by our gadget, but now *these* Bell basis states are the two possible results of measurement. One can extend the gadget so that it truly 'measures in the Bell basis' by having it apply the reverse of the measurement circuit, as shown below,



to each of the four possible states $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, $|1\rangle|1\rangle$ that are the outputs of the original gadget.

[24]**Solution:** Alice applies either I, X, Z or XZ. Bob receives the qubit and then measures both his qubits using the gadget above. By the table, his pair of measurements distinguishes the four cases.

[25]**But anyway:** to demonstrate quantum teleportation algebraically, use the identity $\big(\alpha|0\rangle + \beta|1\rangle\big)\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = \frac{1}{2}\sum_{P \in \{I,X,Z,XZ\}} \frac{1}{\sqrt{2}} P\big(|00\rangle + |11\rangle\big) P\big(\alpha|0\rangle + \beta|1\rangle\big)$ to show that when Alice measures the first two qubits of

$$\big(\alpha|0\rangle + \beta|1\rangle\big)\,|\Phi\rangle = \tfrac{1}{\sqrt{2}}\big(\alpha|0\rangle + \beta|1\rangle\big)\big(|00\rangle + |11\rangle\big)$$

by projecting to the Bell basis (see footnote 23 'Pitfall' above), the result is

$$P\,|\Phi\rangle = \tfrac{1}{\sqrt{2}} P\big(|00\rangle + |11\rangle\big) P\big(\alpha|0\rangle + \beta|1\rangle\big),$$

where P is one of I, X, Z or XZ each with equal probability. Thus Bob now has the qubit $\alpha|0\rangle + \beta|1\rangle$ originally held by Alice, up to a Pauli correction that Alice will have to send him by two classical bits; this correction is the only reason why quantum teleportation does not violate causality. (Look up 'No communication theorem' for a precise formulation of this, and see also §4.1 for the related 'No cloning theorem'.) Quantum teleportation is more elegant in the ZX-calculus (you can easily find this on the web, but of course I like the account in my blog post `https://wildonblog.wordpress.com/2021/10/24/q-is-for-quantum/` reviewing Rudolph's book *Q is for quantum* [11]) and exceptionally elegant in the string-diagram formalism, where it becomes the basic yank relation: see for instance [2, §3c].

[26]**Lie:** this is only true for particles of spin $\frac{1}{2}$ such as the electron. Photons are mathematically an equally good model for a qubit, but physically behave differently, because of circular polarisation.

nearly as obvious as it might seem from our naive idea of magnetism or spinning tops. (Hence all the fuss about the Bloch sphere in §1.4.) The Bell state shows that spin polarisation already fails for two qubits, or more.

Exercise 2.7. Alice has the first qubit of a Bell state and Bob the second. Show that the expected value of an Alice measurement of Z on the first qubit is zero. (The general definition of Z-basis measurement in Definition 4.1, but you will probably guess the right thing to do: it is mathematically intuitive, even if the physical consequences are less so!) Show that the same holds if Alice switches from measurement in the $\widehat{\mathbf{z}}$ direction to an arbitrary direction $\widehat{\mathbf{n}} \in \mathbb{R}^3$.[27] Resolve the apparent paradox, as stated in [13, page 167]: 'How can that be? How could we know *as much as can possibly be known* about the Alice-Bob system of two spins, and yet know *nothing* about the individual spins that are its subcomponents?'[28] I took 'the theoretical minimum' in the title for these notes from the title of [13], and can highly recommend it as an introduction to quantum mechanics.

Exercise 2.8. Show that $E = X \otimes X + Y \otimes Y + Z \otimes Z$ is an observable of states in the Bell basis (or stated mathematically, the Bell states are its eigenvectors) and that its eigenvalues distinguish the *spin singlet* state $\frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$ from the other three elements of the Bell basis. What is the representation theoretic interpretation of this?[29]

---

[27]**Solution:** when Alice measures the first qubit of $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ in the Z-basis, she projects to $|00\rangle$ and $|11\rangle$ with equal probability; the measurement results are 0 and 1, corresponding to eigenvalues $+1$ and -1 respectively. Therefore her results are flat random and the expectation is 0. More generally, using the formula $\langle\psi|K\psi\rangle$ for the expectation value of the Hermitian operator K on the normalized state $|\psi\rangle$ we have

$$\begin{aligned}\langle\psi|n_X(X\otimes I) + n_Y(Y\otimes I) + n_Z(Z\otimes I)\psi\rangle \\ = n_X\langle\psi|X\psi\rangle + in_Y\langle\psi|XZ\psi\rangle + n_Z\langle\psi|Z\psi\rangle = 0+0+0 = 0;\end{aligned}$$

this symmetry of the Bell state becomes less surprising if one calculates that $|\Phi\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle\,|+\rangle + |-\rangle\,|-\rangle\big)$; on this calculation, I cannot resist quoting Maudlin's book *Philosophy of physics: Quantum theory* [6, page 71, footnote 6]: '*It's just a little painless algebra that anyone can do, and doing it produces a sense of accomplishment and understanding that can be acquired in no other way*'.

[28]**Solution(?):** for this author, a satisfactory resolution of the paradox is to declare that, in the context of the Bell state — and more generally in any state not factorizing as a tensor product of a state in $\mathcal{H}$ and a state in $\mathcal{H}^{\otimes(n-1)}$ — there is not such thing as an individual spin. This is not satisfactory to many physicists, since they are well used to measuring exactly this quantity; see footnote 4 for a less precise variation on this theme.

[29]**Answer:** we have seen that $X\otimes X$ and $Z\otimes Z$ are stabilisers of $|\Phi\rangle$. Hence so is $(X\otimes X)(Z\otimes Z) = -iXZ\otimes iXZ = -Y\otimes Y$ and it follows that $E\,|\Phi\rangle = (1+1-1)\,|\Phi\rangle = |\Phi\rangle$. Using that distinct Pauli matrices anticommute, we have

$$\begin{aligned}E(X\otimes I) &= (X\otimes X)(X\otimes I) + (Y\otimes Y)(X\otimes I) + (Z\otimes Z)(X\otimes I)\\ &= (X\otimes I)(X\otimes X) - (X\otimes I)(Y\otimes Y) - (X\otimes I)(Z\otimes Z),\end{aligned}$$

and so, using the unambiguous notation of the previous subsection, $E(X\,|\Phi\rangle) = X\,|\Phi\rangle + X\,|\Phi\rangle - X\,|\Phi\rangle = X\,|\Phi\rangle$. Similarly $E(Z\,|\Phi\rangle) = Z\,|\Phi\rangle$. For XZ we have

$$E(XZ\otimes I) = -(XZ\otimes I)(X\otimes X) + (XZ\otimes I)(Y\otimes Y) - (XZ\otimes I)(Z\otimes Z)$$

3. Many qubits: quantum computation

In this section we show that quantum computers are amazingly good at computing the Discrete Fourier Transform. From the point of view of this section, which emphasises the symmetry between the Z-basis and X-basis, this comes down to a simple change-of-basis. As a corollary we prove that a quantum computer can solve certain problems on Boolean functions using exponentially fewer logic gates than classical computers.

3.1. Z-basis.

The correct way to model n qubits is by the tensor product $\mathcal{H} \otimes \cdots \otimes \mathcal{H}$ which we usually denote $\mathcal{H}^{\otimes n}$. Given $v \in \mathbb{F}_2^n$ let

$$|v\rangle = |v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle \in \mathcal{H}^{\otimes n}.$$

Thus $\mathcal{H}^{\otimes n}$ is a 2^n-dimensional space having as an orthonormal basis $|v\rangle$ for $v \in \mathbb{F}_2^n$. This is the *Z-basis* of $\mathcal{H}^{\otimes n}$ of eigenvectors for $Z \otimes Z \otimes \cdots \otimes Z$. Note this notation is consistent with our earlier $|0\rangle, |1\rangle \in \mathcal{H}$ and $|00\rangle, |01\rangle, |10\rangle, |11\rangle \in \mathcal{H} \otimes \mathcal{H}$. We emphasise the distinction between the two vector spaces $\mathcal{H}^{\otimes n}$ and $\mathbb{F}_2$:

- $\mathcal{H}^{\otimes n}$ is the 2^n-dimensional complex Hilbert space modelling n qubits;
- $\mathbb{F}_2^n$ is a finite $\mathbb{F}_2$-vector space whose elements index the Z-basis of $\mathcal{H}^{\otimes n}$.[30]

We say that a state $|\psi\rangle$ is *normalized* if $\langle\psi|\psi\rangle = 1$, or equivalently, if $\sum_{v\in\mathbb{F}_2^n} |a_v|^2 = 1$, where $|\psi\rangle = \sum_{v\in\mathbb{F}_2^n} a_v |v\rangle$.

Definition 3.1 (Z-basis measurement of all qubits)**.** Let $|\psi\rangle = \sum_{v\in\mathbb{F}_2^n} a_v |v\rangle$ be a normalized state. *Measuring $|\psi\rangle$ in the Z-basis* projects it to $|v\rangle$ with probability $|a_v|^2$. The measurement result is $v \in \mathbb{F}_2^n$.

Again let us observe the traditional pause to remember that *measurement changes the state.*

---

and so $E(XZ|\Phi\rangle) = -XZ|\Phi\rangle - XZ|\Phi\rangle - XZ|\Phi\rangle = -3XZ|\Phi\rangle$. Therefore E has eigenvalue -3 on the spin singlet state $XZ|\Phi\rangle$ and eigenvalue 1 on the other Bell basis states. The representation-theoretic significance is that E commutes with the action of SU_2 on $\mathcal{H}\otimes\mathcal{H}$ and so, as expected from Schur's Lemma, its eigenspaces split $\mathcal{H}\otimes\mathcal{H}$ into its two irreducible subrepresentations, namely $\bigwedge^2\mathcal{H} = \langle |01\rangle - |10\rangle \rangle$ and $\mathrm{Sym}_2\mathcal{H} = \langle |00\rangle, |11\rangle, |01\rangle + |10\rangle \rangle$. If you have ever sat through a lecture on $\mathsf{sl}_2(\mathbb{C})$ in which the lecturer pulled the Casimir element $\frac{1}{2}h\otimes h + e\otimes f + f\otimes e \in \mathcal{U}(\mathsf{sl}_2(\mathbb{C}))$ out of a hat, you might be amused that interpreted in su_2, it is, up to a scalar, $X\otimes X + Y\otimes Y + Z\otimes Z$, lying in the quadratic component of the universal enveloping algebra $\mathcal{U}(\mathsf{su}_2)$. Here the $\mathsf{sl}_2(\mathbb{C})$-generators are

$$h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

and the claim follows from the isomorphism $\mathsf{su}_2 \otimes_{\mathbb{R}} \mathbb{C} \cong \mathsf{sl}_2(\mathbb{C})$ defined by $-\frac{iZ}{2} \mapsto \frac{ih}{2}$, $-\frac{iX}{2} \mapsto \frac{1}{2}(e-f)$, $-\frac{iY}{2} \mapsto \frac{i}{2}(e+f)$, where the su_2 generators are as in footnote 11. This is one of the best examples the author knows where a physical motivation has a clear benefit in a non-trivial pure mathematics problem.

[30] **Aside, please ignore if it is not helpful to you:** a slightly similar indexing scheme occurs in the theory of ϑ functions where lattice points in $\mathbb{R}^2$ index an orthonormal basis of an infinite dimensional Hilbert space.

3.2. **Transverse Hadamard.** We saw earlier that the one-qubit Hadamard gate satisfies $H\left|0\right\rangle = \left|+\right\rangle$ and $H\left|1\right\rangle = \left|-\right\rangle$. It will now be useful to combine the cases by writing

$$(\star) \qquad H|b\rangle = \tfrac{1}{\sqrt{2}}\big(\left|0\right\rangle + (-1)^b \left|1\right\rangle\big).$$

for $b \in \mathbb{F}_2$. The n-fold tensor product $H \otimes \cdots \otimes H = H^{\otimes n}$ is a unitary transformation of $H^{\otimes n}$; it is sometimes called *transverse Hadamard* to emphasise that one H gate is applied to each qubit separately. Let $\cdot$ denote the dot product on $\mathbb{F}_2^n$, defined as usual by $v \cdot w = v_1 w_1 + \cdots + v_n w_n \in \mathbb{F}_2$.

Lemma 3.2 (Transverse Hadamard)**.** *Given $v \in \mathbb{F}_2^n$ we have*

$$H^{\otimes n}\left|v\right\rangle = \frac{1}{2^{n/2}} \sum_{w \in \mathbb{F}_2^n} (-1)^{v \cdot w} \left|w\right\rangle .$$

Proof. Using $(\star)$ for the second equality we have

$$\begin{aligned}
H^{\otimes n}\left|v\right\rangle &= H\left|v_1\right\rangle \otimes \cdots \otimes H\left|v_n\right\rangle \\
&= \tfrac{1}{\sqrt{2}}\big(\left|0\right\rangle + (-1)^{v_1}\left|1\right\rangle\big) \otimes \cdots \tfrac{1}{\sqrt{2}}\big(\left|0\right\rangle + (-1)^{v_n}\left|1\right\rangle\big) \\
&= \frac{1}{2^{n/2}} \Big(\sum_{w_1 \in \mathbb{F}_2} (-1)^{v_1 w_1} \left|w_1\right\rangle \Big) \otimes \cdots \otimes \Big(\sum_{w_n \in \mathbb{F}_2} (-1)^{v_n w_n} \left|w_n\right\rangle \Big) \\
&= \frac{1}{2^{n/2}} \sum_{w_1, \ldots, w_n \in \mathbb{F}_2} (-1)^{v_1 w_1 + \cdots + v_n w_n} \left|w_1\right\rangle \ldots \left|w_n\right\rangle \\
&= \frac{1}{2^{n/2}} \sum_{w \in \mathbb{F}_2^n} (-1)^{v \cdot w} \left|w\right\rangle
\end{aligned}$$

as required. □

3.3. X**-basis.** The X-*basis* of $\mathcal{H}^{\otimes n}$ is $H^{\otimes n}\left|v\right\rangle$ for $v \in \mathbb{F}_2^n$. For example the X-basis of $\mathcal{H}^{\otimes 2}$ is shown left below, with the change of basis matrix $H^{\otimes 2}$ to the right, using our usual order $\left|00\right\rangle, \left|01\right\rangle, \left|10\right\rangle, \left|11\right\rangle$.

$$\begin{aligned}
\left|+\right\rangle\left|+\right\rangle &= H^{\otimes 2}\left|00\right\rangle = \tfrac{1}{2}\big(\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle\big) \\
\left|+\right\rangle\left|-\right\rangle &= H^{\otimes 2}\left|01\right\rangle = \tfrac{1}{2}\big(\left|00\right\rangle - \left|01\right\rangle + \left|10\right\rangle - \left|11\right\rangle\big) \\
\left|-\right\rangle\left|+\right\rangle &= H^{\otimes 2}\left|10\right\rangle = \tfrac{1}{2}\big(\left|00\right\rangle + \left|01\right\rangle - \left|10\right\rangle - \left|11\right\rangle\big) \\
\left|-\right\rangle\left|-\right\rangle &= H^{\otimes 2}\left|11\right\rangle = \tfrac{1}{2}\big(\left|00\right\rangle - \left|01\right\rangle - \left|10\right\rangle + \left|11\right\rangle\big)
\end{aligned}
\qquad
\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

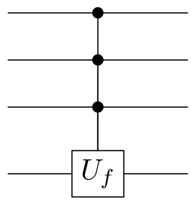
Up to the scalar $2^{-n/2}$, $H^{\otimes n}$ is the character table of $\mathbb{F}_2^n$, having as its rows the characters of $\mathbb{F}_2^n$. Depending on your background, this may make the application to Boolean functions below seem almost inevitable; if not, well great, you can now regard a large part of classical cryptanalysis as an application of basic character theory.

3.4. **Controlled gates.** Given a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ on n bits, how can we implement f as a quantum gate? For example, what unitary transformation will encode logical AND, defined by $f(x, y) = xy$? It is well worth finding the answer for yourself. As a hint, consider the case $n = 1$ aiming to implement NOT using two qubits. Remember that since quantum gates are unitary maps, and so invertible, the input bits must be recoverable from the output.

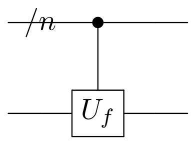
Definition 3.3 (Controlled gates)**.** Given $f : \mathbb{F}_2^n \to \mathbb{F}_2$ a Boolean function, *controlled* f is the unitary map on $n+1$ qubits defined on the Z-basis of $\mathcal{H}^{\otimes(n+1)}$ by

$$U_f \left|v\right\rangle \left|b\right\rangle = \left|v\right\rangle \left|b + f(v)\right\rangle$$

where $v \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$.



Observe that since the Z-basis of $\mathcal{H}^{\otimes(n+1)}$ is permuted by U_f, this map is unitary, as required. Taking $n = 1$ and $f(x) = x$ we recover the CNOT operator and taking $n = 2$ and $f(x, y) = xy$ gives the Toffoli gate (see [9, page 159]) that is the quantum analogue of logical AND. The circuit diagram in the margin shows how to draw U_f when $n = 3$; the three black dots indicate that the output qubit is controlled on all 3 input qubits. For general n a tick is used to indicate there are n input wires.



If you would like to find your own path to Theorem 3.6 a good start is the following question. For the author, at least half its interest lies in the fact that it can be stated *at all*: do programs in your favourite classical programming language have eigenvectors?

Exercise 3.4. What are the eigenvectors and eigenvalues of U_f?[31]

3.5. **Graph states.** Generalizing Exercise 2.1, considering what happens when we apply U_f to an input that is not a Z-basis state, but instead a superposition, such as $\left|+\right\rangle\left|+\right\rangle$ seen in §3.3. As in this exercise, it is immediate from linearity that

$$U_f\big(\left|+\right\rangle \ldots \left|+\right\rangle \left|0\right\rangle\big) = \tfrac{1}{2^{n/2}} \sum_{v \in \mathbb{F}_2^n} U_f \left|v\right\rangle \left|0\right\rangle = \tfrac{1}{2^{n/2}} \sum_{v \in \mathbb{F}_2^n} \left|v\right\rangle \left|f(v)\right\rangle .$$

Thus it is tempting to say that a quantum computer computes 'all the values of a function at once'. The state above is the quantum encoding of the graph of f. For the circuit diagram see Figure 2 below.

Exercise 3.5. What is the result of measuring the graph state above in the Z-basis? Are you yet persuaded to splash out on a quantum computer?[32]

Now see what happens if we change to the X-basis *everywhere*.

3.6. **Moving the output to the phase.** A standard trick in quantum computing is to move a computational result such as $\left|f(v)\right\rangle$ to the phase of its qubit, by replacing an input $\left|0\right\rangle$ with $\left|-\right\rangle$: thus

$$\begin{aligned} U_f \left|v\right\rangle\left|-\right\rangle &= \tfrac{1}{\sqrt{2}} U_f\big(\left|v\right\rangle\left|0\right\rangle - \left|v\right\rangle\left|1\right\rangle\big) \\ &= \tfrac{1}{\sqrt{2}}\big(\left|v\right\rangle\left|f(v)\right\rangle - \left|v\right\rangle\left|\overline{f(v)}\right\rangle\big) = (-1)^{f(v)} \left|v\right\rangle\left|-\right\rangle \end{aligned}$$

[31]**Solution:** for each $w \in \mathbb{F}_2^n$, $\left|w\right\rangle\left|+\right\rangle$ is an eigenvector with eigenvalue 1; $\left|w\right\rangle\left|-\right\rangle$ is an eigenvector with eigenvalue $(-1)^{f(w)}$. This is part of the calculation in §3.6.

[32]**Solution:** by Definition 3.1, the measurement projects the state to some $\left|v\right\rangle\left|f(v)\right\rangle$ where v is distributed uniformly at random on $\mathbb{F}_2^n$. This is clearly *worse* than a classical computer, because you don't even get to choose v.

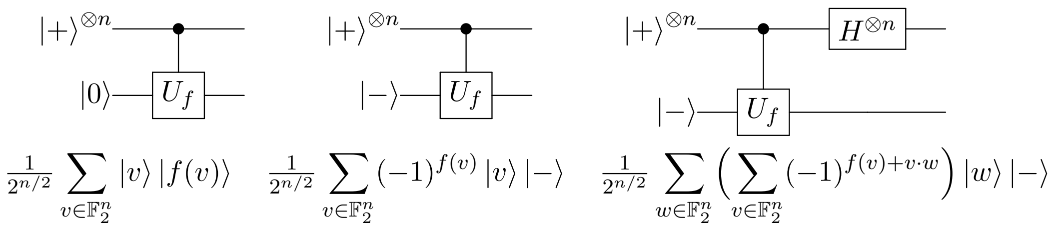


FIGURE 2. Final outputs of circuit for U_f where $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function: (1) graph circuit; (2) result moved to phase; (3) with $H^{\otimes n}$, computing $\sum_{w \in \mathbb{F}_2^n} c_f(w) \left|w\right\rangle \left|-\right\rangle$.

and so, as shown in the middle circuit in Figure 2,

$$U_f\big(\left|+\right\rangle \ldots \left|+\right\rangle \left|-\right\rangle\big) = \tfrac{1}{2^{n/2}} \sum_{v \in \mathbb{F}_2^n} U_f \left|v\right\rangle \left|-\right\rangle = \tfrac{1}{2^{n/2}} \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)} \left|v\right\rangle \left|-\right\rangle .$$

3.7. **The Quantum Discrete Fourier Transform in $\mathbb{F}_2^n$.** We now move the output to the X-basis as well by applying a final transverse Hadamard on the first n-qubits. Calculating using Lemma 3.2 and the previous result gives

$$\begin{aligned}
(H^{\otimes n} \otimes I)U_f\big(\left|+\right\rangle \ldots \left|+\right\rangle \left|-\right\rangle\big) &= \frac{1}{2^{n/2}} \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)} \big(H^{\otimes n} \left|v\right\rangle\big) \left|-\right\rangle \\
&= \frac{1}{2^{n/2}} \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)} \sum_{w \in \mathbb{F}_2^n} (-1)^{v \cdot w} \left|w\right\rangle \left|-\right\rangle \\
(\dagger) \qquad &= \sum_{w \in \mathbb{F}_2^n} \frac{1}{2^n} \Big(\sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)+v \cdot w} \Big) \left|w\right\rangle \left|-\right\rangle .
\end{aligned}$$

The quantity $\frac{1}{2^n} \sum_{v \in \mathbb{F}_2^n} (-1)^{f(v)+v \cdot w}$ is the *correlation* between f and the linear map $v \mapsto v \cdot w$. We shall denote it $c_f(w)$. Observe that

$$c_f(w) = \mathbb{P}_v[f(v) = v \cdot w] - \mathbb{P}_v[f(v) \neq v \cdot w]$$

where the probability is with respect to v uniformly distributed over $\mathbb{F}_2^n$. Since $H^{\otimes n} \otimes I$ is unitary, and so norm preserving, we have $\sum_{v \in \mathbb{F}_2^n} c_f(v)^2 = 1$. Correlations even slightly greater than the average $2^{-n/2}$ can often be used as the basis of a cryptographic attack, but, using only a classical computer, it appears there is no efficient way to find them.

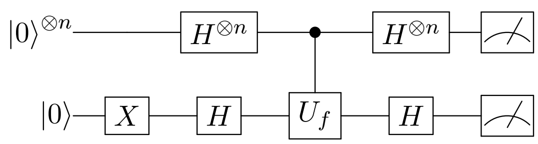
Theorem 3.6 (Quantum Discrete Fourier Transform in $\mathbb{F}_2^n$)**.** *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. There is a quantum circuit with input $\left|0\right\rangle^{\otimes(n+1)}$, using one X gate, $2(n+1)$ Hadamard gates and one controlled U_f gate, that prepares the state $\sum_{v \in \mathbb{F}_2^n} c_f(v) \left|v\right\rangle \left|1\right\rangle$. Measuring this state in the Z-basis returns $\left|v\right\rangle \left|1\right\rangle$ with probability $c_f(v)^2$. Computing the exact value of any single $c_f(v)$ by a classical computer requires 2^n evaluations of f.*

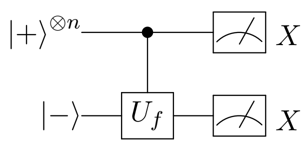
Proof. Since

$$H^{\otimes(n+1)}(I^{\otimes n} \otimes X) \left|0\right\rangle^{\otimes n} = (H^{\otimes n} \otimes H)\big(\left|0\right\rangle^{\otimes n} \otimes \left|1\right\rangle\big) = \left|+\right\rangle^{\otimes n} \left|-\right\rangle$$

we can prepare the input state for the rightmost circuit in Figure 2 using n Hadamard gates and one X-gate. The circuit itself uses one U_f gate and n Hadamard gates, and we use one further Hadamard gate to switch the final qubit $|-\rangle$ to $|1\rangle$, just to make the final Z-basis measurement deterministic on the final qubit. The theorem now follows from the definition of correlation and the previous calculation (†). □

The circuit in Theorem 3.6 is shown left below. On the right is the equivalent version where we prepare and measure in the X-basis. Its simplicity is a compelling demonstration of the power of changing the basis!





3.8. **Deutsch–Jozsa.** You are given $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and told that *either*

- f is constant *or*
- f is balanced, equal to 0 and 1 with equal probability.

The output of the circuit for Theorem 3.6 is $|0\rangle\,|0\rangle$ in the first case, and, since a balanced function has zero correlation with the constant 'all-ones' function, $|w\rangle\,|0\rangle$ for some $w \neq 0$ in the second case. (Note this is after measuring.) Thus only one use of U_f is required to distinguish the two cases. To decide classically requires, in the adversarial worst case, $2^{n-1} + 1$ evaluations of f. While of little (no?) practical importance, the Deutsch–Jozsa Problem was one of the first examples of a problem that could be solved by a quantum algorithm *exponentially faster* than any deterministic classical algorithm.[33]

3.9. **Shor's algorithm.** Shor's algorithm makes an ingenious use of the Quantum Discrete Fourier Transform, but now working in the group $\mathbb{Z}/2^n\mathbb{Z}$, to find the period of, for instance, the doubling function $x \mapsto 2^x \bmod N$, and so (by an easy classical endgame that uses a largish prime factor of $\phi(N)$) factor N. Because the Fourier transform has to be taken in $\mathbb{Z}/2^n\mathbb{Z}$ rather than $\mathbb{Z}/\phi(N)\mathbb{Z}$, there is a small probability of error[34]; this can be made exponentially small by running the algorithm polynomially many times.[35]

[33]**Objection:** three evaluations of f give a classical algorithm guaranteed to succeed when f is constant, and with error probability $\frac{1}{4}$ when f is balanced. This error probability can, as usual, be made arbitrarily small by repeated runs of the algorithm. Thus the Deutsch–Jozsa problem is in BPP. Simon's Problem shows that a probabilistic quantum algorithm (in the class BQP) may be exponentially faster than any probabilistic classical algorithm; again this uses the Quantum Discrete Fourier Transform on $\mathbb{F}_2^n$ but now with n output bits: see [8, §2.5].

[34]**Why:** for RSA numbers $N = pq$, because finding $\phi(pq) = pq - p - q + 1$ is exactly as hard as factoring pq

[35]**Reference:** see [9, §5.1]. Or better, read the easier and more motivated following section §5.2 on phase estimation, and then work out the circuit in §5.1 for yourself. For an excellent exposition of the ideas that follows this order, see §10.8 and §10.9 in [3].

3.10. **BQP and complexity theory⋆.** The complexity class EXACTQP is, roughly put, all problems solvable on a quantum computer starting at the $|0\rangle^{\otimes n}$ state for some chosen n, applying polynomially many gates — drawn from a fixed universal gate set[36] — and then measuring the result in the Z-basis. (The principle of deferred measurement implies that, perhaps contrary to one's intuition, allowing multiple measurements does not boost the computational power.[37]) Because quantum computers can be used to simulate classical computers, EXACTQP contains P. Shor's algorithm lies in the bigger class BQP in which a bounded probability of error is allowed. Thus Shor's algorithm shows that BQP contains a problem widely believed to be in NP but not in P. It is possible that BQP contains NP, or that NP contains BQP, and both possibilities are consistent with $\mathsf{P} = \mathsf{NP}$. It is much more widely believed that neither of BQP nor NP contains the other; in this case $\mathsf{P} \neq \mathsf{NP}$ and, as shown in Figure 3, factoring is an example of a problem in the intersection of BQP and NP that may not also be in P.[38]

Oracles. It is important to note that the quantum gate U_f and the classical subroutine implementing f are each given as a black box. For the Deutsch–Jozsa problem, it is conceivable that, knowing how f is implemented as a sequence of polynomially many classical logic operations, one can quickly tell whether f is constant or balanced, without having to evaluate f at all.[39] Thus all we have proved is that EXACTQP, and so BQP, properly contain P *when both are taken relative to a polynomial time oracle.*

3.11. **Unitary gates and the Schrödinger equation⋆.** We finish by motivating our assumption that quantum gates are unitary, and making the connection with quantum mechanics as you probably were first taught it.

Why unitary gates. Our statement of the Born rule (see Definition 1.2) strongly motivates the axiom that quantum states evolve in a way that *preserves their norm.* It is a nice exercise in sesquilinear algebra to show that if $\mathcal{K}$ is a Hilbert space and $L : \mathcal{K} \to \mathcal{K}$ is a norm-preserving linear map

[36]**Universal gate set:** a popular choice is the S gate (which satisfies $S^2 = Z$), the Hadamard gate H, the CNOT gate, and one extra gate, such as the T-gate (which satisfies $T^2 = S$), or the 3-qubit Toffoli gate; this extra gate makes the step from the finite Clifford subgroup of U_{2^n} to a countable dense subgroup of U_{2^n}. Roughly put, the Solovay–Kitaev theorem states that an arbitrary unitary gate can be well-approximated by an efficient *and efficiently findable* composition of gates from the chosen generating set. Still this approximation process introduces some overhead; this is one motivation for measurement-based quantum computation, in which the overhead reappears as a sometimes more manageable cost in making ancilla states.

[37]**Caveat:** provided no errors occur. Repeated measurement is vital to quantum error correction, see §4.4.

[38]**Reference:** for much more on this see [1].

[39]**Aside:** to make this seem less likely, reflect that the hash function SHA-256 is implemented as a sequence of polynomially many simple operations, but almost certainly you do not have a quick way to produce inputs whose outputs end with lots of zeros.

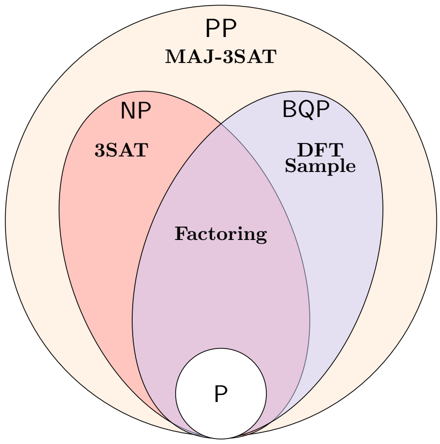


FIGURE 3. One possible configuration of the complexity theory landscape. PP is (although not by the usual definition) the class of decision problems solvable in polynomial time with error probability for *either* answer strictly less than $\frac{1}{2}$. For example 3SAT is in PP: guess an assignment of the n variables and if it works, reports SAT; otherwise report UNSAT with probability $\frac{1}{2}+\frac{1}{2^{n+1}}$. The decision problem **MAJ-3SAT** asks 'do the majority of assignments satisfy the 3SAT clauses': it is unlikely to have a polynomial time certificate. Decision problems based on sampling DFT coefficients, such as Deutsch–Jozsa and Simon's Problem are in BQP, and (see the subsection on oracles below) may not in P. It is known that P $\subseteq$ NP $\subseteq$ PP $\subseteq$ PSPACE $\subseteq$ EXPTIME and that at least one of these containments is proper.

then L is unitary.[40] So let's take this also as axiomatic. Then we can suppose that a gate is a smooth family of unitary maps $t \mapsto U(t)$ for $0 \le t \le 1$, and that what we see in our quantum computer are the outputs $U(1)\,|\psi(0)\rangle$ where $|\psi(0)\rangle$ is our starting state, for instance a zero qubit.[41] By a familiar argument from naive Lie theory, we have $U(\varepsilon) = I + \varepsilon M + O(\varepsilon^2)$ for some matrix M which, since $U(\varepsilon)$ is unitary, satisfies

$$(I + \varepsilon \overline{M})^{\mathrm{t}}(I + \varepsilon M) = I + O(\varepsilon^2).$$

Thus $\overline{M}^{\mathrm{t}} + M = 0$, and so $\overline{M}^{\mathrm{t}} = -M$. That is, M is anti-Hermitian. We may therefore write $M = -iH$ for some Hermitian H. We choose the minus sign so that the punchline of this section does not need a sign change.

To the Schrödinger equation. Mathematically, it is appealing to suppose that $U(t)$ is in fact the one-parameter subgroup

$$t \mapsto \exp(-iHt)$$

[40]**Outline proof:** given any v, $w \in \mathcal{K}$ we have $||v+w||^2 = ||v||^2 + ||w||^2 + 2\,\mathrm{Re}\,\langle v|w\rangle$ and $||L(v+w)||^2 = ||Lv||^2 + ||Lw||^2 + 2\,\mathrm{Re}\,\langle Lv|Lw\rangle$. Since L is norm preserving, we have $\mathrm{Re}\,\langle v|w\rangle = \mathrm{Re}\,\langle Lv|Lw\rangle = \mathrm{Re}\,\langle v|\overline{L}^{\mathrm{t}}Lw\rangle$, implying that $\mathrm{Re}\,\langle v|(\overline{L}^{\mathrm{t}}L - I)w\rangle = 0$. Since v was arbitrary, we may take $v = (\overline{L}^{\mathrm{t}}L - I)w$ to deduce that $\overline{L}^{\mathrm{t}}L - I = 0$, i.e. L is unitary.

[41]**Oversimplification:** we ignore that gates might use measurement 'under the hood'. Measurement is norm-preserving by the Born rule, but of course not unitary.

of the unitary group on $\mathcal{K}$. Supposing this is the case, we find that a starting state $|\psi(0)\rangle$ evolves as $|\psi(t)\rangle = \exp(-iHt)\,|\psi(0)\rangle$, and so satisfies the differential equation

$$\frac{\mathrm{d}\,|\psi(t)\rangle}{\mathrm{d}t} = -iH|\psi(t)\rangle\,.$$

The equation above is, up to a missing reduced Planck's constant, the Schrödinger equation

$$i\hbar\frac{\mathrm{d}\,|\psi(t)\rangle}{\mathrm{d}t} = H|\psi(t)\rangle\,.$$

One can work out that $\hbar$ should be on the left in the Schrödinger equation by remembering one other formula using Planck's constant and then using dimensional analysis on the Hamiltonian H.[42] (Another heuristic is that the energy given by applying the H operator is very small, whereas derivatives may be large, so we should scale the derivative by the tiny $\hbar \approx 1.05 \times 10^{-34}\mathrm{kg}\,\mathrm{m}^2\,\mathrm{s}^{-1}$.) See [13, §9.2] for why we should now take $H = -\frac{\hbar^2}{2m}\frac{\mathrm{d}^2}{\mathrm{d}x^2} + V(x)$ to model a non-relativistic particle of mass m moving in a potential V; substituting and replacing $|\psi(t)\rangle$ with a traditional wave function $\psi(t,x)$ gives Schrödinger equation in the form

$$i\hbar\frac{\mathrm{d}\psi(t,x)}{\mathrm{d}t} = -\frac{\hbar^2}{2m}\frac{\mathrm{d}^2\psi(t,x)}{\mathrm{d}x^2} + V(x)\psi(t,x)$$

you might recall from a traditional first course in quantum mechanics.[43]

4. Too many qubits: quantum error correction

This section is particularly idiosyncratic: we first develop just enough of the theory of stabiliser codes to give a carefully (maybe laboriously) motivated quantum code that will correct a single X-error, but will not guard against general quantum errors. We then show our construction is a special case of the key quantum technique of 'measuring a stabiliser' and use this to define error correction for the $[[7,1,3]]$-Steane code.

4.1. **Motivation: No cloning theorem.** In classical error correction we can discover the error, provided it is not *too* high weight, by direct examination of the data. The error is then a classical vector of bits. In quantum error correction, the data is a quantum state, and to avoid decohering it, we shall see that we must take great care to learn only the syndrome of the

[42]**Units:** you do not need quantum mechanics to derive that energy has units $\mathrm{kg}\,\mathrm{m}^2\,\mathrm{s}^{-2}$. From the formula $E = \hbar\nu$ for the energy of a photon in terms of its angular frequency, we deduce that $\hbar$ has units $\mathrm{kg}\,\mathrm{m}^2\,\mathrm{s}^{-1}$. (This formula is $E = hf$ in terms of the usual frequency $f = \nu/2\pi$.) Then since H is a Hamiltonian, with units of energy, dimensional consistency in Schrödinger equation requires that $\hbar$ appears on the left in $i\hbar\frac{\mathrm{d}|\psi(t)\rangle}{\mathrm{d}t}$. **To do: natural units**

[43]**Opinion:** isn't it about time such courses entered the 21st Century? Is it the misguided belief that solving differential equations is 'easy' whereas Hilbert spaces such as $\mathbb{C}^2$ and operators are 'hard' that stops this happening? Or perhaps Hilbert spaces are indeed 'hard': the Hilbert space relevant to the Schrödinger equation above is the space of time-dependent square-integrable functions on $\mathbb{R}$, on which the unitary operator e^{-iHt} is defined on a dense subset. See [5, Ch. 14] for a rigorous account of the Stone–von Neumann theorem.

error, and not the error itself. The error is resolved in the course of measurement to a combination of Pauli operators. We make this precise in §4.4. And, since the map $\mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ defined by $|\psi\rangle \mapsto |\psi\rangle\,|\psi\rangle$ is not even linear, and, as defined here, not invertible, there is no unitary map that we could use to back up quantum data. This is a simple version of the 'No cloning theorem': see [9, §1.3.5].

4.2. **Measurement for quantum error correction.** For quantum error correction one often needs to measure a subset of the qubits. Definition 3.1 (measurement of all qubits in the Z-basis) generalizes as follows.

Definition 4.1. [Z-basis measurement of some qubits] Let

$$|\psi\rangle = \sum_{v \in \mathbb{F}_2^m} |\psi_v\rangle \otimes a_v|v\rangle \in \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes m}$$

be a normalized state in which $\langle \psi_v | \psi_v \rangle = 1$ for all $v \in \mathbb{F}_2^m$. *Measuring* $|\psi\rangle$ *on the final* m *qubits in the* Z*-basis* projects it to $|\psi_v\rangle$ with probability $|a_v|^2$. The measurement result is v.

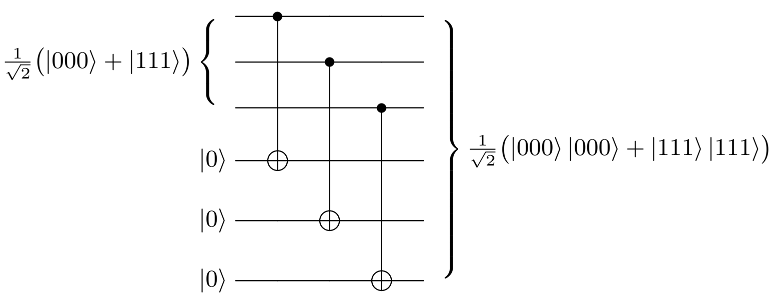
For example measuring the Bell state $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ in Exercise 2.1 on its second qubit projects it to $|00\rangle$ and $|11\rangle$ with equal probability; the measurement results are 0 and 1, respectively. Depending on your tolerance for the joke, one last traditional pause might now be observed.

4.3. **A toy code.** The classical length three repetition code $\{000, 111\} \subseteq \mathbb{F}_2^3$ can correct a single bit flip. Motivated by this, we might hope that the subspace $\mathcal{C}$ of $\mathcal{H}^{\otimes 3}$ spanned by $|000\rangle$ and $|111\rangle$ can be used as a quantum code to correct a single X-error. Here, by 'used as a quantum code', we mean that a general bare qubit $\alpha|0\rangle + \beta|1\rangle$ is *encoded* in $\mathcal{C}$ as the *data state*

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

and we have available a set of *logical gates* that implement the usual single qubit gates X, Z and H directly on the encoded qubits.[44] Decoding an

[44]**Logical operations:** the transverse operator $X \otimes X \otimes X$ swaps $|000\rangle$ and $|111\rangle$ and so implements logical X, and either $Z \otimes I \otimes I$ or the transverse $Z \otimes Z \otimes Z$ fixes $|000\rangle$ and flips the sign on $|111\rangle$, so implements logical Z. One limitation of this code is shown by the difficulty of implementing logical Hadamard. The circuit below implements logical CNOT between two different code blocks; the example has input $\frac{1}{\sqrt{2}}\big(|000\rangle + |111\rangle\big)\big)\,|000\rangle$ which is the tensor product of the logical plus $\frac{1}{\sqrt{2}}\big(|000\rangle + |111\rangle\big)$ and logical zero states $|000\rangle$; the output is the logical Bell state.



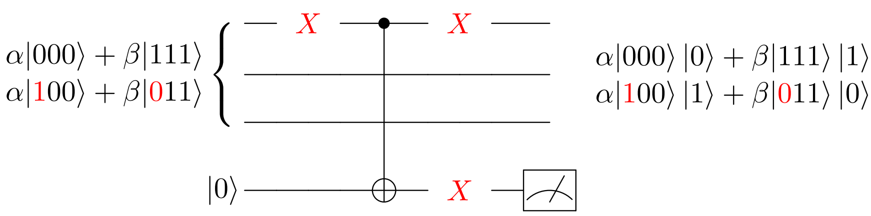
output state known to be either $|000\rangle$ or $|111\rangle$ to a single classical bit is easy: just measure every qubit in the Z-basis. But this also shows the basic problem in quantum error correction.

Exercise 4.2. Suppose that the data state $\alpha|000\rangle + \beta|111\rangle$ has an X-error on the first qubit, and so it is

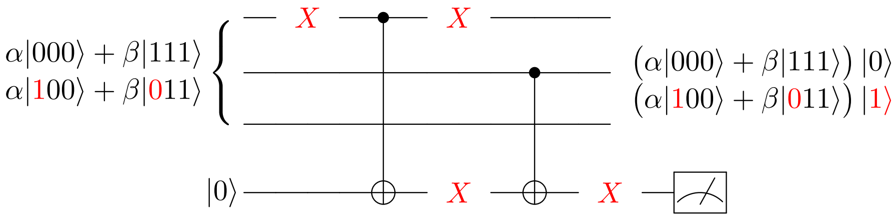
$$(X \otimes I \otimes I)\big(\alpha|000\rangle + \beta|111\rangle\big) = \alpha|100\rangle + \beta|011\rangle\,.$$

Arguing that in a healthy data state, the first two qubits are equal (in each Z-basis summand), we might decide to measure the first two qubits in the Z-basis. Is this a good plan?[45]

Measuring onto an ancilla. A key idea in quantum error correction is that rather than directly measuring the data state[46], we first interact the data state with a suitable ancilla, and then measure the ancilla. In this case a suitable ancilla is the zero qubit $|0\rangle$ and the necessary interaction can be done using CNOT gates. As an indication of how to perform this interaction, the diagram below shows a plausible but wrong circuit. Two possible input/output pairs are shown: the top is clean data, the bottom has an X-error on the first qubit copied to the ancilla.



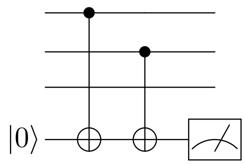
By Definition 4.1, measuring the ancilla collapses the data state: for instance if 0 is the measurement result that the new state is $|000\rangle\,|0\rangle$ if there is no error, or $|011\rangle\,|0\rangle$ if there is an error. The problem is that the ancilla *learns about the data state*: the measurement result determines not just whether or not there is an X-error on one of the first two qubits, but also distinguishes the two logical codewords $|000\rangle$ and $|111\rangle$. What if instead we could somehow learn just about the error, and nothing about the data? (This is your final chance to discover the key circuit for yourself.)



[45]**Solution:** by Definition 4.1, the measurement projects the data state to either $|000\rangle$ or $|111\rangle$ if there is no X-error, or to either $|100\rangle$ or $|011\rangle$ if the error is $X \otimes I \otimes I$, and the measurement result is 00, 11 or 10, 01, respectively, so we know which case applies. The operation is a success, but the patient dies: we have destroyed the superposition and lost the information in the coefficients α and β. This is *not* a successful decoding algorithm.

[46]**Trigger warning:** even the thought of this action makes the author feel uneasy.

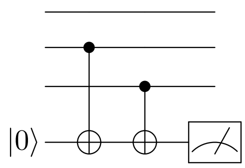
In this modified circuit we also CNOT from the second data qubit to the ancilla. This mirrors the parity check equation $x_1 + x_2 = 0$ satisfied by the classical codewords 000 and 111. In both cases, clean data and X-error, the output state is a pure tensor product of the input data state (with its X-error if relevant) and $|b\rangle$, where $b = 1$ if there is a single X-error on either of the first two qubits, and $b = 0$ otherwise. We may therefore measure the ancilla qubit without collapsing the data state. By Definition 4.1, the measurement result is 0 or 1 *and the data state is unchanged.*



Full syndrome information on X-errors for the toy code. Generally we may suppose (see §4.7 below) that the X-error is $X^{e_1} \otimes X^{e_2} \otimes X^{e_3}$ for some e_1, e_2, $e_3 \in \mathbb{F}_2$. For instance, a single X-error on the first qubit is $e = 100$. The circuit just defined (repeated in the margin) has measurement result $e_1 + e_2$. This is the syndrome for the first row of the parity check matrix

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

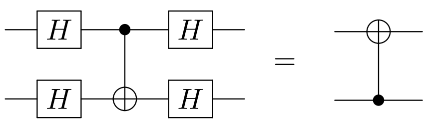
of the classical repetition code of length 3. Correspondingly $Z \otimes Z \otimes I$ is a stabiliser of our code: since $(Z \otimes Z \otimes I)\,|000\rangle = |000\rangle$ and $(Z \otimes Z \otimes I)\,|111\rangle = |111\rangle$, we have $(Z \otimes Z \otimes I)\,|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathcal{C}$. A similar circuit (see the margin) in which the CNOTs are from the second and third data qubits measures the syndrome for the second row. Correspondingly, $I \otimes Z \otimes Z$ is a stabiliser of $\mathcal{C}$. Therefore we may learn $e_1 + e_2$ and $e_2 + e_3$ which, since the classical repetition code of length 3 is 1-error correcting, is sufficient to determine the position of any single X-error.



Exercise 4.3. If the two measurement results are $(1, 1)$, what single gate will correct the data state? Assume that at most one X-error has occurred.[47]

An easy generalization of this exercise shows that the toy code can correct an arbitrary single X-error.

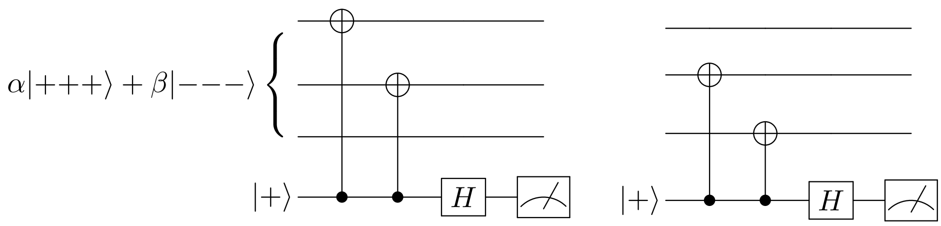
4.4. **Measuring a stabiliser.** To put this in a more general framework we dualize, as in §3, by applying Hadamard gates to everything in sight. By the identity $(H \otimes H)\,\mathrm{CNOT}_{12}(H \otimes H) = \mathrm{CNOT}_{21}$, diagrammed below,



this swaps the control and target in every CNOT gate. The *dual toy code* has codewords $|+\rangle\,|+\rangle\,|+\rangle$ and $|-\rangle\,|-\rangle\,|-\rangle$ which we abbreviate as $|{+}{+}{+}\rangle$ and $|{-}{-}{-}\rangle$ The dualized measurement circuits below now measure syndromes of Z-errors. The final measurement is, thanks to the H gate on the ancilla, correctly in the Z-basis; compare the two circuits ending §3.7. Note that by the copy rule for Z-faults, a single Z-fault on the data will be copied to

[47]**Solution:** the unique solution to $e_1 + e_2 = 1$ and $e_2 + e_3 = 1$ having $e \in \mathbb{F}_2^3$ of weight 1 is $e = 010$. We therefore correct by applying an X-gate to the second qubit.

the ancilla wires, swapped to an X-fault by the Hadamard gates, and then recorded by the measurement results.



Exercise 4.4. The stabilisers found above of $\mathcal{C}$ become stabilisers $X \otimes X \otimes I$ and $I \otimes X \otimes X$ of the dual code. Using this, show that in the absence of errors each circuit implements the identity operation.[48]

This exercise is the rigorous rephrasing of the property we saw is essential, that the ancilla should 'learn nothing about the data state'.

Example 4.5. Suppose that there is a Z-error on the first qubit. Thus, since $Z\,|+\rangle = |-\rangle$, the data state is $|\psi\rangle = \alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle$. To find the output of the first dualized circuit we could use the previous Exercise 4.4 and the copy rule for Z-faults. Instead, to motivate Lemma 4.6, we calculate

$$\begin{aligned}
&\mathrm{CNOT}_{41}\,\mathrm{CNOT}_{42}\big(\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle\big)\,|+\rangle \\
&\qquad = \mathrm{CNOT}_{41}\,\mathrm{CNOT}_{42}\big(\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle\big)\tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \\
&\qquad = \big(\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle\big)\tfrac{1}{\sqrt{2}}\,|0\rangle - \big(\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle\big)\tfrac{1}{\sqrt{2}}\,|1\rangle \\
&\qquad = \big(\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle\big)\tfrac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \\
&\qquad = \big(\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle\big)\,|-\rangle \\
&\qquad = |\psi\rangle\,|-\rangle
\end{aligned}$$

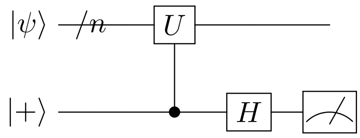
and deduce that, since $H\,|-\rangle = |1\rangle$, the measurement result is 1, with output data state $\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle$ unchanged from the input. The argument for the second circuit is very similar, but in this case, because $I \otimes X \otimes X$ commutes with $Z \otimes I \otimes I$, there is no Z-fault copied to the ancilla (see also Exercise 4.10 below; this copying up is called 'phase kick-back' in the setting of Lemma 4.6), and so the measurement result is 0. Again the output data state is unchanged from the input.

Observe that each Z-syndrome measurement circuit is an instance of the general *stabiliser measurement circuit* shown below, in which U is a unitary operator on $\mathcal{H}^{\otimes n}$ controlled on the bottom qubit. Exercise 4.4 and Example 4.5 generalizes as follows.

---

[48]**Solution:** in the first circuit, the controlled CNOTs specify $X \otimes X \otimes I$ on the data state, which is a stabiliser of the dual code. Thus, by a calculation similar to footnote 17 or the following Example 4.5, the controlled operation is the identity. (That $X \otimes X \otimes I$ *is* a stabiliser can be seen without going through the duality by noting that since $X\,|+\rangle = |+\rangle$, $X\,|-\rangle = -\,|-\rangle$, an arbitrary data state $\alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$ is stabilised by this circuit. The proof for the second circuit is very similar.

Lemma 4.6 (Measuring a stabiliser)**.** *Let* $U : \mathcal{H}^{\otimes n} \to \mathcal{H}^{\otimes n}$ *be a unitary map with eigenvalues* $+1$ *and* -1*. Let* $|\psi\rangle \in \mathcal{H}^{\otimes n}$ *be a normalized state with unique expression* $|\psi\rangle = |\psi_0\rangle + |\psi_1\rangle$ *as a linear combination of a* $+1$*-eigenvector of* U *and a* -1*-eigenvector of* U*. The output of the circuit below is* $|\psi_0\rangle |0\rangle$ *or* $|\psi_1\rangle |1\rangle$ *with probabilities* $\langle\psi_0|\psi_0\rangle$ *or* $\langle\psi_1|\psi_1\rangle$ *respectively, and measurement results* 0 *or* 1 *respectively.*



Proof. Suppose first of all that $|\psi\rangle$ is an eigenstate with eigenvalue ± 1. Then the output before the H gate on the control qubit or measurement is

$$\begin{aligned} \tfrac{1}{\sqrt{2}} |\psi\rangle |0\rangle + \tfrac{1}{\sqrt{2}} U |\psi\rangle |1\rangle &= \tfrac{1}{\sqrt{2}} |\psi\rangle |0\rangle \pm \tfrac{1}{\sqrt{2}} U |\psi\rangle |1\rangle \\ &= \tfrac{1}{\sqrt{2}} |\psi\rangle \big(|0\rangle \pm |1\rangle\big) = |\psi\rangle |\pm\rangle . \end{aligned}$$

Since $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$ it follows by linearity that the state created by the circuit just before measurement on a general $|\psi\rangle$ is $|\psi_0\rangle |0\rangle + |\psi_1\rangle |1\rangle$. Now by Definition 4.1, measuring the final qubit projects the state to either $|\psi_0\rangle$ or $|\psi_1\rangle$ with the claimed probabilities. □

Remark 4.7. Thus the stabiliser measurement circuit is the identity in the case where $|\psi\rangle$ is a stabiliser state of U, i.e. $U|\psi\rangle = |\psi\rangle$. The name 'stabiliser measurement' is perhaps misleading, but is standard.

The stabiliser measurement circuit can be used to perform all of quantum error correction. For instance, we just saw in Example 4.5 how to use it with X-gates in place for U (so the controlled gate is a composition of CNOTs) to get syndrome information about Z-errors on the dual toy code: specifically, the solution to Exercise 4.5 shows that $Z^{e_1}\big(\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle\big)$ is an eigenstate of $X \otimes X \otimes I$ with eigenvalue $(-1)^{e_1}$ and of $I \otimes X \otimes X$ with eigenvalue 1. Observe that these stabilisers correspond to the rows of the parity check matrix P of the classical repetition code of length 3 shown in §4.3 and repeated in the margin.[49] As a further demonstration, in §4.6, we use the syndrome measurement circuit to show how to decode the Steane code and to justify our implicit assumption that every quantum error is a combination of the Pauli X- or Z-operators.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Remark 4.8 (One circuit is all you need)**.** By Lemma 4.6, and as just seen from Exercise 4.5, the stabiliser measurement circuit performs phase estimation for eigenstates with ± 1 eigenvalues. It can be generalized to perform arbitrary phase estimation and hence, allowing ancillae on multiple

[49]**How it works for the toy code:** to use the stabiliser measurement circuit to get syndrome information about X-faults on the original toy code, we need to measure a Z-stabiliser, using gates controlled by the ancilla qubit. This can be done using CZ-gates. In §4.3, since the aim was to do everything using CNOT gates, we instead measured the Z-stabiliser in a way that is less obvious, using CNOT gates controlled by the *data* qubits. But the effect is the same. In [9, Figure 10.15] this is called a 'useful implication'.

qubits, the Quantum Discrete Fourier Transform on $\mathbb{Z}/2^n\mathbb{Z}$. A taste of this is given by the circuits for the Quantum Discrete Fourier Transform on $\mathbb{F}_2^n$ at the end of §3.7; note they are upside down for this section, having controls on the *top* wires.

4.5. **Fun with stabilisers*.** Here we use stabilisers to show that a class of 'locally realistic' interpretations of quantum theory are fundamentally flawed. Please skip to §4.6 if you want to get straight to the Steane code. Let $|\chi\rangle = \frac{1}{\sqrt{2}}\big(|000\rangle + |111\rangle\big)$ be the *cat state* on three qubits.[50] Since $|\chi\rangle$ lies in the toy code it is stabilised by $Z \otimes Z \otimes I$ and $I \otimes Z \otimes Z$. Clearly $X \otimes X \otimes X$ is also a stabiliser. Since $Y = iXZ$, it follows that

$$(X \otimes X \otimes X)(I \otimes Z \otimes Z) = X \otimes \tfrac{1}{i}Y \otimes \tfrac{1}{i}Y = -X \otimes Y \otimes Y$$

is a stabiliser. Noting the minus sign on the right-hand side, we deduce that $|\chi\rangle$ is a -1-eigenvector for $X \otimes Y \otimes Y$. Physically, this means that if three qubits are entangled in the cat state, and then measured in the x-, y- and y-directions, the product of the measured eigenvalues is -1. In a strong version of a *locally realistic* interpretation of quantum theory, there are hidden variables x_1, x_2, x_3, y_1, y_2, y_3 which are the deterministic, 'known to God', results of measuring the 3 qubits in the x- and y-directions. Thus $x_1y_2y_3 = -1$. By symmetry, we also have $y_1x_2y_3 = -1$ and $y_1y_2x_3 = -1$. Hence

$$x_1x_2x_3 = (x_1y_2y_3)(y_1x_2y_3)(y_1y_2x_3) = (-1)^3 = -1.$$

According to the locally realistic interpretation, this means that the result of measuring the 3-qubits all in the x-direction is -1. But since $X \otimes X \otimes X$ is a stabiliser of $|\chi\rangle$, in fact the result is 1.[51]

4.6. **The Steane $[[7,1,3]]$-code.** In §4.3 we made a quantum code whose Z-stabilisers $I \otimes I \otimes I$, $Z \otimes Z \otimes I$, $Z \otimes I \otimes Z$, $I \otimes Z \otimes Z$ corresponding to rows in the row-space of the parity check matrix P of the repetition code of length 3. The dual code has X-stabilisers obtained by replacing each Z with X, and these were what we measured in the previous subsection.

---

[50]**Etymology:** the cat state is named after Schrödinger's cat: by Definition 4.1, when any single qubit is measured in the Z-basis, the state collapses to either $|000\rangle$ or $|111\rangle$

[51]**Further remarks:** this *GHZ-experiment* is an improvement on the earlier 'Bell's paradox' experiment using two qubits entangled in the Bell state. This demonstrates a higher correlation between single qubit measurements that is possible with classical physics, but it is still conceivable (just overwhelmingly improbable) that a locally realistic theory gives the same results in repeated experiments. In contrast, the GHZ-experiment is 'one-shot': it has been performed in the laboratory using spatially separated qubits (so the hidden variables for qubit 2 cannot 'update' themselves after qubit 1 is measured, but just before qubit 2 is measured, without breaking causality). The account above is a simplified version of [7]. See also [6, Experiment 8, page 29]. Incidentally, Maudlin is clear that my interpretation of 'local realism' is unhelpful and too strong: 'Bell proved that no local theory, full stop, can predict violations of his inequality. ... If I had my druthers "realist" and "anti-realist" would be banned from these foundational discussions.' [6, page xiii]

A stabiliser code. We now copy this strategy replacing P with the parity check matrix of the Hamming $[[7,4,3]]$-code below, chosen so that for each $i \in \{1,\dots,7\}$, column i is the binary form of i.

$$P = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

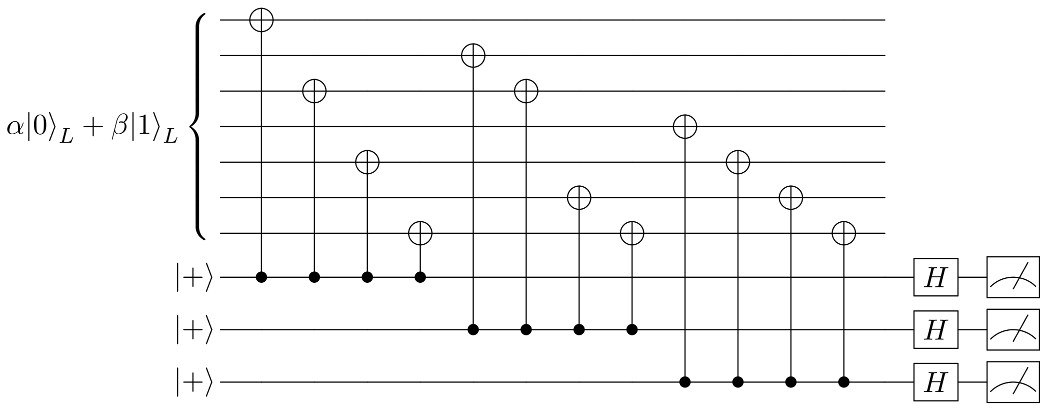
Given $u \in \mathbb{F}_2^7$, let $X^u = X^{u_1} \otimes \cdots \otimes X^{u_7}$ and similarly let $Z^w = Z^{w_1} \otimes \cdots \otimes Z^{w_7}$. The Steane code is then the subspace $\mathcal{C}$ of $\mathcal{H}^{\otimes 7}$ of all vectors fixed by each X^u and Z^w for $u, w \in \langle P \rangle_{\text{row}}$, the row span of P. Define the *zero-logical* and *one-logical* states by

$$|0\rangle_L = \frac{1}{\sqrt{2^3}} \sum_{v \in \langle P \rangle_{\text{row}}} |v\rangle$$

$$|1\rangle_L = \frac{1}{\sqrt{2^3}} \sum_{v \in \langle P \rangle_{\text{row}}} |\overline{v}\rangle$$

where $\overline{v} = v + 1111111$ is the bit flip of v. (The normalization factor is $\sqrt{2^3}$ because P has three linearly independent rows, and so $\langle P \rangle_{\text{row}}$ has 2^3 elements.) Since $X^u|v\rangle = |u+v\rangle$ for all $u, v \in \mathbb{F}_2^7$, it is clear that $|0\rangle_L$ and $|1\rangle_L$ are fixed by the X-stabiliser subgroup. We leave it as an extended exercise using Lemma 3.2 to show that $|0\rangle_L$ and $|1\rangle_L$ are also fixed by the Z-stabiliser group and so $|0\rangle_L, |1\rangle_L \in \mathcal{C}$. With a bit more work, this approach shows that $\mathcal{C}$ is exactly the 2-dimensional subspace of $\mathcal{H}^{\otimes 7}$ spanned by the logical codewords $|0\rangle_L$ and $|1\rangle_L$. Alternatively this follows from the general theory of CSS codes[52] noting that $\langle P \rangle_{\text{row}}^{\perp} = \langle P \rangle_{\text{row}} \oplus \langle 1111111 \rangle$ and so $\langle P \rangle_{\text{row}}^{\perp} / \langle P \rangle_{\text{row}}$ consists of the two cosets $\langle P \rangle_{\text{row}}$ and $1111111 + \langle P \rangle_{\text{row}}$. Thus $\mathcal{C}$ uses 7 physical qubits to encode 1 logical qubit.

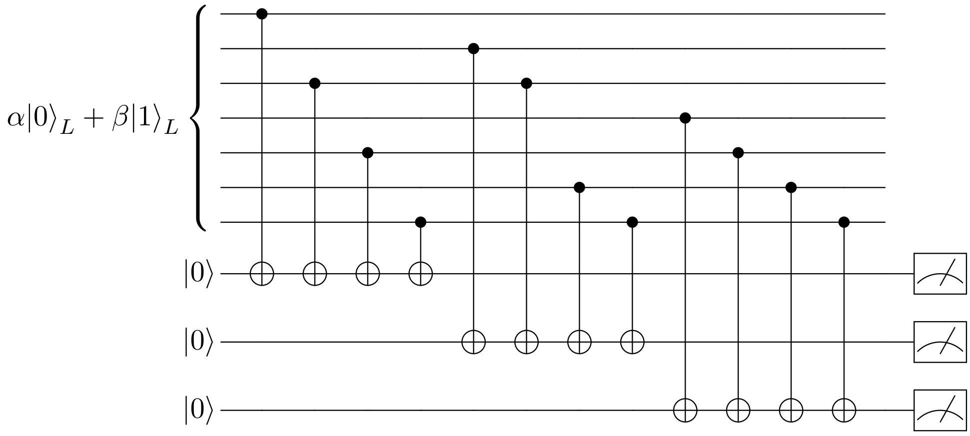
Syndrome extraction. The circuit below measures the X-stabiliser for each row of P as in Lemma 4.6



Dualizing this circuit (so going in the opposite direction to the passage from the toy code to the dual toy code) we get a circuit as in §4.3, still using only

[52]**Reference:** see [9, §10.4.2] or, for a mathematician friendly introduction to CSS codes and stabiliser codes going into much more detail than these notes, [10, Ch. 7].

CNOT gates, that measures the Z-stabilisers.



Exercise 4.9. Suppose that the results of X-stabiliser measurement are $(1,0,1)$ and the results of Z-stabiliser measurement are $(0,1,0)$. Assuming that at most one X-error and at most one Z-error have occurred, what correction would you impose on the data state?[53]

It is a routine generalization from this exercise to see that $\mathcal{C}$ is 1-error correcting. It is therefore a $[[7,1,3]]$-quantum code. In fact, writing P_i for a Pauli operator on qubit i, where P is either X or Z, there is a direct sum $\mathcal{D} = \mathcal{C} \oplus X_1\mathcal{C} \oplus \cdots \oplus X_7\mathcal{C}$ and then, by dimension counting using that $\dim \mathcal{H}^{\otimes 7} = 2^7$ while $\dim \mathcal{D} = 8 \times 2 = 16 = 2^4$, we have $\mathcal{H}^{\otimes 7} = \mathcal{D} \oplus Z_1\mathcal{D} \oplus \cdots \oplus Z_7\mathcal{D}$: the reason from quantum error correction that the subspaces form a direct sum is because they have different syndromes. More mathematically, it is because they are distinct joint eigenspaces for the X- and Z-stabiliser subgroups. This is the quantum analogue of the classical fact that the Hamming $[7,4,3]$-code is perfect, that is, the Hamming balls of radius 1 about codewords partition $\mathbb{F}_2^7$.

Exercise 4.10. Suppose that the data state is error free, but a Z-fault occurs on the first ancilla qubit after the first two CNOT gates. What are the X-stabiliser and Z-stabiliser measurements (supposing we measure the X-stabilisers first)? What is the result of error correction? Conclude that in this case 'the cure was worse than the disease'. [54]

$$\begin{pmatrix} \mathbf{1} & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & \mathbf{1} & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 \end{pmatrix}$$

Making $|0\rangle_L$. Recall from §2 that a CNOT gate is a device for creating entanglement: for instance this was seen in Exercise 2.1. The highlighted pivot columns in the Steane code P-matrix shows that qubit 1 should be

[53]**Solution:** since $(1,0,1)$ and $(0,1,0)$ are columns 5 and 2 of P respectively, and X-stabilisers give syndrome information about Z-errors (and *vice-versa*), the correction is X_2Z_5.

[54]**Solution**: by the copy rules in §2.2 the Z-fault copies up to a Z-error $Z^{0000101} = I \otimes I \otimes I \otimes I \otimes Z \otimes I \otimes Z$ on the data. This would have been detected by the X-stabiliser measurements, except that they have already been performed. Thus, since the data state began error-free, all stabiliser measurements are 0 and no correction is imposed. But a single Z-fault in the process became a weight 2-error. Such 'explosive' faults mean that the naive version of Shor-style error correction in this section is impractical. There are

entangled with qubits $3, 5, 7$; qubit 2 should be entangled with qubits $3, 6, 7$ and qubit 4 should be entangled with qubits $5, 6, 7$. This should motivate the CNOT circuit in Figure 4 that prepares $|0\rangle_L$ in the Steane code.

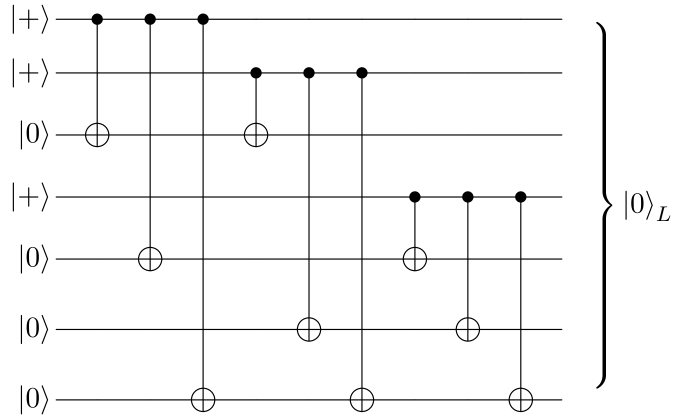


FIGURE 4. Preparation circuit for zero logical $|0\rangle_L$ in the Steane code.

The calculation below shows the effect of each group of three CNOT gates on a Z-basis input state:

$$\begin{aligned} &|b_1\rangle\,|b_2\rangle\,|0\rangle\,|b_4\rangle\,|0\rangle\,|0\rangle\,|0\rangle \\ &\qquad\mapsto |b_1\rangle\,|b_2\rangle\,|b_1\rangle\,|b_4\rangle\,|b_1\rangle\,|0\rangle\,|b_1\rangle \\ &\qquad\mapsto |b_1\rangle\,|b_2\rangle\,|b_1+b_2\rangle\,|b_4\rangle\,|b_1\rangle\,|b_2\rangle\,|b_1+b_2\rangle \\ &\qquad\mapsto |b_1\rangle\,|b_2\rangle\,|b_1+b_2\rangle\,|b_4\rangle\,|b_1+b_4\rangle\,|b_2+b_4\rangle\,|b_1+b_2+b_4\rangle\,. \end{aligned}$$

The result now follows by linearity (as in Exercise 2.1, which is the analogous result for the smaller P-matrix $(1\,1)$), using that the input state is

$$|+\rangle\,|+\rangle\,|0\rangle\,|+\rangle\,|0\rangle\,|0\rangle\,|0\rangle = \tfrac{1}{2^{3/2}} \sum_{b_1,b_2,b_4\in\{0,1\}} |b_1\rangle\,|b_2\rangle\,|0\rangle\,|b_4\rangle\,|0\rangle\,|0\rangle\,|0\rangle\,,$$

and that, since columns 1, 2 and 4 are pivot columns, a general element in $\langle P\rangle_{\mathrm{row}}$ is $(b_1, b_2, b_1+b_2, b_4, b_1+b_4, b_2+b_4, b_1+b_2+b_4)$.

Exercise 4.11. Use the fault pushing rules as in Exercise 2.5 to give an alternative proof that the output of the circuit has X-stabiliser group given by the row span of P and so is $|0\rangle_L$. [*Hint:* you are encouraged to use the shortcut that the output of any CNOT network is a CSS state, of the form $2^{-\dim M/2}\sum_{v\in M}|v\rangle$ for some matrix M.][55]

---

ways around the problem, at the cost of using more complicated ancillae, but they are beyond the scope of these notes. See for instance Exercise 10.73 in [9].

[55]**Solution:** X-faults on the qubits initialized $|+\rangle$ copy to the rows of the P-matrix; thus the X-stabiliser group of the input, namely $\langle X_1, X_2, X_4\rangle$ is conjugated to $\langle X^u : u \in \langle P\rangle_{\mathrm{row}}\rangle$, which by the hint implies that the output state is $|0\rangle_L$.

Exercise 4.12. Show that transverse X, i.e. $X_1X_2X_3X_4X_5X_6X_7 = X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X$ is the X-logical operation for the Steane code that swaps $|0\rangle_L$ and $|1\rangle_L$, and hence find a circuit preparing $|1\rangle_L$. Hence, or otherwise, find a circuit preparing a general $\alpha|0\rangle + \beta|1\rangle$. [*Hint:* conjugate transverse X back through the circuit.][56]

One motivation for making $|0\rangle_L$ is that this is the ancilla state for Steane style error correction of Z-errors. For more on this see [12].

4.7. **Justifying the stochastic X- and Z-error model.** We finish with an example justifying our implicit assumption that quantum errors appear as Pauli operators on one or more qubits.

Example 4.13. The data state in the Steane code was

$$|-\rangle_L = \tfrac{1}{\sqrt{2}}\big(|0\rangle_L - |1\rangle_L\big)$$

until a rogue environmental electron got entangled with it, forming the new state on 8 qubits

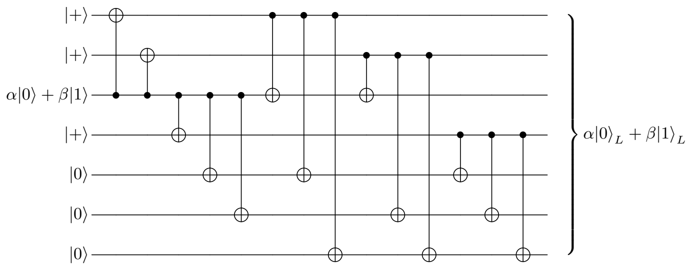
$$|\phi\rangle = \tfrac{4}{5}\,|0\rangle_{\mathrm{env}}\,|-\rangle_L + \tfrac{3}{5}X_2\,|1\rangle_{\mathrm{env}}\,|-\rangle_L\,.$$

Here we use the notation just introduced, that X_2 is a Pauli X on the second qubit. Measuring the first Z-stabiliser $Z_1Z_3Z_5Z_7$, corresponding to the first row 1010101 of P, leaves $|\phi\rangle$ unchanged. But since $Z_2Z_3Z_6Z_7$, corresponding to the second row 0110011 of P, anticommute with X_2, the state in the first

[56]**Solution:** by definition

$$|1\rangle_L = \sum_{v\in\langle P\rangle_{\mathrm{row}}} |\overline{v}\rangle = \sum_{v\in\langle P\rangle_{\mathrm{row}}} |v + 1111111\rangle = X\otimes\cdots\otimes X \sum_{v\in\langle P\rangle_{\mathrm{row}}} |v\rangle = X\otimes\cdots\otimes X\,|0\rangle_L\,.$$

Therefore applying a final transverse X-operation, i.e. X gates on all 7 qubits, to the preparation circuit for $|0\rangle_L$ makes $|1\rangle_L$. Conjugating this back through the circuit by the copy rules in §2.2 gives $X_1X_2X_3X_4X_5X_6 = X\otimes X\otimes X\otimes X\otimes X\otimes X\otimes I$. It follows that the image of $|+\rangle\,|+\rangle\,(\alpha|0\rangle + \beta\,|1\rangle)\,|+\rangle\,|0\rangle\,|0\rangle\,|0\rangle$ under the composition of $\mathrm{CNOT}_{31}\,\mathrm{CNOT}_{32}\ldots\mathrm{CNOT}_{36}$ followed by the preparation circuit making $|0\rangle_L$ is $\alpha|0\rangle_L + \beta|1\rangle_L$, as shown in the diagram below.



See [4, §4.2] for generalizations of this. Another important way to encode uses an auxiliary qubit in state $\alpha|0\rangle + \beta|1\rangle$; a transverse CNOT with this qubit as the control with target $|0\rangle_L$ gives the state $\alpha|0\rangle\,|0\rangle_L + \beta|1\rangle\,|1\rangle_L$; now apply a Hadamard gate to the top qubit to get

$$\alpha|+\rangle\,|0\rangle_L + \beta|-\rangle\,|1\rangle_L = \tfrac{1}{\sqrt{2}}\,|0\rangle\,\big(\alpha\,|0\rangle_L + \beta\,|1\rangle_L\big) + \tfrac{1}{\sqrt{2}}\,|1\rangle\,\big(\alpha\,|0\rangle_L - \beta\,|1\rangle_L\big).$$

Thus measuring the top qubit in the Z-basis gives the required state if the measurement result is 0. If the measurement result is 1 then transverse Z must be applied.

syndrome extraction circuit above *just before measurement* is

$$\tfrac{4}{5}\,|0\rangle_{\text{env}}\,|-\rangle_L\,|0\rangle + \tfrac{3}{5}X_2\,|1\rangle_{\text{env}}\,|-\rangle_L\,|1\rangle\,.$$

By Definition 4.1, measuring the ancilla qubit gives output state $|0\rangle_{\text{env}}\,|-\rangle_L$ with probability $\frac{16}{25}$ (result is 0) and output state $|1\rangle_{\text{env}}\,X_2\,|-\rangle_L$ with probability $\frac{9}{25}$ (result is 1). Note that the environment state is no longer entangled with the data state, and that after the final Z-stabiliser $Z_4Z_5Z_6Z_7$, corresponding to the third row 0001111 of P, is measured, we, or rather the quantum computer, now know what X-correction to impose on the data state.

More generally, one can write an arbitrary quantum error as a linear combination of the Pauli matrices and use a generalization of this example to show that the process of stabiliser measurement (or equivalently, syndrome extraction) forces the error to decohere into a specific combination of Pauli operators. Thus it is *not* a law of nature that quantum errors manifest as X- and Z-faults on the data: rather this is an emergent property of our decoding logic.[57] It is a notable feature of the example above that the entanglement needed only one extra qubit, and its measurement is something that happens deep inside our quantum computer, showing that the theory that any collapse of the wave function requires a conscious observer is misconceived. A quantum computer with functioning error correction will be the strongest test to date that the view of quantum theory, informally presented in these notes, with its strange mixture of unitary evolution punctuated by projections collapsing the quantum state onto an eigenbasis of a Hermitian operator, is an accurate model for how the universe works.[58]

Acknowledgements. I thank Michael D., Alastair Kay, and Tony Skyner for helpful comments on an earlier version of these notes.

References

[1] Scott Aaronson, *Quantum computing since Democritus*, Cambridge University Press, Cambridge, 2013.

[2] Bob Coecke, *Kindergarten quantum mechanics*, arXiv:510032, October 2005, 18 pages.

[3] Artur Ekert, Timothy Hosgood, Alastair Kay, Chiara Macchiavello, *Introduction to Quantum Information Science*, version of July 2025, `https://qubit.guide/index`.

[4] Daniel Gottesman, *Stabiliser codes and quantum error correction*, arXiv:quant-ph/9705052, May 1997.

[5] Brian C. Hall, *Quantum theory for mathematics*, Graduate Texts in Mathematics 267, Springer, 2013.

[6] Tim Maudlin, *Philosophy of physics: Quantum theory*, Princeton University Press, Princeton, 2019.

[57] **In practice:** everyone seems to pretend that nature is sufficiently obliging so as to create errors in the mathematically convenient fashion, and thanks in part to the principle of deferred measurement, we get away with this.

[58] **Reference:** it could be that quantum theory is merely a remarkably accurate model or — and I think this is the mathematically appealing alternative — that quantum states really are the basic 'ontic' elements of reality. See [6] for discussion of this question.

[7] N. David Mermin, *What's wrong with these elements of reality*, Physics Today **43** (1990) 9–11.

[8] N. David Mermin, *Quantum computer science*, Cambridge University Press, Cambridge, 2007.

[9] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[10] John Preskill, *Notes for Physics 219/Computer Science 219*, available from `https://www.preskill.caltech.edu/ph229/`, regularly updated.

[11] Terry Rudolph, *Q is for Quantum*, 2017, all three parts available from `https://www.qisforquantum.org`.

[12] A. M. Steane, *Active stabilization, quantum computation, and quantum state synthesis*, Phys. Rev. Lett. **78** (1997), 2252.

[13] Leonard Susskind and Art Friedman, *Quantum mechanics: The theoretical minimum*, Penguin, April 2015.

[14] John van de Wetering, *ZX-calculus for the working quantum computer scientist*, arXiv:2012.13966, December 2020, 93 pages.