

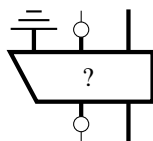
9

Picturing Phases and Complementarity

When spider webs unite, they can tie up a lion.

– *Ethiopian proverb*

In the previous chapter spiders entered the picture. Their initial role seemed essentially just to shuttle classical data around or to provide transit to and from ‘planet quantum’, leaving all of the interesting, fully quantum stuff to happen inside some generic quantum process:



Since we can’t apply any of our funky rules like spider fusion, this ‘black box’ is basically a diagrammatic dead end. This chapter is about ‘opening up’ those boxes. We already half-opened the boxes in Section 8.2.5 when we showed that all linear maps, and hence all quantum maps, consist of spiders and ‘black box’ isometries. We will now finish opening those boxes.

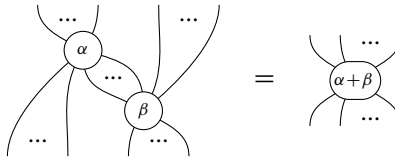
What do we find inside? An arachnophobe’s worst nightmare: more spiders, of course! Unlike here on earth, where the arthropods’ role has been reduced primarily to food or fertiliser, in this book, they become the dominant species and, in fact, the only one!

Indeed, by the end of this chapter, we will be able to build arbitrary maps using just spiders. But before we get there, we need to further diversify the spider population. These (final) additions to the graphical language are motivated by two key notions in quantum theory: *phases* and *complementarity* (a.k.a. mutual unbiasedness).

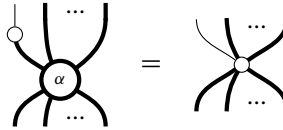
Phases are ‘decorations’ that can be carried by a spider:



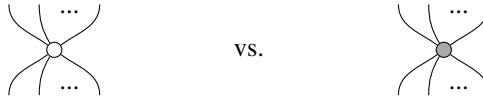
These decorations have two important features. First, when spiders fuse, their decorations combine together:



Second, these decorations are the stuff that doesn't survive the passage from the quantum to the classical realm. Indeed, when a decorated quantum spider makes any attempt to make contact with the classical realm, its decoration vanishes:



As foreshadowed in the previous chapter, we will now also consider spiders of different colours:



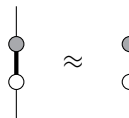
which represent different ONBs. These spiders of different colours no longer fuse, but they still should interact in a simple way. In fact, how they interact is kind of the opposite to fusing. Whereas spiders of the same family like each other, *complementary spiders* do not, and the resulting spider wars will cause some serious loss of limbs:

(9.1)

That is, spiders of the same family fuse together, while, when complementary spiders 'shake legs', those legs fall off (but always in pairs). If we take the essential part of the above equation:

(9.2)

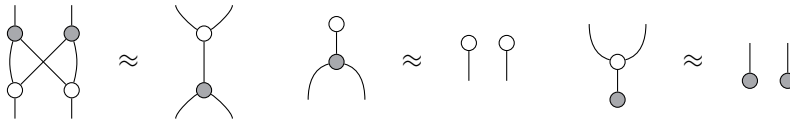
and write it in terms of bastard spiders:



there is a clear operational reading for complementary basis:

(encode in \circ) THEN (measure in \bullet) = (no data transfer)

While complementarity seems to be saying something about what we ‘can’t do’, equation (9.2) proves itself to be quite powerful. In particular, we will sketch out how to exploit complementarity for *quantum cryptography* in Section 9.2.6. Even more useful than equation (9.2) are these equations:



which are satisfied by particularly nice pairs of complementary spiders called *strongly complementary spiders*. While they are only a very recent player in the field of quantum research, these new equations aren’t ad hoc at all and have already been around for quite a while in a variety of disciplines of pure mathematics, where they are the defining equations of a *bialgebra*.

These new equations provide significantly more proving power, so much more in fact that these, along with the (decorated) spider-fusion laws, form the core of a set of equations called the *ZX-calculus*, which are *complete* for proving equations between a large class of quantum maps called **Clifford maps**. The ZX-calculus will become our graphical Swiss Army knife in the following chapters as we study applications in quantum computing, quantum foundations, and theories of (quantum) resources.

9.1 Decorated Spiders

So, let’s start decorating.

9.1.1 Unbiasedness and Phase States

From now on, we will refer to a family of spiders (or equivalently, an ONB via Theorem 8.41) simply by a dot of the appropriate colour, e.g. \circ .

Definition 9.1 A normalised pure state is *unbiased* for \circ if we have:

$$\begin{array}{c} \circ \\ | \\ \triangle \psi \end{array} = \frac{1}{D} \circ \quad (9.3)$$

or equivalently:

$$\begin{array}{c} \circ \\ / \quad \backslash \\ \triangle \psi \quad \triangle \psi \end{array} = \frac{1}{D} \circ \quad (9.4)$$

So what does this mean? In the LHS of (9.3) we see a quantum state $\hat{\psi}$ being measured. In the RHS of (9.3) we see the uniform probability distribution. So, what is required here is that measurement of $\hat{\psi}$ yields a uniform probability distribution over all outcomes, or in

other words: the quantum state $\widehat{\psi}$ has no bias towards any of the measurement outcomes and, hence, is ‘unbiased’.

We can also restate Definition 9.1 in terms of the Born rule:

$$\begin{array}{c} \triangle i \\ \downarrow \\ \widehat{\psi} \end{array} \stackrel{(8.6)}{=} \begin{array}{c} \triangle i \\ \downarrow \\ \circ \\ \downarrow \\ \widehat{\psi} \end{array} \stackrel{(9.3)}{=} \frac{1}{D} \begin{array}{c} \triangle i \\ \downarrow \\ \circ \end{array} = \frac{1}{D}$$

That is, for each outcome the Born rule gives the same probability. The converse also holds.

Exercise 9.2 Show that a normalised pure state is *unbiased* for an ONB-measurement if for all i we have:

$$\begin{array}{c} \triangle i \\ \downarrow \\ \widehat{\psi} \end{array} = \frac{1}{D}$$

Example 9.3 We could ask what the analogue would be in probability theory. There, an ‘unbiased probability distribution’ would be one that has the same probability for each ‘outcome’ i . Of course, there is only one, namely, the uniform probability distribution itself. Hence, the notion of an unbiased probability distribution doesn’t give us anything new.

Evidently, unbiasedness for quantum states does give us something new, otherwise we wouldn’t have defined it. In order to establish that for an ONB-measurement there exist many unbiased states, let’s look at what the matrix form of an unbiased state is. Using the correspondence given in (8.32), the LHS of (9.4) is the Hadamard product of ψ with its conjugate. Hence, written in terms of matrices, equation (9.4) becomes:

$$\begin{pmatrix} \overline{\psi^0} \psi^0 \\ \vdots \\ \overline{\psi^{D-1}} \psi^{D-1} \end{pmatrix} = \begin{pmatrix} \frac{1}{D} \\ \vdots \\ \frac{1}{D} \end{pmatrix}$$

that is, for all i we have:

$$\overline{\psi^i} \psi^i = \frac{1}{D}$$

We saw in Section 6.1.2 that numbers satisfying:

$$\overline{\psi^i} \psi^i = 1$$

can always be written as $e^{i\alpha}$ for some angle $\alpha \in [0, 2\pi)$. Thus there exist complex phases $\alpha_1, \dots, \alpha_D$ such that:

$$\begin{pmatrix} \psi^0 \\ \vdots \\ \psi^{D-1} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{D}} e^{i\alpha_0} \\ \vdots \\ \frac{1}{\sqrt{D}} e^{i\alpha_{D-1}} \end{pmatrix} \quad (9.5)$$

So there are indeed many unbiased quantum states!

and hence the adjoint becomes:



We will see in Section 9.1.4 why we have chosen this notation.

The defining equality (9.6) for phase states now becomes:

(9.9)

or equivalently:

(9.10)

By (9.9), the *phase* data $\tilde{\alpha}$ is totally obliterated as soon as it comes into contact with the classical world via measurement. Thus:

phase := the data destroyed by the quantum-classical passage

While the ONB-states represent purely classical data, phase states represent the opposite notion: they are extremely non-classical, or ‘maximally quantum’. This goes hand in hand with the fact that unbiased states, and hence phase states, have no meaningful classical counterpart (cf. Example 9.3). It should then also come as no surprise that they will play a crucial role in many quantum features that also have no classical counterpart. We’ll elaborate more on this essential non-classicality of phases in the following section.

Before we do so, let’s have a look at where phase states live on the Bloch sphere. In the case where the dimension $D = 2$, a phase state depends only on a single complex phase α . In that case, we have:

(9.11)

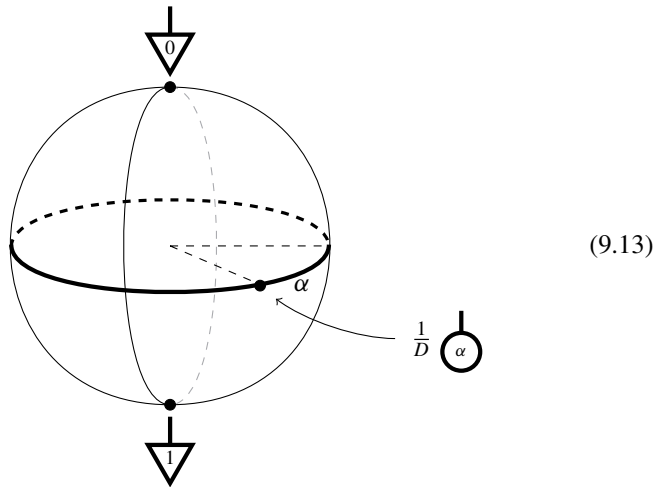
so the form of a phase state simplifies to:

(9.12)

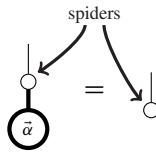
Recall from Section 6.1.2 that any two-dimensional pure state can be written in Bloch sphere coordinates as:

$$\text{double} \left(\cos \frac{\theta}{2} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \end{array} + \sin \frac{\theta}{2} e^{i\alpha} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \end{array} \right)$$

Then, states of the form of (9.12) are precisely those where $\theta = \pi/2$. In other words, they live on the equator of the Bloch sphere:

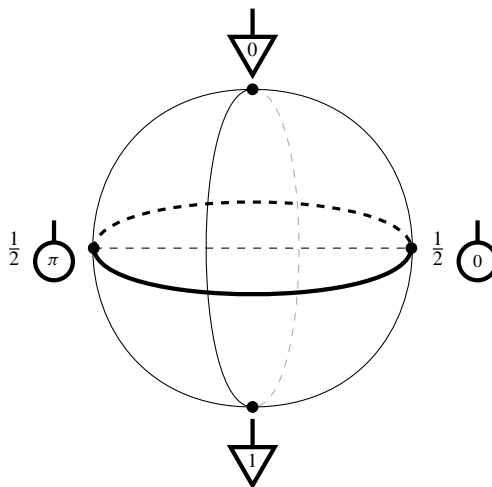


Remark 9.6 In most other texts on quantum theory, phases are introduced in this geometric manner. However, we defined phase states entirely in the language of spiders, without using any other ingredients of **linear maps**:



So they are intrinsic to the diagrammatic language. One consequence of this is that they are also meaningful in many other process theories, as we shall see in Section 11.2.2.

Example 9.7 When comparing the representation of phase states on the Bloch sphere with the picture of Exercise 6.7, we see that the X-basis states are in fact phases for \odot :



$$\begin{array}{c} | \\ \text{0} \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} | \\ \text{0} \end{array} \qquad \begin{array}{c} | \\ \text{1} \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} | \\ \pi \end{array}$$

Exercise* 9.8 The D -dimensional generalisation of this ONB of phases is called the *Fourier basis*:

$$\left\{ \frac{1}{\sqrt{D}} \textcircled{\vec{\kappa}_j} \right\}_i \quad \text{where} \quad \textcircled{\vec{\kappa}_j} := \sum_k e^{\frac{2\pi i}{D}jk} \text{\texttriangleup}^k$$

$$\sum_{k=0}^{D-1} r^k = \frac{r^D - 1}{r - 1}$$

Since phases constitute ‘maximally quantum’ data, we will primarily use them to ‘decorate’ quantum spiders. To decorate a quantum spider, we simply plug in a phase state at one of its legs.

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \bigcirc \\ \diagdown \quad \diagup \\ \dots \end{array} := \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \bigcirc \\ \diagdown \quad \diagup \\ \bigcirc \\ \diagdown \quad \diagup \\ \dots \end{array} \quad (9.14)$$

Proposition 9.10 The transpose of a phase spider is a phase spider with the same phase. In particular, if a phase spider has the same number of inputs as outputs, it is self-transposed.

$$\text{Diagram with a central vertex and four external lines, one of which is a loop labeled } \bar{\alpha} = \text{double} \left(\sum_j e^{i\alpha_j} \text{Diagram with a central vertex and four external lines, one of which is a loop labeled } j \right)$$

and the generalised copy rule (8.38), we obtain the matrix form of a spider:

$$\text{spider}(\alpha) = \text{double} \left(\sum_j e^{i\alpha_j} \begin{array}{c} \downarrow j \\ \dots \\ \downarrow j \\ \uparrow j \\ \dots \\ \uparrow j \end{array} \right)$$

As before, we can remove a global phase and assume $\alpha_0 = 0$. So, in two dimensions, this simplifies to:

$$\text{spider}(\alpha) = \text{double} \left(\begin{array}{c} \downarrow 0 \dots \downarrow 0 \\ \uparrow 0 \dots \uparrow 0 \end{array} + e^{i\alpha} \begin{array}{c} \downarrow 1 \dots \downarrow 1 \\ \uparrow 1 \dots \uparrow 1 \end{array} \right)$$

Whenever a decorated quantum spider attempts to make contact with the classical realm, it loses its decoration.

Theorem 9.11 If any leg of a phase spider is measured, its phase vanishes:

$$\text{spider}(\alpha) \text{ with one leg measured} = \text{spider}(\alpha) \text{ with one leg removed} \quad (9.15)$$

Proof Using bastard spider fusion we have:

$$\text{spider}(\alpha) \text{ with one leg measured} \stackrel{(9.14)}{=} \text{spider}(\alpha) \text{ with one leg removed} = \text{spider}(\alpha) \text{ with one leg removed} \stackrel{(9.9)}{=} \text{spider}(\alpha) \text{ with one leg removed} = \text{spider}(\alpha) \text{ with one leg removed}$$

□

In Section 8.3.2 we showed that decoherence witnesses classicality, in that decoherence-invariant inputs/outputs behave the same as classical inputs/outputs. Hence one would expect decoherence to be pretty destructive as well.

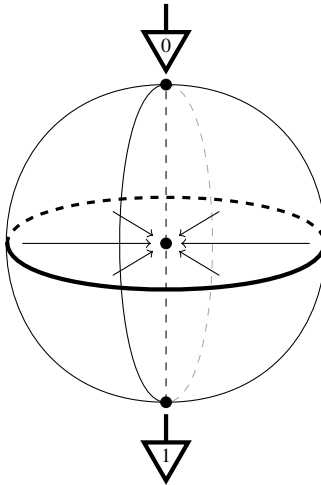
Corollary 9.12 Decoherence erases phases:

$$\text{spider}(\alpha) \text{ with one leg measured} = \text{spider}(\alpha) \text{ with one leg removed} \quad (9.16)$$

A phase state itself is a special case of a phase spider, in which case equation (9.16) specialises to:

$$\text{---} \circ \text{---} \circ \bigcirc_{\bar{\alpha}} = \text{---} \circ = \text{---} \perp$$

In Section 8.3.2, we showed that we can picture decoherence on a two-dimensional system as projecting on to the centre line of the Bloch ball. This gives us a geometric picture of how decoherence destroys phases. The phase states on the equator all get projected to the middle, i.e. the maximally mixed state:



Exercise 9.13 Show that, more generally, whenever a phase spider fuses with any bastard spider, the phase vanishes:

$$\text{---} \circ \bigcirc_{\bar{\alpha}} \text{---} = \text{---} \circ \text{---} \quad (9.17)$$

9.1.3 Phase Spider Fusion

So, we now know what happens when a phase spider fuses with a bastard spider, but what about when two phase spiders fuse together? Using quantum spider fusion we have:

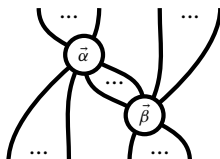
$$\text{---} \circ \bigcirc_{\bar{\alpha}} \text{---} \bigcirc_{\bar{\beta}} \text{---} = \text{---} \circ \bigcirc_{\bar{\alpha}} \text{---} \bigcirc_{\bar{\beta}} \text{---} = \text{---} \circ \bigcirc_{\bar{\alpha}} \bigcirc_{\bar{\beta}} \text{---}$$

The RHS is again a phase spider.

Lemma 9.14 Let $\vec{\alpha}$ and $\vec{\beta}$ be phases. Then:

$$\begin{array}{c} | \\ \circ \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \vec{\alpha} \quad \vec{\beta} \end{array} \quad (9.18)$$

is a phase state, and hence.



is a phase spider.

Proof Using bastard spider fusion we have:

$$\begin{array}{c} | \\ \circ \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \vec{\alpha} \quad \vec{\beta} \end{array} = \begin{array}{c} | \\ \circ \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \vec{\alpha} \quad \vec{\beta} \end{array} \stackrel{(9.9)}{=} \begin{array}{c} | \\ \circ \\ \swarrow \quad \searrow \\ \circ \quad \circ \end{array} = \begin{array}{c} | \\ \circ \end{array}$$

So equation (9.9) is indeed satisfied for the state (9.18). \square

By introducing some new notation for this combined phase, we have the following.

Theorem 9.15 Phase spiders fuse as follows:

$$\begin{array}{c} \dots \quad \dots \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \vec{\alpha} \quad \vec{\beta} \\ \swarrow \quad \searrow \\ \dots \quad \dots \end{array} = \begin{array}{c} \dots \\ \swarrow \quad \searrow \\ \circ \\ \vec{\alpha+\beta} \\ \swarrow \quad \searrow \\ \dots \end{array} \quad (9.19)$$

where we used the shorthand:

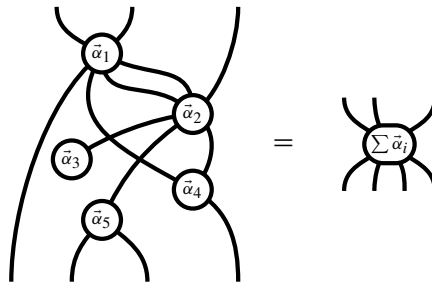
$$\begin{array}{c} | \\ \circ \\ \vec{\alpha+\beta} \end{array} := \begin{array}{c} | \\ \circ \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \vec{\alpha} \quad \vec{\beta} \end{array}$$

Clearly the order of $\vec{\alpha}$ and $\vec{\beta}$ is irrelevant:

$$\begin{array}{c} | \\ \circ \\ \vec{\alpha+\beta} \end{array} = \begin{array}{c} | \\ \circ \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \vec{\alpha} \quad \vec{\beta} \end{array} = \begin{array}{c} | \\ \circ \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \vec{\beta} \quad \vec{\alpha} \end{array} = \begin{array}{c} | \\ \circ \\ \vec{\beta+\alpha} \end{array}$$

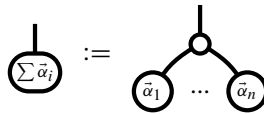
and we can extend this notation straightforwardly to n phases, obtaining a ‘decorated’ version of Corollary 8.35.

Corollary 9.16 Any diagram consisting only of phase spiders and that is moreover connected is itself a phase spider, whose phase is the sum of the phases of each of the component spiders:



$$(9.20)$$

where we used the shorthand:

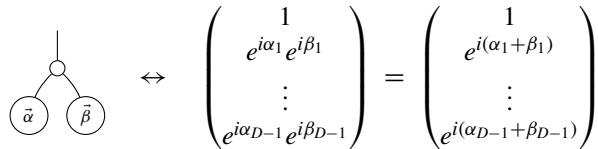


$$\circlearrowleft \sum \vec{\alpha}_i := \circlearrowleft \begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \vec{\alpha}_1 \quad \dots \quad \vec{\alpha}_n \end{array}$$

So why did we choose to write this ‘phase mingling’ as a sum? Let’s have a look at what is happening with the underlying linear maps. First, note that when we multiply two complex phases, the angles add together:

$$e^{i\alpha} e^{i\beta} = e^{i(\alpha+\beta)}$$

Then, by expressing (9.18) as a Hadamard product (8.32), we have:

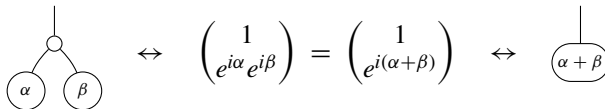


$$\circlearrowleft \begin{array}{c} \vec{\alpha} \quad \vec{\beta} \end{array} \Leftrightarrow \begin{pmatrix} 1 \\ e^{i\alpha_1} e^{i\beta_1} \\ \vdots \\ e^{i\alpha_{D-1}} e^{i\beta_{D-1}} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{i(\alpha_1+\beta_1)} \\ \vdots \\ e^{i(\alpha_{D-1}+\beta_{D-1})} \end{pmatrix}$$

Hence the resulting phase is indeed the pointwise sum of the two phases we started with:

$$\vec{\alpha} + \vec{\beta} := (\alpha_1 + \beta_1, \dots, \alpha_{D-1} + \beta_{D-1})$$

In two dimensions, this simplifies to:



$$\circlearrowleft \begin{array}{c} \alpha \quad \beta \end{array} \Leftrightarrow \begin{pmatrix} 1 \\ e^{i\alpha} e^{i\beta} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{i(\alpha+\beta)} \end{pmatrix} \Leftrightarrow \circlearrowleft \alpha + \beta$$

We conclude this section with an analogue to Corollary 8.35.

Corollary 9.17 When phase spiders are composed, then, if the resulting diagram is connected, it depends only on:

- the number of inputs and outputs and
- the total sum of the phases.

9.1.4 The Phase Group

In the previous section, we saw how spiders can be used to define a ‘sum’ operation for phase states. In this section, we will see that the set of phase states in fact forms a *commutative group*. You may have already encountered groups in algebra, but in case you haven’t, here’s a quick review.

Definition 9.18 A *commutative group* is a set A with:

- a *group-sum* operation that returns $a + b \in A$ given any $a, b \in A$,
- a distinguished element $0 \in A$ called the *unit*, and
- an operation *inverse* that returns $-a \in A$ given any $a \in A$,

which satisfy the following equations, for all $a, b, c \in A$:

$$a + (b + c) = (a + b) + c \quad a + b = b + a \quad a + 0 = a \quad -a + a = 0$$

These equations are typically referred to as *associativity*, *commutativity*, *unitality*, and the *inverse law*, respectively.

Taking phase states to be group elements:

$$\begin{array}{c} | \\ \bigcirc \\ \vec{\alpha} \end{array} \leftrightarrow a$$

we have already identified a candidate for the group-sum:

$$\begin{array}{c} | \\ \bigcirc \\ \diagup \quad \diagdown \end{array} \leftrightarrow + \qquad \begin{array}{c} | \\ \bigcirc \\ \diagup \quad \diagdown \\ \bigcirc \quad \bigcirc \\ \vec{\alpha} \quad \vec{\beta} \end{array} \leftrightarrow a + b$$

So it only remains to find the unit and the inverse.

Lemma 9.19 Let $\vec{\alpha}$ be a phase. Then:

$$\begin{array}{c} | \\ \bigcirc \end{array} \qquad \begin{array}{c} | \\ \bigcirc \\ -\vec{\alpha} \end{array}$$

are phase states.

Proof Using spider fusion we have:

$$\begin{array}{c} | \\ \bigcirc \\ | \end{array} = \begin{array}{c} | \\ \bigcirc \\ \diagup \quad \diagdown \\ \bigcirc \quad \bigcirc \end{array} = \begin{array}{c} | \\ \bigcirc \end{array}$$

So equation (9.9) is satisfied. We can show that the conjugate of a phase state is again a phase state by conjugating both sides of (9.9):

$$\begin{array}{c} | \\ \bigcirc \\ \bigcirc \\ -\vec{\alpha} \end{array} = \begin{array}{c} | \\ \bigcirc \end{array}$$

□

Theorem 9.20 For any family of spiders \bigcirc , the set of phase states:

$$\left\{ \bigcirc_{\vec{\alpha}} \right\}_{\vec{\alpha}}$$

form a commutative group where:

- the group-sum is:

$$\bigcirc_{\vec{\alpha} + \vec{\beta}} := \bigcirc_{\vec{\alpha}} \bigcirc_{\vec{\beta}}$$

- the unit is:

$$\bigcirc_{\vec{0}} := \bigcirc$$

- the inverse is:

$$\bigcirc_{-\vec{\alpha}}$$

Proof In Lemmas 9.14 and 9.19 we already established the candidate group-sum, unit, and inverse. So it only remains to verify the group equations. Associativity, commutativity, and unit laws follow from spider fusion:

$$\begin{array}{c} \text{Spider fusion diagrams showing associativity, commutativity, and unit laws.} \end{array}$$

For example, in the case of associativity we have:

$$\begin{array}{c} \text{Associativity diagram: } \bigcirc_{\vec{\alpha}} (\bigcirc_{\vec{\beta}} \bigcirc_{\vec{\gamma}}) = (\bigcirc_{\vec{\alpha}} \bigcirc_{\vec{\beta}}) \bigcirc_{\vec{\gamma}} \end{array}$$

Then, the inverse law arises by doubling (9.10):

$$\begin{array}{c} \text{Inverse law diagram: } \bigcirc_{-\vec{\alpha}} \bigcirc_{\vec{\alpha}} = \bigcirc_{\vec{0}} \end{array} \quad (9.21)$$

which completes the proof. \square

So, using just spider rules and the definition of unbiasedness we showed that the phase states always form a group. In particular, we never made any reference to the explicit form of phases:

$$\textcircled{\vec{\alpha}} := \text{double} \left(\sum_j e^{i\alpha_j} \text{---} \nabla_j \right)$$

Exercise 9.21 Show using the following properties of complex numbers:

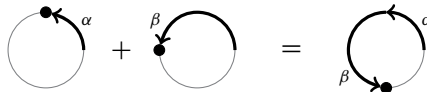
$$e^{i0} = 1 \qquad \overline{e^{i\alpha}} = e^{-i\alpha}$$

that $\vec{0}$ and $-\vec{\alpha}$ can be given explicitly as:

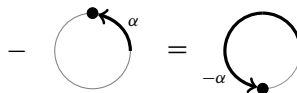
$$\vec{0} := (0, \dots, 0) \qquad \text{and} \qquad -\vec{\alpha} := (-\alpha_1, \dots, -\alpha_{D-1})$$

respectively.

In the case of $D = 2$, we can represent a phase by just a single angle. In that case, the phase group has elements represented by angles $\alpha \in [0, 2\pi)$, and the group-sum is addition of angles, i.e. addition modulo 2π :



The inverse is just sending an angle to its opposite angle:



For obvious reasons, this is sometimes called the *circle group*. In slightly more sophisticated language, this group is also called $U(1)$, owing to the fact that phases are the same thing as 1×1 unitary matrices:

$$e^{i\alpha} \quad \leftrightarrow \quad (e^{i\alpha})$$

In higher dimensions, we just get more copies of $U(1)$. That is, the phase group is always of the form:

$$\underbrace{U(1) \times \dots \times U(1)}_{D-1}$$

9.1.5 Phase Gates

We already encountered phase states as one particularly important example of phase spiders. We will now study another one that plays a central role in the remainder of this book.

Definition 9.22 A *phase gate* is a quantum process of the form:

$$\text{Phase gate } \vec{\alpha} := \text{Cup with } \vec{\alpha} \text{ on the right} \quad (9.22)$$

As with all phase spiders, taking the adjoint (or equivalently the conjugate) of a phase gate introduces a minus sign to its phase:

$$\text{Cup with } -\vec{\alpha} = \text{Cap with } \vec{\alpha} = \text{Cup with } \vec{\alpha} = \text{Cap with } -\vec{\alpha}$$

As a consequence, we have the following proposition.

Proposition 9.23 Phase gates are unitary.

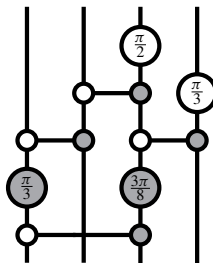
Proof Using spider fusion we have:

$$\text{Cap with } \vec{\alpha} \text{ followed by Cup with } \vec{\alpha} = \text{Cap with } \vec{0} = \text{Cup with } \vec{0} = \text{Identity line}$$

Composing in the other order similarly yields the identity. \square

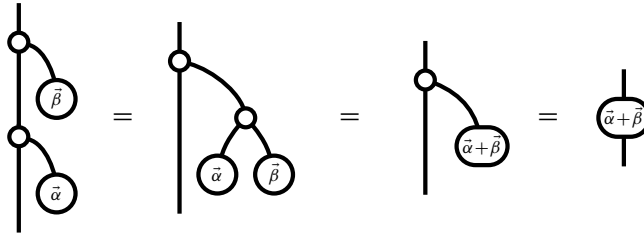
Hence, phase gates are prime examples of *quantum gates* (cf. Section 5.3.4 and Example 6.13).

Example 9.24 Picking up where we left off in Example 6.13, phase gates allow us to write quantum circuits that have no classical counterpart:



A set of quantum gates is *universal* when arbitrary unitaries can be obtained as a quantum circuit including only gates of that set, and we shall show in Section 12.1.3 that a set consisting of the quantum CNOT-gate and phase gates is universal. Consequently, phase gates play a central role in quantum computing.

Since phase gates are examples of phase spiders, the group structure from the previous sections carries immediately over into phase gates, e.g.:



Corollary 9.25 For any family of spiders \bigcirc , the set of phase gates:

$$\left\{ \begin{array}{c} \bigcirc \\ \vec{\alpha} \end{array} \right\}$$

forms a commutative group where:

- the group-sum is:



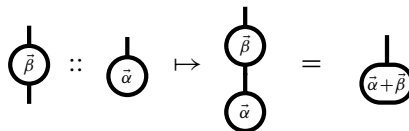
- the unit is:



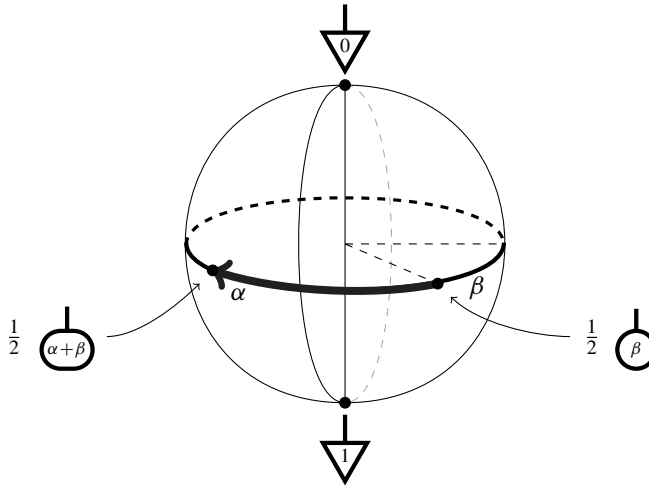
- the inverse is:



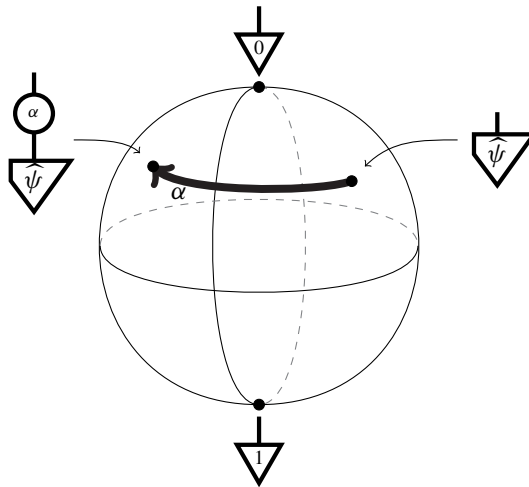
So what do these phase gates actually do? We can figure this out by looking at how they act on phase states:



So a phase gate with phase $\vec{\beta}$ sends a phase state with phase $\vec{\alpha}$ to another phase state with phase $\vec{\alpha} + \vec{\beta}$. In two dimensions, this corresponds to a Bloch sphere rotation about the axis fixed by the two basis states:



Since phase gates are unitary, and unitaries correspond to rotations on the Bloch sphere (cf. Proposition 7.2), it immediately follows that phase gates rotate all states around the Z-axis:



Unsurprisingly, the matrices of phase gates are closely related to the matrices of their associated phase states. For:

$$\begin{array}{c} | \\ \textcircled{\vec{\alpha}} \end{array} := \sum_j e^{i\alpha_j} \begin{array}{c} | \\ \nabla_j \end{array}$$

(where we take $\alpha_0 := 0$) we obtain:

$$\begin{array}{c} | \\ \textcircled{\vec{\alpha}} \end{array} = \begin{array}{c} | \\ \textcircled{} \end{array} \begin{array}{c} \searrow \\ \sum_j e^{i\alpha_j} \nabla_j \end{array} = \sum_j e^{i\alpha_j} \begin{array}{c} | \\ \nabla_j \end{array} \begin{array}{c} | \\ \nabla_j \end{array}$$

Hence, for a phase state:

$$\text{---} \bigcirc \bar{\alpha} \leftrightarrow \begin{pmatrix} 1 \\ e^{i\alpha_1} \\ \vdots \\ e^{i\alpha_{D-1}} \end{pmatrix}$$

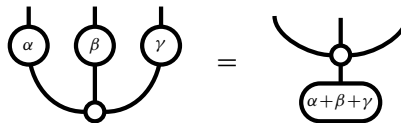
the matrix of the associated phase gate is:

$$\text{---} \bigcirc \bar{\alpha} \leftrightarrow \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & e^{i\alpha_1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e^{i\alpha_{D-1}} \end{pmatrix}$$

For $D = 2$, the matrix of a phase map is of this form:

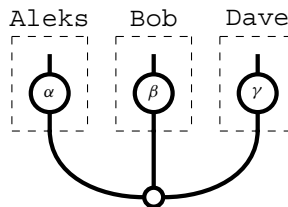
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

Example 9.26 In Example 8.70 we already encountered the three-system GHZ state. When we apply a phase gate to each of the systems we obtain:



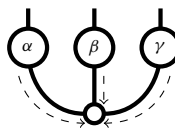
While this is a seemingly innocent application of phase spider fusion, when we interpret this equation physically the implications are somewhat shocking!

Assume that the three parties that perform the three phase gates:

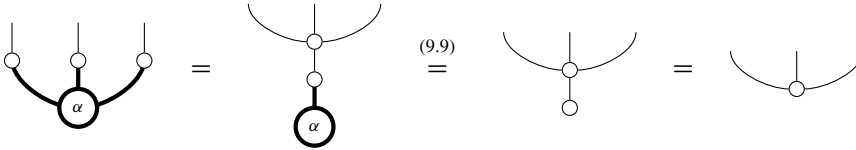


are so far apart that light does not have the time to travel between them.

While the choices of the angles α , β , and γ are made independently, at very distant locations, the resulting state depends only on the group-sum of the three phases. So if, for instance, these phases would have been permuted, the resulting state would be the same. This hints at the fact that these processes are interacting instantaneously over a long distance. The diagram literally shows that it is as if the three phases are travelling backwards in time to meet up with each other:



and in contrast to our discussion in Section 4.4.3, which involved (non-causal) caps, all the processes involved here are perfectly causal. Of course, all of this happens at the level of a quantum state, and naïve measurement kills the phases, and hence all the magic:

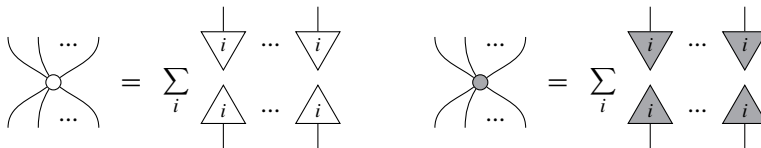


Below in Section 9.3.3 we will pick up this story again and show that an alternative choice of measurements won't kill the magic.

9.2 Multicoloured Spiders

Spiders of the same species happily mate and mingle their phases. However, it is not all love and peace in spider land. Now we introduce spiders of distinct species, and expose the carnage that happens when these species clash.

As we did in Section 5.3.5 we will represent two distinct ONBs, and now their associated spiders, using different colours:



This will enable us to consider measurement and encoding operations in two different bases and, in particular, to study how these operations interact.

9.2.1 Complementary Spiders

The concept of a phase state (a.k.a unbiasedness) has a very clear interpretation as proper quantumness and gives rise to diagrammatic creatures called phase spiders. A simple diagrammatic rule that concerns how spiders of different colours interact yields a related and perhaps even more important concept.

Definition 9.27 Spiders \circ and \bullet are *complementary* if:

$$\text{Black spider with 1 input, 1 output} \circ \text{White spider with 1 input, 1 output} = \frac{1}{D} \text{Black spider with 1 input, 1 output} \circ \text{White spider with 1 input, 1 output} \quad (9.23)$$

or equivalently:

$$\begin{array}{c} \bullet \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ \circ \end{array} \quad (9.24)$$

So what does this mean? In the LHS of (9.23) we are encoding classical data in the white basis then measuring in the grey one. Then, (9.23) says this is equivalent to just deleting the classical input:



and outputting a uniform probability distribution:



Thus the classical data at the input vanishes and is replaced by randomness. In summary:

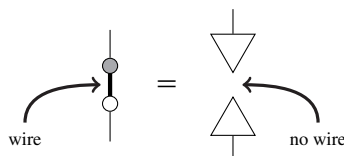
$$\boxed{(\text{encode in } \circ) \text{ THEN } (\text{measure in } \bullet) = (\text{no data flow})} \quad (9.25)$$

Remark 9.28 Note that the uniform probability distribution arising from a \bullet -measurement is given as a \bullet -spider. We'll say more about this in Section 9.2.4.

Condition (9.25) says that the white basis is a very poor way of encoding classical data with respect to the grey measurement. For example, if we encode a classical value i as the i -th white ONB state of a quantum system and we measure it with the white measurement, we will get outcome i with certainty. On the other hand, if we measure it with the grey measurement, we are equally likely to obtain any outcome, so this gives us no information whatsoever about the encoded value. Another way of saying this is that if we have maximal information about a system with respect to one basis (i.e. it is in a pure ONB state), we have no information with respect to the other basis.

Example* 9.29 A well-known instance of this phenomenon in quantum mechanics is that if one perfectly knows the position of a quantum system, then one cannot know anything about its momentum. One usually treats position as a continuous variable, which necessitates moving to infinite-dimensional systems. However, the fundamental principle is the same as the discrete version of complementarity we present here.

While equation (9.23) required a separation into a particular state and effect, namely (white) deleting followed by the (grey) uniform probability distribution, it actually suffices to say that the LHS above simply separates:



Thus, (9.25) can be taken as a literal statement of complementarity. More precisely, we can give several variations on this theme.

Proposition 9.30 The following are equivalent for \circ and \bullet :

(i) complementarity:

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

(ii) complementary measurements on a Bell state give a uniform probability distribution for two classical systems:

$$\frac{1}{D} \begin{array}{c} \circ \\ | \\ \bullet \\ | \\ \bullet \end{array} = \frac{1}{D} \begin{array}{c} \circ \end{array} \frac{1}{D} \begin{array}{c} \bullet \end{array}$$

(iii) the existence of an effect p and a state q such that:

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \begin{array}{c} \triangle q \\ | \\ \triangle p \\ | \end{array}$$

(iv) there exist states p and q such that:

$$\frac{1}{D} \begin{array}{c} \circ \\ | \\ \bullet \\ | \\ \bullet \end{array} = \begin{array}{c} \triangle p \\ | \end{array} \begin{array}{c} \triangle q \\ | \end{array}$$

Proof Equivalence of (i) and (ii) is trivial, and so is equivalence of (iii) and (iv), and since (i) implies (iii), it only remains to be shown that (iii) implies (i). First, we can show that q is \bullet , up to some number λ :

$$\begin{array}{c} \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \stackrel{(8.70)}{=} \begin{array}{c} \bullet \\ | \\ \equiv \end{array} \stackrel{(8.70)}{=} \begin{array}{c} \bullet \\ | \\ \circ \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \begin{array}{c} \triangle q \\ | \\ \triangle p \\ | \\ \circ \end{array} = \lambda \begin{array}{c} \triangle q \\ | \end{array}$$

Then, by a similar argument:

$$\begin{array}{c} \circ \end{array} = \lambda' \begin{array}{c} \triangle p \\ | \end{array}$$

Note that λ and λ' must both be non-zero, so we can deduce that:

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \frac{1}{\lambda\lambda'} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \quad (9.26)$$

We can figure out what this number is by means of the recipe outlined at the end of Section 3.4.3. Pre- and post-composing with dots yields:

$$D = \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \stackrel{(8.60)}{=} \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \frac{1}{\lambda\lambda'} \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \frac{D^2}{\lambda\lambda'}$$

so $\lambda\lambda' = D$. Plugging this into (9.26) yields (i). \square

We will now contrast the behaviour of complementary spiders with the usual spider-fusion rules. Rather than fusing, complementary spiders do the opposite: they break apart. We will see the complementarity equation taking on several guises in the next few chapters. The first is for bastard spiders.

Proposition 9.31 For complementary \circ and \bullet we have:

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} = \frac{1}{D} \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} \quad (9.27)$$

Proof A bit of spider fusion:

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} = \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ | \\ \bullet \\ | \\ \bullet \\ \diagdown \quad \diagup \\ \dots \end{array}$$

and a bit of complementarity:

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ | \\ \bullet \\ | \\ \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} \stackrel{(9.23)}{=} \frac{1}{D} \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ \diagdown \quad \diagup \\ \dots \end{array}$$

and another bit of spider fusion:

$$\frac{1}{D} \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ | \\ \bullet \\ | \\ \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} = \frac{1}{D} \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ \diagdown \quad \diagup \\ \dots \end{array}$$

\square

The second guise of complementarity is for classical spiders. Here we think of \bullet as classical maps for \circ , or vice versa (see Section 9.3.5 below).

Proposition 9.32 For complementary \circ and \bullet we have:

$$\text{Diagram} = \frac{1}{D} \text{Diagram} \quad (9.28)$$

The proof is nearly identical; just replace (9.23) with (9.24). The third guise of complementarity doesn't have any direct connection to measurements or classical data at all. Nonetheless, it will be remarkably useful for quantum protocols and algorithms. It is just the doubled form of (9.28).

Proposition 9.33 For complementary \circ and \bullet we have:

$$\text{Diagram} = \frac{1}{D^2} \text{Diagram} \quad (9.29)$$

One thing you might have noticed from this section is we are starting to get a lot of D s popping up all over the place. Well, we have some bad news and some good news. The bad news is, this is basically unavoidable. If we renormalise spiders to get rid of these numbers, the spider-fusion rule becomes really horrible.

Exercise* 9.34 How would the spider-fusion rule look when we renormalise spiders such that we have the following?

$$\text{Diagram} = \text{Diagram}$$

However, the good news is that (as explained in Section 3.4.3) we can pretty much always ignore these numbers. So we can rewrite complementarity as:

$$\text{Diagram} \approx \text{Diagram} \quad (9.30)$$

and the derived 'spider detachment' rules become:

$$\text{Diagram} \approx \text{Diagram} \quad (9.31)$$

$$\text{Diagram} \approx \text{Diagram} \quad (9.32)$$

$$(9.33)$$

Isn't that nicer? And we can recover the ignored numbers too.

Proposition 9.35 For spiders \circ and \bullet :

$$\bullet \circ \approx \bullet \Rightarrow \bullet \circ = \frac{1}{D} \bullet$$

Proof Assuming:

$$\bullet \circ = \lambda \bullet$$

and pre- and post-composing with dots just as we did in the proof of Proposition 9.30, we obtain:

$$D = \text{double line with } \bullet = \lambda \text{ double line} = \lambda D^2$$

so $\lambda = \frac{1}{D}$. □

Remark 9.36 The spiders we use in this chapter will continuously hop between being **linear maps** and **quantum maps/cq-maps**. This means there could be some ambiguity whether \approx means 'up to a complex number' (i.e. the numbers in **linear maps**) or 'up to a positive number' (i.e. the numbers in **cq-maps**). We will always specify this explicitly when there could be some confusion.

Exercise 9.37 Show that equations (9.32) and (9.33) extend to phase spiders; that is, prove:

$$(9.34)$$

$$(9.35)$$

9.2.2 Complementarity and Unbiasedness

Both unbiasedness and complementarity have something to do with an obstruction of information flow across measurements, so it shouldn't come as a surprise that they are closely connected. In fact, complementarity can be formulated entirely in terms of unbiasedness. First, note that, for complementary \circ and \bullet , we have the following:

$$\begin{array}{c} \triangleup_j \\ \downarrow \\ \triangleleft_i \end{array} \stackrel{(8.6)}{=} \begin{array}{c} \triangleup_j \\ \downarrow \bullet \\ \circ \\ \downarrow \\ \triangleleft_i \end{array} \stackrel{(9.23)}{=} \frac{1}{D} \begin{array}{c} \triangleup_j \\ \downarrow \bullet \\ \circ \\ \downarrow \\ \triangleleft_i \end{array} \stackrel{(8.13)}{=} \frac{1}{D} \quad (9.36)$$

Hence, in the light of Exercise 9.2, the basis state:

$$\begin{array}{c} \downarrow \\ \triangleleft_i \end{array} \quad \text{is unbiased for} \quad \begin{array}{c} \bullet \\ | \end{array}$$

and by vertically reflecting, we can also show that:

$$\begin{array}{c} \downarrow \\ \triangleleft_i \end{array} \quad \text{is unbiased for} \quad \begin{array}{c} \circ \\ | \end{array}$$

This particular mutual relationship has a standard name.

Definition 9.38 Two ONBs:

$$\left\{ \begin{array}{c} \downarrow \\ \triangleleft_i \end{array} \right\}_i \quad \text{and} \quad \left\{ \begin{array}{c} \downarrow \\ \triangleleft_j \end{array} \right\}_j$$

are *mutually unbiased* if every state of one ONB is unbiased for the other ONB; that is, if for all i, j we have:

$$\begin{array}{c} \triangleup_j \\ \downarrow \\ \triangleleft_i \end{array} = \frac{1}{D} \quad (9.37)$$

Remark 9.39 The defining equation (9.37) for mutually unbiased ONBs can also be written in undoubled form, which may look more familiar to some:

$$\left| \begin{array}{c} \triangleup_j \\ \downarrow \\ \triangleleft_i \end{array} \right| = \frac{1}{\sqrt{D}}$$

Theorem 9.40 Spiders \circ and \bullet are complementary:

$$\begin{array}{c} \bullet \\ | \\ \circ \\ | \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \\ | \end{array}$$

if and only if their associated ONBs are mutually unbiased:

$$\forall i, j : \begin{array}{c} \triangleup_j \\ \hline \triangleleft_i \end{array} = \frac{1}{D} \quad (9.38)$$

Proof For \circ and \bullet complementary, (9.36) already showed that the associated ONBs are mutually unbiased. Conversely, if the two ONBs are mutually unbiased, then we obtain:

$$\begin{array}{c} \triangleup_j \\ \bullet \\ \circ \\ \triangleleft_i \end{array} \stackrel{(8.6)}{=} \begin{array}{c} \triangleup_j \\ \hline \triangleleft_i \end{array} \stackrel{(9.23)}{=} \frac{1}{D} \stackrel{(8.13)}{=} \frac{1}{D} \begin{array}{c} \triangleup_j \\ \bullet \\ \circ \\ \triangleleft_i \end{array}$$

So the matrix entries of the LHS and RHS of the complementarity equation (9.23) agree for these bases, and hence the equation holds. \square

This relationship with mutual unbiasedness gives us another bunch of alternative characterisations of complementarity.

Corollary 9.41 The following are equivalent for \circ and \bullet :

(i) complementarity:

$$\begin{array}{c} \bullet \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ \circ \end{array}$$

(ii) for all i :

$$\begin{array}{c} \bullet \\ \triangleleft_i \end{array} = \frac{1}{D} \bullet \quad (9.39)$$

(iii) for all i there exists a phase $\vec{\kappa}$ such that:

$$\begin{array}{c} \triangleleft_i \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ \vec{\kappa} \end{array} \quad (9.40)$$

(iv) for all j :

$$\begin{array}{c} \circ \\ \triangleup_j \end{array} = \frac{1}{D} \circ \quad (9.41)$$

(v) for all j there exists a phase $\vec{\kappa}$ such that:

$$\begin{array}{c} \triangleup_j \end{array} = \frac{1}{D} \begin{array}{c} \circ \\ \vec{\kappa} \end{array} \quad (9.42)$$

(vi) mutual unbiasedness:

$$\forall i, j : \begin{array}{c} \triangle_j \\ \vdots \\ \triangle_i \end{array} = \frac{1}{D}$$

Example 9.42 One advantage of the characterisation of complementarity in terms of mutual unbiasedness is that it is easy to check that a pair of ONBs induces complementary spiders. For example, the Z-basis and the X-basis, which, as we already saw a while back, can be expressed in terms of the Z-basis as:

$$\begin{array}{c} | \\ \hline \triangle_0 \end{array} := \frac{1}{\sqrt{2}} \left(\begin{array}{c} | \\ \hline \triangle_0 \end{array} + \begin{array}{c} | \\ \hline \triangle_1 \end{array} \right) \quad \begin{array}{c} | \\ \hline \triangle_1 \end{array} := \frac{1}{\sqrt{2}} \left(\begin{array}{c} | \\ \hline \triangle_0 \end{array} - \begin{array}{c} | \\ \hline \triangle_1 \end{array} \right)$$

are indeed mutually unbiased:

$$\begin{array}{c} \triangle_j \\ \vdots \\ \triangle_i \end{array} = \frac{1}{2}$$

Hence they induce complementary spiders, and hence we are entitled to represent them by means of complementary colours:

$$\begin{array}{c} | \\ \hline \bigcirc \end{array} := \text{Z-measurement} \quad \begin{array}{c} | \\ \hline \bullet \end{array} := \text{X-measurement}$$

Exercise 9.43 In order to establish equivalence in Theorem 9.40 we relied on explicitly plugging in white and grey basis states. Instead, establish equivalence between (i) and (ii) above by plugging in states from only one basis.

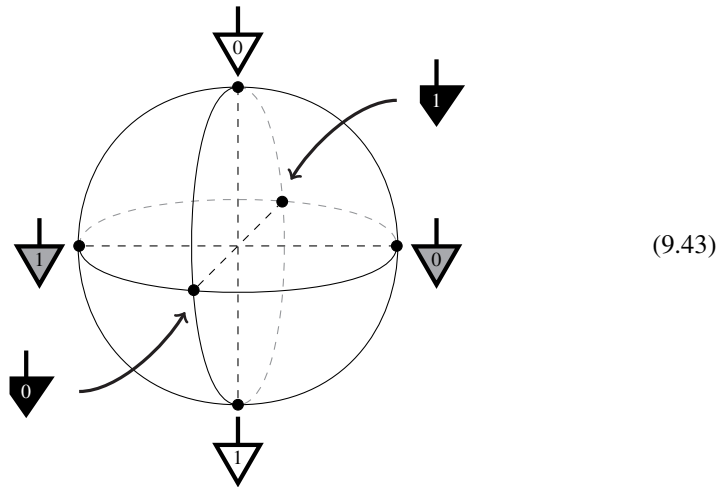
Example 9.44 A set of ONBs is called *pairwise mutually unbiased* if each pair of distinct ONBs in the set is mutually unbiased. Up to an overall unitary, there are three ONBs for qubits that are pairwise mutually unbiased. The Z-basis, the X-basis, and the Y-basis:

$$\begin{array}{c} | \\ \hline \blacktriangle_0 \end{array} := \frac{1}{\sqrt{2}} \left(\begin{array}{c} | \\ \hline \triangle_0 \end{array} + i \begin{array}{c} | \\ \hline \triangle_1 \end{array} \right) \quad \begin{array}{c} | \\ \hline \blacktriangle_1 \end{array} := \frac{1}{\sqrt{2}} \left(\begin{array}{c} | \\ \hline \triangle_0 \end{array} - i \begin{array}{c} | \\ \hline \triangle_1 \end{array} \right)$$

For all i, j , we have:

$$\begin{array}{c} \triangle_j \\ \vdots \\ \blacktriangle_i \end{array} = \begin{array}{c} \blacktriangle_j \\ \vdots \\ \triangle_i \end{array} = \begin{array}{c} \blacktriangle_j \\ \vdots \\ \blacktriangle_i \end{array} = \frac{1}{2}$$

and hence these ONBs are indeed pairwise mutually unbiased. (Note that, while the Y-basis does not consist of self-conjugate basis states, our definition of mutual unbiasedness straightforwardly extends to these.) On the Bloch sphere, they mark the three main axes:



A set of pairwise mutually unbiased bases is called *maximal* if it cannot be extended. Determining the size of such maximal sets for all dimensions is an (extremely hard) open problem, comparable in difficulty to the problem of classifying SIC-POVMs mentioned in Section 7.4.2. In dimension 2, these maximal sets are always of size 3, as above. More generally, if $D = p^N$ for some prime number p , the answer is $p^N + 1$. However, at the time of this writing, the answer for other dimensions, e.g. $D = 6$, is completely unknown.

In (9.43) we depicted the basis states of some very important measurements on the Bloch sphere. In diagrammatic terms, the characteristic property of such a basis state is that they are copied by the relevant spiders:

$$\begin{array}{ccc}
 \text{Spider with white circle} = \text{Spider with white circle} & \text{Spider with grey circle} = \text{Spider with grey circle} & \text{Spider with black circle} = \text{Spider with black circle} \\
 \text{Spider with white circle} = \text{Spider with white circle} & \text{Spider with grey circle} = \text{Spider with grey circle} & \text{Spider with black circle} = \text{Spider with black circle} \\
 \text{Spider with white circle} = \text{Spider with white circle} & \text{Spider with grey circle} = \text{Spider with grey circle} & \text{Spider with black circle} = \text{Spider with black circle}
 \end{array}$$

Since these basis states satisfy several mutual unbiasedness relationships, by Corollary 9.41 we moreover know that each of these states is also a phase state for its complementary spiders, yielding more useful equations. Let's figure out what these phases precisely are for these six states.

We already saw in Example 9.7 that:

$$\begin{array}{ccc}
 \text{Spider with white circle} = \frac{1}{2} \text{ Spider with white circle} & \text{Spider with grey circle} = \frac{1}{2} \text{ Spider with grey circle} & (9.44) \\
 \text{Spider with white circle} = \frac{1}{2} \text{ Spider with white circle} & \text{Spider with grey circle} = \frac{1}{2} \text{ Spider with grey circle} & \\
 \text{Spider with white circle} = \frac{1}{2} \text{ Spider with white circle} & \text{Spider with grey circle} = \frac{1}{2} \text{ Spider with grey circle} &
 \end{array}$$

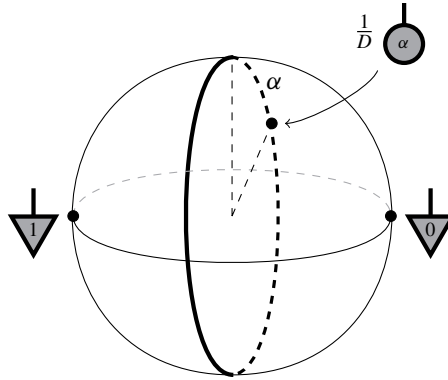
and comparing (9.43) with (9.13) we also have:

$$\begin{array}{ccc}
 \text{Spider with white circle} = \frac{1}{2} \text{ Spider with white circle} & \text{Spider with grey circle} = \frac{1}{2} \text{ Spider with grey circle} & (9.45) \\
 \text{Spider with white circle} = \frac{1}{2} \text{ Spider with white circle} & \text{Spider with grey circle} = \frac{1}{2} \text{ Spider with grey circle} & \\
 \text{Spider with white circle} = \frac{1}{2} \text{ Spider with white circle} & \text{Spider with grey circle} = \frac{1}{2} \text{ Spider with grey circle} &
 \end{array}$$

But we can of course also do something similar in terms of X -phase states, which according to equation (9.12) have the following matrix form:

$$\textcircled{\alpha} = \text{double} \left(\downarrow_0 + e^{i\alpha} \downarrow_1 \right)$$

These grey phase states lie on the equator for the axis that goes through the doubled grey basis states:



and comparing with (9.43) yields:

$$\downarrow_0 = \frac{1}{2} \textcircled{0} \quad \downarrow_1 = \frac{1}{2} \textcircled{\pi} \quad (9.46)$$

$$\blacktriangledown_0 = \frac{1}{2} \textcircled{-\frac{\pi}{2}} \quad \blacktriangledown_1 = \frac{1}{2} \textcircled{\frac{\pi}{2}} \quad (9.47)$$

We could do the same for \bullet too, but we won't bother, since later we will see that for our purposes, we will only need pairs of complementary spiders (see Theorem 9.66). To summarise all the above we present the phase states representing basis states (up to $\frac{1}{2}$) on the Bloch sphere:

(9.48)

Example 9.45 We noted back in Section 5.3.5 that the adjoint of the X -copying map behaves as an XOR operation on the Z basis, more precisely:

$$\text{XOR} = \frac{1}{\sqrt{2}} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

This fact can now be verified simply by using phase spider fusion:

$$\begin{aligned} \text{XOR} &= \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \\ \text{XOR} &= \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \\ \text{XOR} &= \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \\ \text{XOR} &= \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{2} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \end{aligned}$$

9.2.3 The CNOT-Gate from Complementarity

In previous chapters, we have been assuming the existence of certain ‘black boxes’ that have useful properties (e.g. measurements and controlled unitaries). Now that we have a variety of spiders at hand:

- classical, quantum, and bastard spiders:



- phase spiders:



- complementary spiders:



we can start constructing these things. For our first trick, we will show how a pair of complementary spiders always induces a unitary quantum map. In the case of the Z and X complementary pair of Example 9.42, this unitary is the CNOT-gate that we saw in Section 5.3.4:

$$\begin{array}{ccc}
 \begin{array}{|c|} \hline \triangle \\ \hline 0 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 0 \\ \hline \end{array} & + & \begin{array}{|c|} \hline \triangle \\ \hline 0 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & + & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & + & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 0 \\ \hline \end{array} & + & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} \\
 \begin{array}{|c|} \hline \triangle \\ \hline 0 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 0 \\ \hline \end{array} & & \begin{array}{|c|} \hline \triangle \\ \hline 0 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 0 \\ \hline \end{array} & & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array} & \begin{array}{|c|} \hline \triangle \\ \hline 1 \\ \hline \end{array}
 \end{array} \quad (9.49)$$

The notation that we used to denote the CNOT-gate:



includes a white and a grey dot, which clearly points in the direction of two families of spiders. However, what does a horizontal line mean?

Lemma 9.46

$$\begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} = \begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} = \begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} = \begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} \quad (9.50)$$

Proof The proof relies on the fact that:

$$\begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} = \begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} = \begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array}$$

We prove the first equation of (9.50):

$$\begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} = \begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} = \begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array} = \begin{array}{|c|} \hline \circ \\ \hline \end{array} \begin{array}{|c|} \hline \bullet \\ \hline \end{array}$$

The remainder of the proof is left as an exercise. □

Exercise 9.47 Complete the proof of Lemma 9.46.

So since it doesn't really matter how we make the passage from the white to the grey dot with a wire, we can just depict it as a horizontal line. The following now also straightforwardly follows.

Lemma 9.48 For spiders \circ and \bullet the map:



is always self-adjoint.

And we indeed recover the CNOT-gate, at least up to a number.

Exercise 9.49 Show that if we choose \circ and \bullet to be spiders for the Z-basis and the X-basis as in Example 9.42, then:

$$\sqrt{2} \begin{array}{c} | \\ \circ \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array}$$

is the CNOT-gate (9.49).

The fact that \circ and \bullet induce a unitary map gives us yet another collection of alternative characterisations for complementarity.

Proposition 9.50 The following are equivalent for \circ and \bullet :

(i) The spiders are complementary:

$$\begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \circ \\ | \end{array} = \frac{1}{D} \begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \circ \\ | \end{array}$$

(ii) The following linear map is unitary:

$$\sqrt{D} \begin{array}{c} | \\ \circ \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} \quad (9.51)$$

(iii) The following quantum map is unitary:

$$D \begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} \quad (9.52)$$

Proof First, we show that (i) implies (ii). Since (9.51) is self-adjoint, it suffices to show that this map composed with itself is the identity:

$$\begin{array}{c} \sqrt{D} \\ \circ \\ \sqrt{D} \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = D \begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} \stackrel{(9.28)}{=} \begin{array}{c} | \\ \circ \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = \begin{array}{c} | \\ | \\ | \end{array}$$

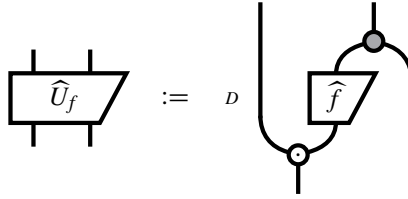
(ii) implies (iii) by doubling the unitarity equations. Conversely, if (9.52) is unitary, then (9.51) is unitary by Theorem 6.20. Thus, it suffices to show that (ii) implies (i):

$$\begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = \frac{1}{D} \begin{array}{c} \sqrt{D} \\ \circ \\ \sqrt{D} \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = \frac{1}{D} \begin{array}{c} | \\ \circ \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = \frac{1}{D} \begin{array}{c} | \\ | \\ | \end{array}$$

where the first step is just spider fusion (and some number juggling), and the second step uses unitarity of (9.51). \square

Exercise 9.51 Give an alternative proof that (i) implies (iii) by first showing causality of (iii).

Remark 9.52 We will see in Section 12.2 that complementarity is equivalent to unitarity of:



for any (doubled) function map f (cf. Definition 8.13). Then, Proposition 9.50 is just the special case where f is the identity. Whereas \hat{f} may not be causal (and hence not a quantum process), \hat{U}_f is always a quantum process. Such a unitary quantum process \hat{U}_f is called a *quantum oracle* and forms a crucial component to many quantum algorithms.

9.2.4 ‘Colours’ of Classical Data

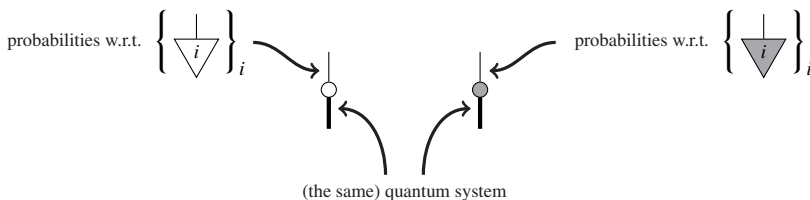
The careful reader may have noticed that we have thus far glazed over an important point about multicoloured spiders and classical wires. Let’s have a look at the matrix form of the measure processes for two different spiders:



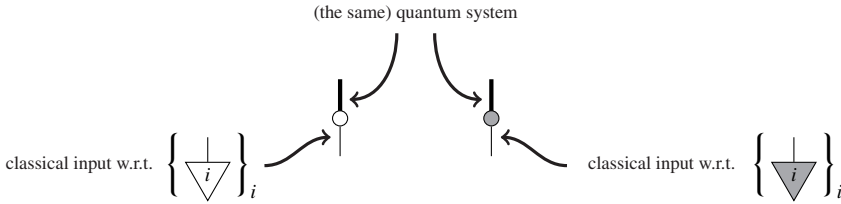
It is clear that these measurements both produce classical states, but these classical states don’t look exactly the same:

$$\sum_i p^i \begin{array}{c} \downarrow \\ i \end{array} \quad \text{vs.} \quad \sum_i p^i \begin{array}{c} \downarrow \\ i \end{array}$$

That is, the classical states are encoded in different ONBs. This is a feature rather than a bug. The numbers that make up a probability distribution are totally useless information, unless we also know what these numbers are probabilities of. In the two classical states above, the ONBs tell us what the numbers p^i are about; namely, they are the probabilities for the outcomes of a particular measurement. More generally, a classical wire carries a specification of how that classical data was produced, i.e. by which measurement:



Similarly, for encoding we have:

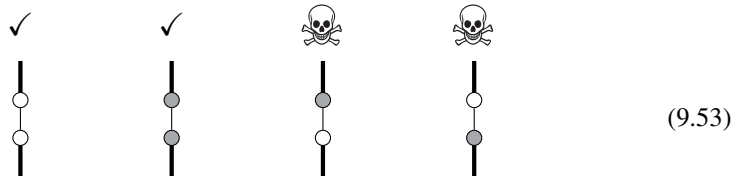


The bottom line is: classical wires carry additional type information about the basis in which the classical data is encoded. We could make this information explicit if, for instance, we labeled wires as follows:

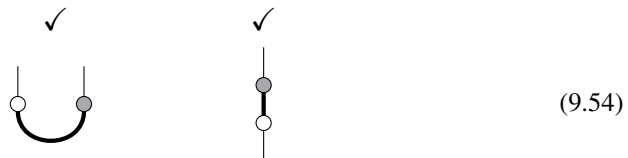


but this won't really be necessary since the type will always be clear from the context. Most importantly, any thin wire connected to a bastard spider carries classical data of that 'colour'.

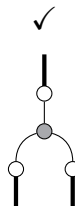
As with any kind of system-types, we don't allow wires of different types to be plugged together:



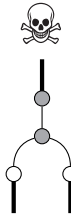
On the other hand, both of these measurement choices (crucially) operate on the same type of quantum system; so, for instance, these compositions are allowed:



The golden rule one should take from (9.53) is that bastard spiders of different colours should never be connected via classical wires. On the other hand, it might sometimes be the case that a classical spider of one colour is actually a valid classical map for another colour. We already encountered such an example in Proposition 5.88 where we saw that an XOR gate in the white basis is matching in the grey basis. In that case, a linear map such as:

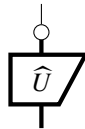


could indeed be a valid cq-map. However:



violates the golden rule, since now bastard spiders of different colours are touching the same type of classical wire.

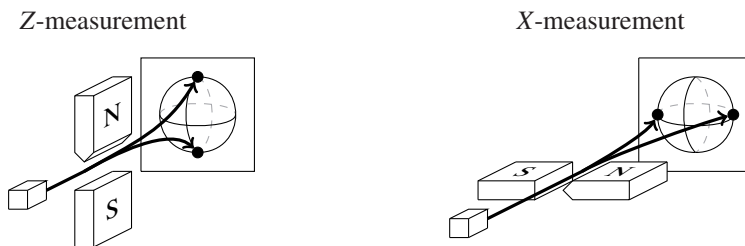
Remark 9.53 We could instead choose to use one fixed basis for classical outcomes and define ONB measurements via a single dot and a unitary, as we did in Section 8.4.1:



However, as we have already seen in the past three sections, representing classical data in different bases substantially simplifies our diagrams and calculations.

9.2.5 Complementary Measurements

Let's use complementarity to show some interesting quantum features. We return to the Stern–Gerlach apparatus that we studied in Sections 7.1.1 and 7.1.2. Recall that we could measure in different ONBs just by rotating the whole device:




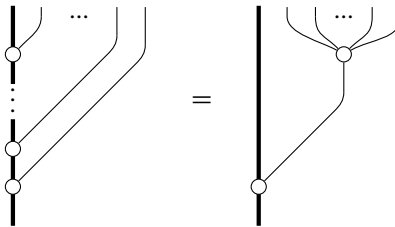
From example 9.42 we also know that the Z- and X-measurements can be described by means of complementary spiders:



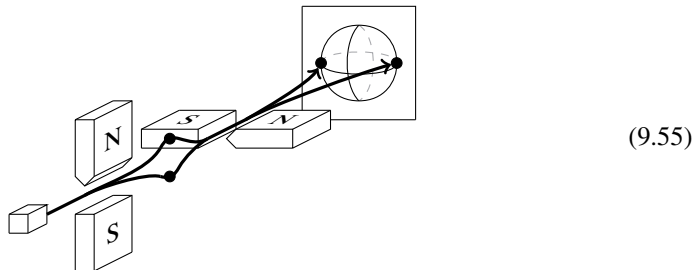
with respect to the Z- and X-bases from Example 9.42. If, rather than letting the particles hit a screen, we allow them to pass on through, we obtain complementary non-demolition measurements (cf. Section 8.4.1):



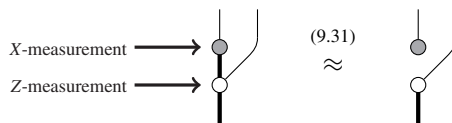
If we pretend we don't know anything about quantum measurements, it could be the case that the particles produced by  have a 'Z-property' that tells us which way they will deflect in a Z-measurement and an 'X-property' that tells us which way they will deflect in an X-measurement, and the operations above correspond to just 'observing' those properties. When we perform these measurements in isolation, this interpretation seems okay. For example, no matter how many times we 'observe the Z-property', we'll get the same result:




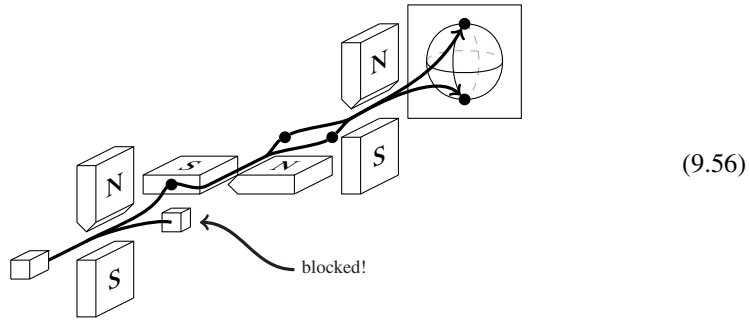
However, when we start combining Z-measurements and X-measurements, this measurement-as-observing idea breaks down. First, suppose we perform a Z-measurement before an X-measurement:



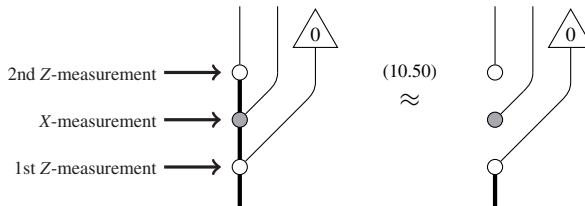
In diagrams, the experimental setup of (9.55) becomes:



That is, the X-measurement always produces a uniform probability distribution, no matter what state we input into the apparatus. If we just observed these probabilities in a lab, without having complete control over the states we input, we might not think this is so strange. It could just be that our particle source  is producing particles that will yield an X-value of 0 half the time and 1 the other half of the time. However, we can definitely convince ourselves that there is something fishy going on if we add a third Stern-Gerlach device:



and block one of the exits of the first Z-measurement. Supposing this is the exit corresponding to outcome 1; the particle will only hit the screen at the end if the first measurement yields 0. We can restrict to just the scenarios where the first measurement yields outcome 0 as follows:

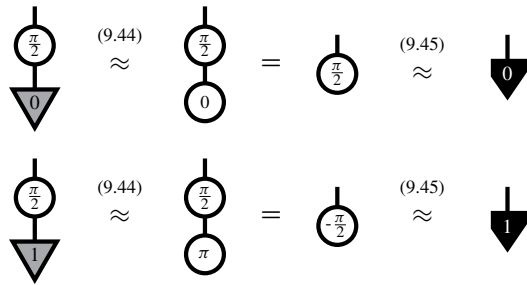


Even when we only allow particles through that yield 0 in the first Z-measurement, by the time we measure Z again, rather than getting 0 again, we get the uniform probability distribution! Of course, it is the presence of the X-measurement in the middle that causes this to happen. This setup is one of the most famous demonstrations of how measurements in quantum theory behave very differently from just ‘observing’ some property of a system. The fact that one measurement affects the outcomes of another one in this manner is referred to as *incompatibility* of measurements. Since complementary measurements will cause each other’s outcomes to be complete noise, they are *maximally incompatible*.

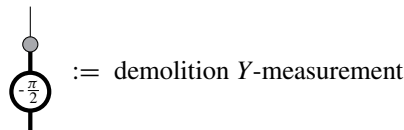
In addition to the fact that it gives one of the most striking physical manifestations of the ‘properly quantum’ feature of complementarity, we have also included this example to show the unreasonable effectiveness of diagrammatic reasoning with spiders! The arguments above each merely required a single application of a spider detachment rule.

Thanks to this simplicity, we can easily consider other similar situations. From Example 9.44 we know that also Y-measurements should be maximally incompatible both with X-measurements and Y-measurements, so we should be able to derive similar results involving Y-measurements along the lines of what we derived above. One way to do so could be introducing a third colour, but that’s not even necessary. It suffices to throw in some decorations.

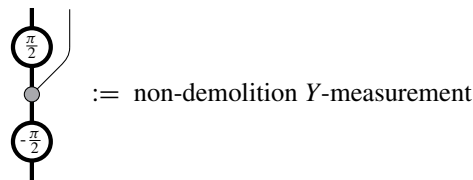
Since both the X-basis states and the Y-basis states lie on the equator of the Bloch sphere (cf. picture (9.43)), we can use a white phase gate to turn one basis into the other:



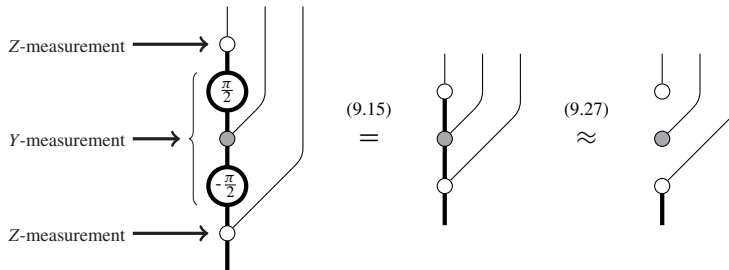
Recalling from Section 8.4.1 that general ONB-measurements consist of a unitary composed with a measure spider, we can transform the X -measurement into a Y -measurement as follows:



with a corresponding:

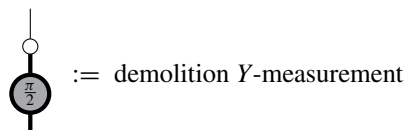


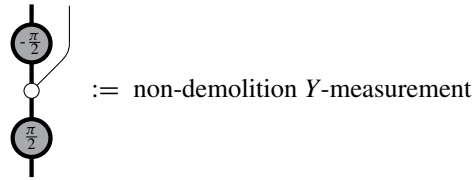
Using phase/bastard spider fusion we have:



Exercise 9.54 Compute the result of first performing a non-demolition Y -measurement, then a Z -measurement, and then again a Y -measurement diagrammatically.

Similarly, one can also represent Y -measurement using X -phase gates:





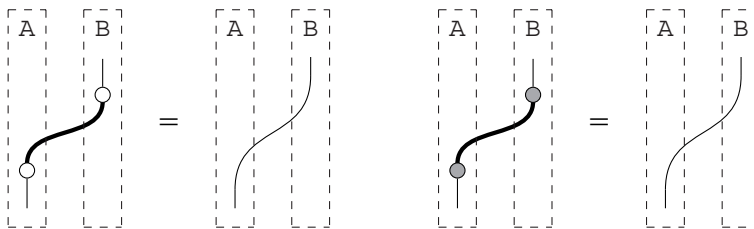
and the same results can of course also be derived in this alternative form.

9.2.6 Quantum Key Distribution

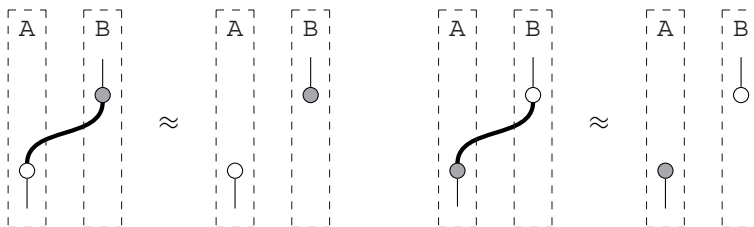
Something very closely related to our analysis of incompatibility in the previous section is *quantum key distribution* (QKD). In particular, we will see how a complementary pair of measurements can be used to establish a common secret (e.g. a cryptographic key) between Aleks and Bob in such a way that they will always be able to tell if someone is eavesdropping (hence justifying the use of the term ‘secret’). The most well-known protocol for QKD is called BB84. The actual quantum part of the protocol is extremely simple. We’ll use bits and qubits to describe the protocol, but it works just fine for $D > 2$. All that is required is complementarity.

Essentially, Aleks has a bunch of random bits that he wants to send to Bob. He doesn’t particularly care if they all get there. He will already be happy if enough of the bits get there to make a cryptographic key, which he can then use to do the ‘real’ secret communication with Bob.

To do so, Aleks and Bob first fix a pair of complementary spiders \circ and \bullet and Aleks selects with equal probability to encode his classical data either using \circ -encode or \bullet -encode. Afterwards, Bob chooses with equal probability to either \circ -measure or \bullet -measure. If the two choices agree, Bob gets Aleks’ bit:

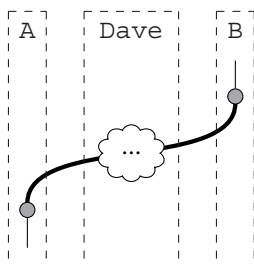


If the two choices are different, Bob gets noise, i.e. the uniform distribution:



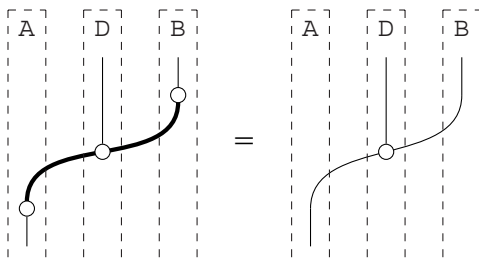
They repeat this for all of the bits Aleks wants to send Bob, knowing that there is a 50% chance Bob will get Aleks' bit, and a 50% chance he will get garbage. Afterwards, to know which is which, Aleks and Bob simply announce which colour of spider they used to encode/measure each bit. For the bits where the colour was the same, they know they have the same value, and the rest they throw away. Since Aleks' encoding and Bob's measurement choices were random, and have nothing to do with the key they are trying to establish, they can broadcast this data publicly, and don't have to worry about any sketchy dodos getting hold of the private key.

On the other hand, what if sketchy Dave is listening in on the channel Aleks is using to send his quantum systems to Bob?

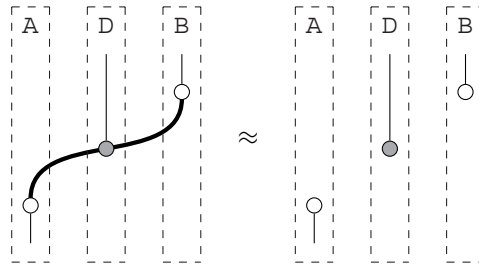


If it were possible to clone a quantum system, Dave could simply keep a copy of every state Aleks sends to Bob, then, once Aleks and Bob announce their bases, Dave can simply measure his copy to get the message. Of course, we've known since Chapter 4 that this isn't possible, so the best Dave can do is perform a measurement of some kind.

First, for simplicity we'll assume that Dave also chooses his measurements from \circ/\bullet . We'll look at the instances where Aleks and Bob intend to keep the bit Aleks is sending, i.e. when their choices of \circ/\bullet are the same. Since Aleks is choosing his encoding bases randomly, the best Dave can do is measure in the correct basis half of the time. When that happens, he does indeed get a copy of Aleks' bit:

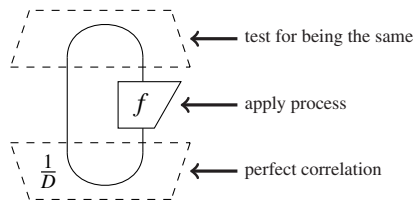


However, the other half of the time, Bob will get noise, just like when he made the wrong measurement choice:



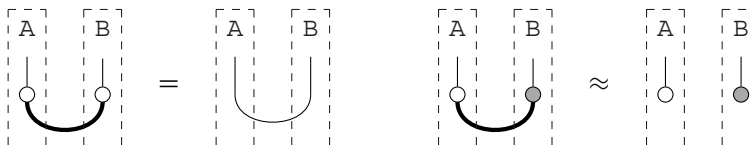
Rather than receiving Aleks' bit correctly half the time, Bob sometimes gets noise instead, so the probability that Bob gets the correct bit goes down. This suggests an easy strategy for detecting eavesdroppers. Every once in a while, Aleks and Bob randomly pick out a bunch of spare bits (i.e. bits Aleks sent but that they don't intend to use) and compare them. If significantly fewer than 50% of the bits are correct, someone must be eavesdropping, so they call it a day.

Exercise* 9.55 What is the probability of Bob getting Aleks' bit when Dave is eavesdropping? Note that, assuming a process is fed a classical state in the uniform probability distribution, the probability that it produces the same input as output can be computed via the Born rule as follows:



Remark 9.56 It can be shown that it is possible to detect Dave even if he is allowed to perform arbitrary quantum processes, not just \circ/\bullet -measurements. However, the analysis is quite a bit trickier (cf. the references in Section 9.7).

One of the benefits of a graphical presentation is we can simply bend the wires around and read off a seemingly different protocol. Suppose instead of Aleks sending systems to Bob along a quantum channel, Aleks and Bob instead share a Bell state. Then, if they both make random choices of measurements, they establish perfect correlations when the measurements are the same, and no correlations when they are different:



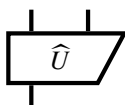
This gives a (simplified version of) a different QKD protocol, called E91. Even though the actual steps in the protocol are different, the result is the same. Ultimately, Aleks and

Bob end up with a perfectly correlated string of random bits. Furthermore, since we are working with essentially the same diagrams, we can check for eavesdropping just as we did before. However, reading BB84 ‘sideways’ has some additional benefits. First, Aleks and Bob do not need to be continuously in (quantum) contact to share the key. They just need to establish some shared Bell states at some point, then ‘use them up’ as needed. Second, Aleks and Bob can be sure they have real Bell states (i.e. they haven’t been tampered with) by checking that their measurement outcomes actually exhibit quantum non-locality, which we will discuss at length in Section 11.1.

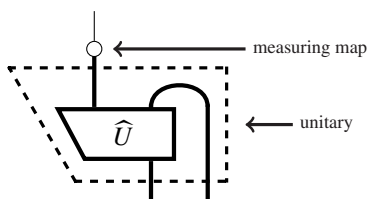
Remark* 9.57 In the full version of E91, Aleks and Bob check for non-locality by incorporating a third measurement and checking that the correlations between their measurement outcome violate what’s known as a *Bell inequality*. Such a violation guarantees non-locality. A nice thing about this technique is they only have to share their outcomes for the ‘garbage’ bits, i.e. where their measurement choices disagree, so they don’t need to sacrifice any usable bits to check security.

9.2.7 Teleportation with Complementary Measurements

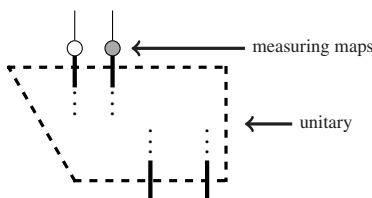
As promised, we can replace the ‘black box’:



used in teleportation by something constructed entirely by means of spiders. Teleportation relies initially on Aleks making a joint measurement on his two systems:

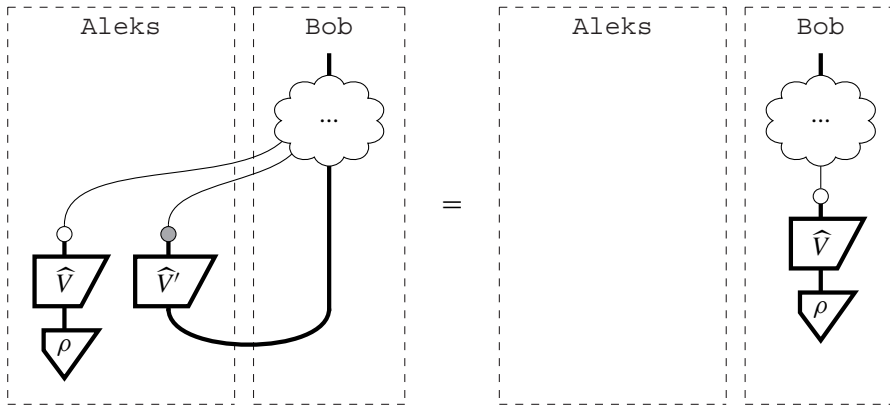


If the quantum systems have dimension D , the classical wire will take D^2 different values. Therefore, we could just as well represent it with two classical wires that each take D possible values:



(9.57)

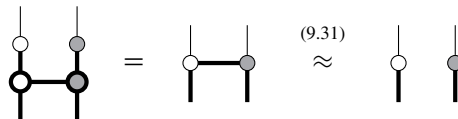
(The fact that we used two different colours anticipates what will follow.) Now, to get some teleportin' done, this measurement better not \otimes -separate, otherwise Bob will, at best, get some decoherent version of Aleks' state, since everything would then have to pass through a classical wire:



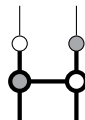
Given that we have a complementary pair of spiders around, we can try to use the induced unitary from Proposition 9.50:



to produce a non-separable measurement. Here's our first attempt:

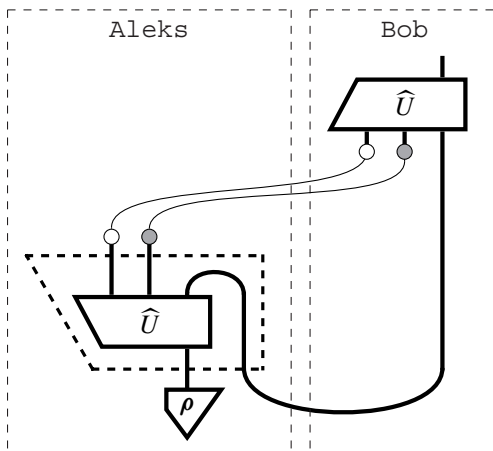


Oops, that didn't work! Applying the CNOT didn't change the measurement at all! In particular, it is still separated. However, since we are trying to do some science, let's experiment some more. What happens if we plug the induced unitary in the other way?

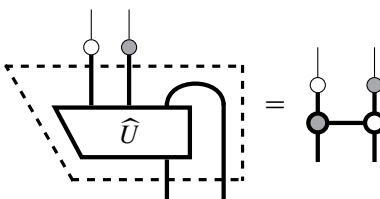


(9.58)

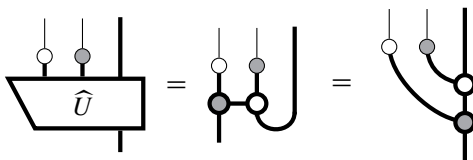
This flipped version is of course also unitary, so (9.58) is still an ONB-measurement, and furthermore it doesn't \otimes -separate in any obvious way. That isn't a proof that it doesn't separate, of course, but we will know that's the case if it gives us a working teleportation protocol. So, let's play 'fill in the boxes' for this teleportation diagram:



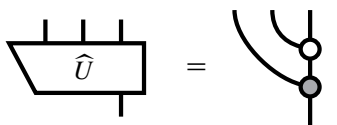
Since we already have a candidate for Aleks' measurement, we just need to find \hat{U} , which is needed for constructing Bob's correction. This amounts to finding a solution to the following equation:



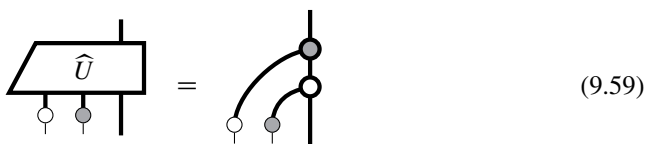
Bending up the wire on both sides yields:



so a valid solution is:

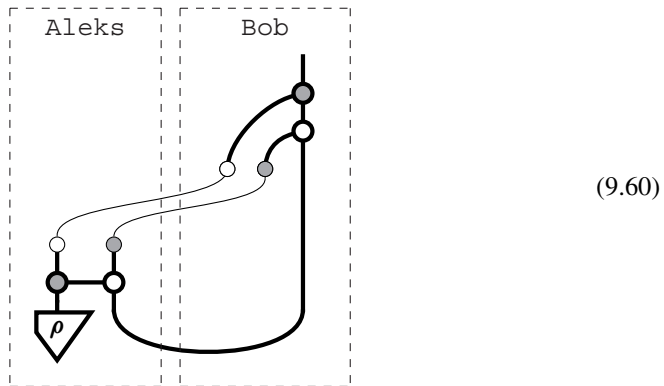


Hence, the correction is:

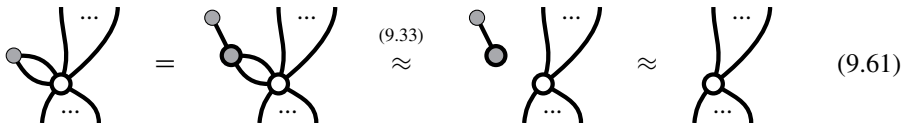


Exercise 9.58 Prove (9.59) is causal and a controlled unitary (up to a number).

Filling in the boxes yields the following candidate teleportation protocol:



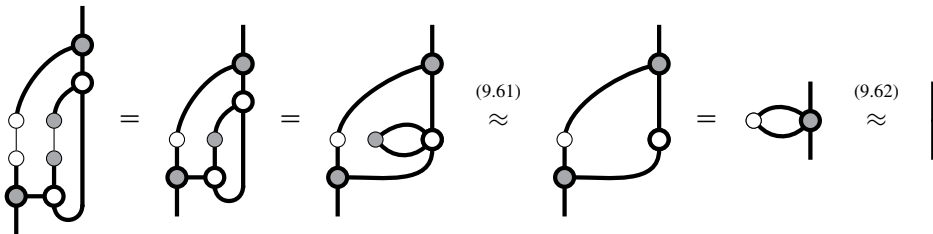
So it only remains to show that the thing actually works for our choice of \hat{U} . Using the spider-fusion rules and complementarity, we can indeed show that (9.60) performs quantum teleportation. We will in particular make use of the following fact:



which uses bastard spider fusion and the quantum ‘spider detachment’ rule. Simply swapping colours we also have:

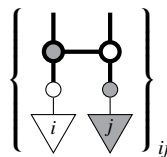


From this, we can conclude that this instance of teleportation indeed works:



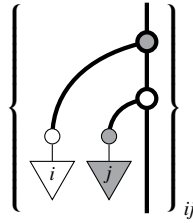
Exercise 9.59 Show, in the case where \circ and \bullet represent the Z- and X-bases, that:

1. The Bell basis is:



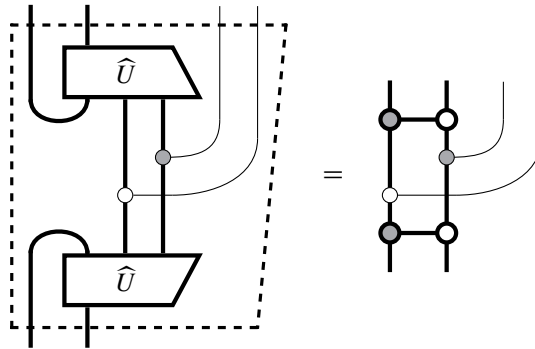
(ignoring numbers) and hence (9.58) is a Bell-basis ONB measurement.

2. The Bell maps are:



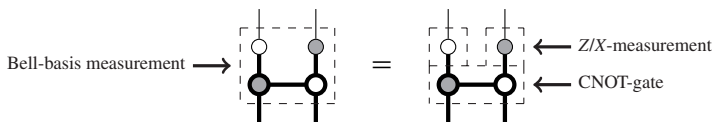
So (9.60) gives us a fully comprehensive diagrammatic presentation of the same quantum teleportation protocol we have been studying all along, but now with a general recipe for ‘filling in’ the boxes. All we need to do is find a complementary pair of spiders for any dimension, and the teleportation protocol (9.60) (along with the proof of correctness!) goes through unmodified.

The same ingredients allow us to do this for dense coding and for entanglement swapping. In the latter case, the required non-demolition measurement becomes:



Exercise 9.60 Prove correctness for dense coding and entanglement swapping only using spider-fusion and spider-detachment rules.

As we have seen many times before, a single diagram can have more than one possible reading. This is also the case of diagram (9.58):



While for our purposes, i.e. unveiling quantum features, this distinction is not of any importance, for someone implementing quantum processes in a laboratory it may make a huge difference. For example, it may be really hard to make any non-separable measurement on two systems; it may be easier to perform a quantum CNOT-gate and perform single-system measurements, which turns out to be the case for most laboratory realisations of quantum systems.

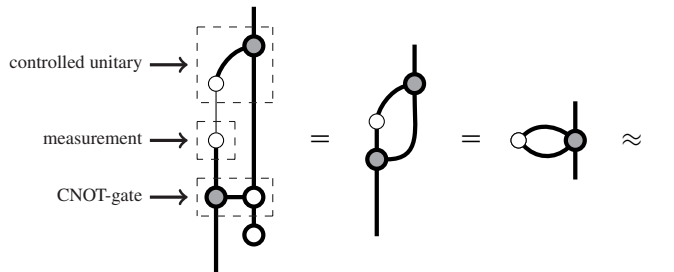
Example 9.61 Quantum teleportation allows us to transfer the state from one system to another, using:

- an ancillary system
- a Bell state
- a quantum CNOT-gate
- two single-system measurements, and
- two single system corrections.

One may wonder if there is a manner of doing the same thing requiring fewer resources, and this is indeed the case. In fact, we only need:

- a \bigcirc -state
- a quantum CNOT-gate
- one single-system measurement, and
- one single system correction.

In particular, no ancillary system is needed. This is how this goes:



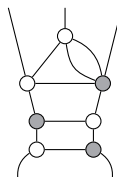
So instead of having two systems prepared in a Bell state, we now only need to have one system prepared in a 0-phase state. The price we pay is that, unlike teleportation, state transfer requires the source and the target system to be in the same place so a CNOT can be applied to both, since at the moment there's no such a thing as a 'non-local CNOT-gate'.

It is also insightful to compare this correctness proof with the one of teleportation; in particular, this proof is essentially the same as the two last steps of the teleportation proof.

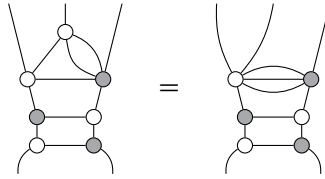
9.3 Strong Complementarity

We've already made great progress in proving things by only using simple diagrammatic rules such as (phase) spider fusion and spider detachment. But how powerful are the rules we have so far? In other words, what sort of diagrams can we simplify just using these rules?

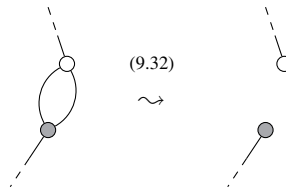
Suppose we have some reasonably complex diagram involving complementary spiders:



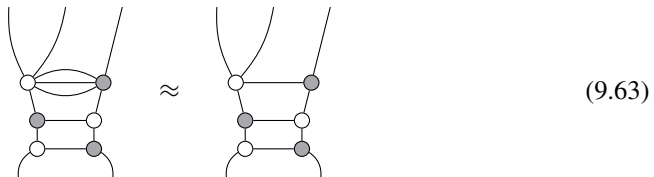
and we want to start simplifying it. We can of course apply spider rules to fuse any dots of the same colour:



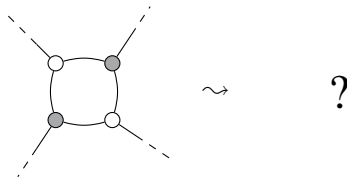
After that, we end up with a diagram that has cycles of spiders with alternating colours, which we can try to get rid of. These are of course always even, so we can ask how to deal with 2-cycles, 4-cycles, etc. For 2-cycles, we can just apply complementarity:



This allows us to reduce the complexity to the above example a bit:



However, now those pesky 4-cycles trip us up, since none of the rules we have so far will apply:



In rewriting terminology, having no rules that apply means you have arrived at a *normal form*, which is sometimes just a nice way of saying ‘you’re stuck’. What should we do? Call it a day? Alternatively, we can try to find the ‘missing rule(s)’ to carry on.

9.3.1 The Missing Rules

Let us focus for a moment on the Z and X spiders. In Example 9.45 we recalled that this pair of spiders satisfies a distinctive property; namely, the adjoint of the X-copying map behaves as an XOR operation on the Z basis:



For one thing, this gives us another way to see why these two spiders are complementary, simply by thinking about classical bits. Namely, XOR-ing any bit with itself always gives the zero bit, so if we copy-then-XOR, that's the same as ignoring the input and outputting a zero:

$$\begin{array}{c} \bullet \\ \circ \end{array} \approx \begin{array}{c} \text{XOR} \\ \circ \end{array} = \begin{array}{c} \triangle 0 \\ \circ \end{array} \stackrel{(9.46)}{\approx} \begin{array}{c} \bullet \\ \circ \end{array}$$

In addition to this property, a (seemingly) unrelated consequence is that the grey dot defines a function map (see Definition 8.13) for the white basis, whose underlying function is of course XOR. In Proposition 8.19 from the last chapter, we gave a succinct characterisation of function maps in terms of copying and deleting. Applying this to XOR yields:

$$\begin{array}{c} \text{XOR} \quad \text{XOR} \\ \circ \quad \circ \end{array} = \begin{array}{c} \circ \\ \text{XOR} \end{array} \quad \begin{array}{c} \circ \\ \text{XOR} \end{array} = \begin{array}{c} \circ \quad \circ \end{array}$$

and we already saw that the \bullet -spider with a single output is, up to a number, part of the \circ -ONB, so:

$$\begin{array}{c} \circ \\ \bullet \end{array} \stackrel{(9.46)}{\approx} \begin{array}{c} \circ \\ \triangle 0 \end{array} = \begin{array}{c} \triangle 0 \quad \triangle 0 \end{array} \stackrel{(9.46)}{\approx} \begin{array}{c} \bullet \quad \bullet \end{array}$$

Replacing the first two of these equations with X -spiders, we obtain:

$$\begin{array}{c} \bullet \quad \bullet \\ \circ \quad \circ \end{array} \approx \begin{array}{c} \circ \\ \bullet \end{array} \quad (9.64)$$

$$\begin{array}{c} \circ \\ \bullet \end{array} \approx \begin{array}{c} \circ \quad \circ \end{array} \quad \begin{array}{c} \circ \\ \bullet \end{array} \approx \begin{array}{c} \bullet \quad \bullet \end{array} \quad (9.65)$$

It now becomes obvious that the role played by Z and X in these equations is interchangeable; that is, the above equations also hold with all of the colours reversed, just by taking the adjoint of each equation. The last two equations also imply one more relating the two single-legged spiders:

$$\begin{array}{c} \circ \\ \bullet \end{array} \approx \boxed{} \quad (9.66)$$

which just amounts to saying the number above is non-zero.

Exercise 9.62 Show that spiders satisfying (9.65) also satisfy (9.66).

While (9.64) and (9.65) seem like an ‘accidental’ property of Z and X , if we assume these equations for an arbitrary pair of spiders, we see that equations (9.64) and (9.65) imply complementarity.

Theorem 9.63 Equations (9.64) and (9.65) imply complementarity.

Proof By Proposition 9.35, it suffices to show the complementarity equation up to \approx . We have:

So, equations (9.64) and (9.65) yield very special pairs of complementary spider families, which suggests the following name.

Definition 9.64 A pair of spiders \circ and \bullet are *strongly complementary* if they satisfy the following equations:

(9.67)

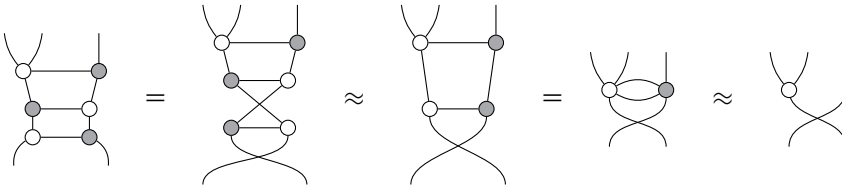
(9.68)

While they aren’t too important, we have included the numbers in the above equations for the sake of completeness. In fact, as with complementarity, they are already fixed by the number-free versions.

Exercise 9.65 Prove the numbers in Definition 9.64 are uniquely fixed by (9.64) and (9.65), as we did for complementarity in Proposition 9.35. Note in particular that it is important here that \approx means equivalence up to a positive number (cf. Remark 9.36).

So what does all of this have to do with our introductory chat about 4-cycles? Well, that’s exactly what this is about, since the LHS of equation (9.67) is nothing but a 4-cycle with a twist:

Hence, we now know what to do with a 4-cycle, and pick up where we left off in (9.63):



Much better!

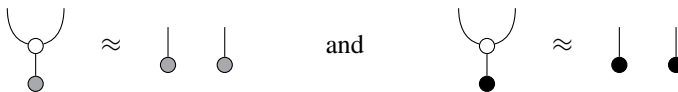
On the other hand, while we introduced complementarity by means of a very crisp canonical interpretation, there isn't really any compelling counterpart to this in the case of strong complementarity. However, despite the lack of a canonical interpretation, strong complementarity will have important consequences in the rest of this chapter (and book). We will look at some of these consequences in the next section. None of these holds for general (not strongly) complementary pairs of spider families.

9.3.2 Monogamy of Strong Complementarity

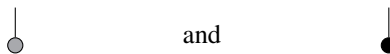
In Example 9.44, we remarked that for most dimensions, the maximum number of pairwise complementary spiders (a.k.a. mutually unbiased ONBs) is unknown. Since strong complementarity puts tighter constraints on which spiders can be related, this number should be smaller. In fact, we can show that strongly complementary spiders only come in pairs.

Theorem 9.66 At most two spiders can be pairwise strongly complementary. That is, for any non-trivial system if \circ/\bullet and \circ/\bullet are both strongly complementary, then \bullet/\bullet cannot be strongly complementary.

Proof Suppose \circ/\bullet and \circ/\bullet are both strongly complementary. Then:



So, by Theorem 8.18:



are both \circ -ONB states, up to a number. Thus, they must be equal (up to a number) or orthogonal. Now, assume \bullet/\bullet are also strongly complementary, then by (9.66):

$$\begin{array}{c} \bullet \\ \bullet \end{array} \approx \boxed{} \neq 0$$

so:



But then:

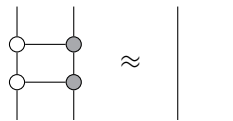


which cannot be the case for any non-trivial system. Hence no non-trivial system can have three pairwise strongly complementary spiders. \square

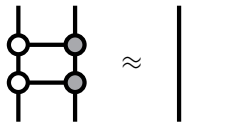
9.3.3 Faces of Strong Complementarity

Earlier we encountered a number of equivalent operational characterisations of complementarity: in terms of measuring after encoding in Definition 9.27, in terms of measuring two systems in a Bell state in Proposition 9.30, and in terms of CNOT-gates in Proposition 9.50. Since strong complementarity implies complementarity, all of these still hold for strongly complementary pairs, but obviously there will be many more consequences. In this section we go through the most important of these.

In Proposition 9.50 we learned that complementarity boils down to unitarity for ‘generalised-CNOT’ gates:

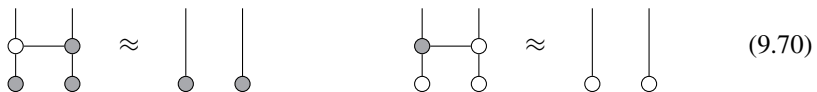
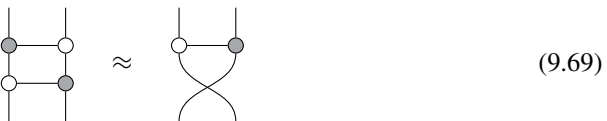


or, equivalently, in terms of ‘generalised-quantum-CNOT’ gates:



This equation can be seen as one between quantum circuits (cf. Examples 6.13 and 9.24). Strong complementarity can be put in a similar form.

Proposition 9.67 Strong complementarity is equivalent to:



Doubling equation (9.69), we obtain:



Consequently, three CNOT-gates make a swap:

Exercise 9.68 Show that, when assuming complementarity, equations (9.69) and (9.71) are indeed equivalent to equations (9.72).

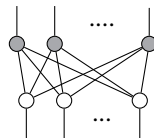
We initiated our search for strong complementarity in order to get rid of 4-cycles, so one might be tempted to think that strong complementarity is really only saying something specifically about 4-cycles. However, it turns out to imply equations between a much more general family of diagrams. As a simple example, we can combine the copying equations:

with spider fusion, to prove the n -ary version of these copying rules:

Proposition 9.69 Strong complementarity implies:

A more complicated example involves the following diagrams:

Definition 9.70 A *complete bipartite diagram* of spiders is a diagram with the property that every spider of one colour is connected to every spider of the other colour, and nothing else:



Even though this diagram seems to be highly connected, we can use strong complementarity to simplify it to two spiders connected by just a single wire.

Theorem 9.71 Strong complementarity of \circ and \bullet is equivalent to:

$$\text{Diagram (9.74)} \quad (9.74)$$

Proof We'll prove this using two inductions. First we'll show the special case where $n = 2$ and m is arbitrary:

$$\text{Diagram (9.75)} \quad (9.75)$$

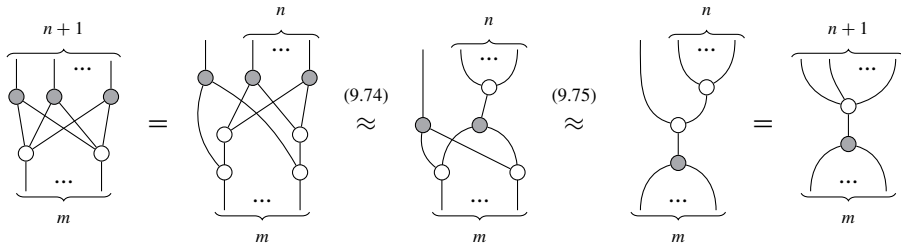
by induction on m . For the base case, $m = 0$, this is simply:

$$\text{Base case } m=0$$

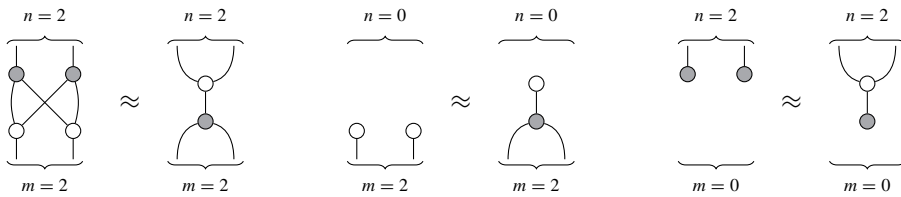
For the step case, we will assume (9.75) for fixed m and prove it for $m + 1$:

$$\text{Step case } m+1$$

Thus we have shown (9.75). From this, we can show (9.74) by induction on n . The base case is just an m -ary copy, like the ones proved in Proposition 9.69. For the step case, we assume (9.74) for fixed n , and show it for $n + 1$. The proof is almost the mirror image of the previous one, except we use (9.75), which is a 'beefed up' version of (9.64):

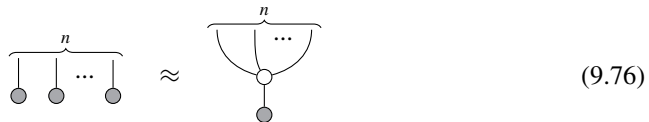


Conversely, the three strong complementarity rules from (9.64) and (9.65) all arise as special cases of (9.74):

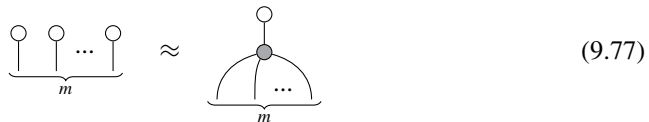


□

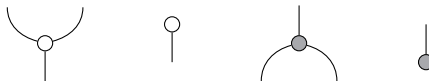
Moreover, restricting equation (9.74) to $m = 0$ yields one of the ‘multi copy’ laws from Proposition 9.69, when read from right to left:



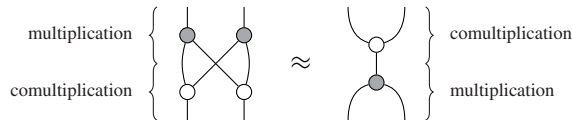
and similarly, restricting to $n = 0$ yields:



Remark* 9.72 At first sight, it might seem like we are just pulling equation (9.74) out of a hat. Thankfully this is not the case, but rather comes from the fact that for any strongly complementary pair, these maps:

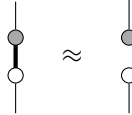


form an algebraic structure called a *bialgebra*, where ‘bi’ refers to the fact that both algebra and coalgebra are involved (cf. Remarks 3.17 and 8.22). The defining equation represents a somewhat funky commutation of the multiplication (i.e. algebra) and the comultiplication (i.e. coalgebra):



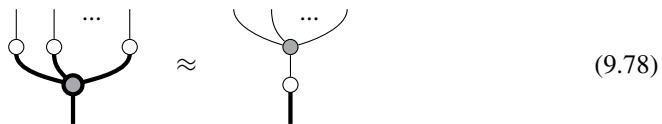
These structures are well understood, and it is possible to construct equations involving them using a technique called *path counting*. This is detailed in Section* 9.6.2.

Theorem 9.71 gives us a second equivalent presentation of strong complementarity. However, none of the presentations of strong complementarity given thus far resembles our initial definition of complementarity, which involved both classical and quantum systems:

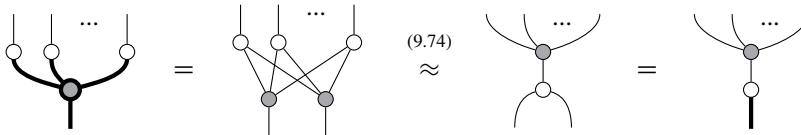


Just by combining some doubled parts of (9.74) into cq-maps, strong complementarity provides us with more equations that help us reason about classical-quantum interaction. The following one will play a crucial role in our derivation of quantum non-locality in Section 11.1.

Corollary 9.73 Strong complementarity of \circ and \bullet implies:



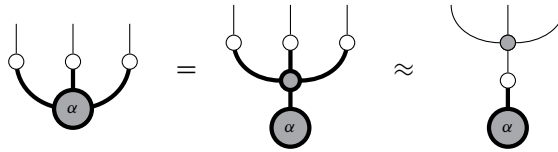
Proof By applying Theorem 9.71, we have:



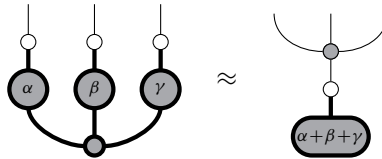
where the first equality is simply undoubling, and the third one is redoubling. \square

The \bullet -spider in the LHS of (9.78) is a quantum process, whereas the \bullet -spider in the RHS is seen here as an operation on classical data. We'll see in Section 9.3.5 what precisely this process does. In the meantime, we can interpret equation (9.78) as follows: if we first apply the given quantum \bullet -spider and \circ -measure all of its outputs, this is the same as performing a \circ -measurement and then the classical \bullet -spider. This of course lacks some of the conceptual crispness of (ordinary) complementarity but is nonetheless very useful.

Example 9.74 In Example 9.26 we saw how phases interact in a very surprising way within a GHZ state. However, attempting to perform a measurement of the same colour as the phases simply destroys the phases. On the other hand, if we perform a measurement of a colour that is strongly complementary to that of the phases, things work out quite differently:

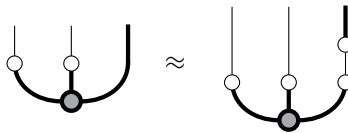


What we have now is that the three measurements are replaced by a single measurement, followed by some classical map. And since the phase is unbiased with respect to \bullet and not \circ , it does not vanish. Moreover, as we will show in Section 11.1, particularly clever choices of measurement phases α , β , and γ in:

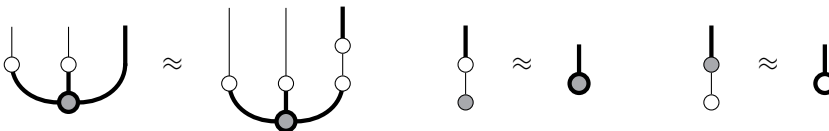


will even leave hard evidence of this surprising ‘backwards movement’ of phase data and predict the existence of interactions between distant quantum systems that cannot be explained by mere probabilistic correlations, i.e. quantum non-locality.

Exercise 9.75 Show that strong complementarity implies:



Can you give an interpretation for this equation? Conversely, show that these equations imply strong complementarity (not so easy!):



9.3.4 The Classical Subgroup

In Section 9.2.2 we saw that for complementary pairs of spiders, the basis states of one colour live in the phase group (cf. Section 9.1.4) of the other colour. In this section we provide another characterisation of strong complementarity in terms of the special role basis states of one colour play in the phase group of the other colour. While the characterisation that we give in this section seems completely different from the one given in Definition 9.64, we will have to do remarkably little work to show it is equivalent.

We saw in Example 9.7 that X -basis states could be represented as phase states, with respect to the Z -basis:

$$\begin{array}{c} \downarrow \\ \text{0} \end{array} \approx \begin{array}{c} \circ \\ \text{0} \end{array} \quad \begin{array}{c} \downarrow \\ \text{1} \end{array} \approx \begin{array}{c} \circ \\ \pi \end{array}$$

and conversely, Z -basis states can be represented as X -phase states:

$$\begin{array}{c} \downarrow \\ \text{0} \end{array} \approx \begin{array}{c} \bullet \\ \text{0} \end{array} \quad \begin{array}{c} \downarrow \\ \text{1} \end{array} \approx \begin{array}{c} \bullet \\ \pi \end{array}$$

We also saw that we can compute their group-sums simply by means of spider fusion (cf. Theorem 9.20):

$$\begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \text{0} \quad \text{0} \end{array} = \begin{array}{c} \circ \\ \text{0} \end{array} = \begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \pi \quad \pi \end{array} \quad (9.79)$$

$$\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \pi \quad \text{0} \end{array} = \begin{array}{c} \bullet \\ \pi \end{array} = \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \text{0} \quad \pi \end{array} \quad (9.80)$$

Notably, all these group sums result in one of the two phase states we started with. That is, the phase states that (up to a number) make up the Z -basis are *closed* under group-summation in the X -phase group. Moreover, they also contain the X -phase group unit and inverses of all of the Z -basis elements (since by (9.79), they are all self-inverse). Hence, they form a *subgroup* of the phase group. In fact, it is a standard result in group theory that a finite subset of a group that is closed under the group-sum is automatically a subgroup, so we actually don't even need to verify the unit and the inverses. Evidently, the same is also true if we exchange the roles of Z and X spiders.

Example 9.76 For the Z - and X -bases, the phase group is the circle group $U(1)$ and the classical subgroup is the two-element cyclic group \mathbb{Z}_2 , which can be represented as no rotation and a half-rotation:

$$\left\{ \begin{array}{c} \circlearrowleft \\ \text{0} \end{array}, \begin{array}{c} \circlearrowleft \\ \pi \end{array} \right\} \subseteq \left\{ \begin{array}{c} \circlearrowleft \\ \alpha \end{array} \right\} \quad (9.81)$$

The appearance of this subgroup is a direct consequence of strong complementarity. In fact, it is equivalent to strong complementarity.

Theorem 9.77 Spiders \circ and \bullet are strongly complementary if and only if the basis states of \circ form a subgroup of the phase group of \bullet , and vice versa. Thinking of basis states as classical outcomes (cf. Section 8.1.1), we call this subgroup of a phase group the *classical subgroup*.

Proof Assuming \circ and \bullet are strongly complementary, we show that the \bullet -sum of two \circ -basis states:

$$\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_j \end{array} \quad (9.82)$$

is again a \circ -basis state. Recall from Theorem 8.18 that:

$$\begin{array}{c} \downarrow \\ \triangleleft_\psi \end{array} \in \left\{ \begin{array}{c} \downarrow \\ \triangleleft_i \end{array} \right\}_i \quad \text{if and only if} \quad \begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \triangleleft_\psi \end{array} \stackrel{(*)}{=} \begin{array}{c} \downarrow \\ \triangleleft_\psi \end{array} \begin{array}{c} \downarrow \\ \triangleleft_\psi \end{array}$$

We can show that (9.83) is a \circ -basis state as follows:

$$\begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \bullet \\ \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_j \end{array} \approx \begin{array}{c} \bullet \quad \bullet \\ \swarrow \quad \searrow \quad \swarrow \quad \searrow \\ \circ \quad \circ \\ \swarrow \quad \searrow \quad \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_j \quad \triangleleft_i \quad \triangleleft_j \end{array} = \begin{array}{c} \bullet \quad \bullet \\ \swarrow \quad \searrow \quad \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_i \quad \triangleleft_j \quad \triangleleft_j \end{array} = \begin{array}{c} \bullet \quad \bullet \\ \swarrow \quad \searrow \quad \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_j \quad \triangleleft_i \quad \triangleleft_j \end{array}$$

So the \circ -basis is a finite subset of the phase group closed under the group-sum, and hence by standard group theory, it forms a subgroup.

The proof of the converse mimics the way we motivated the strong complementarity equations using the behaviour of XOR in Section 9.3.1. We repeat the argument here for the general case. Since \circ -basis states form a subgroup of the \bullet -phase group, the \bullet -sum sends every pair of \circ -basis states to another \circ -basis state (up to a number):

$$\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_j \end{array} \approx \begin{array}{c} \downarrow \\ \triangleleft_k \end{array} \quad (9.83)$$

In particular, this means that the \bullet -sum is (up to a number) a function map. So by Proposition 8.19 this implies that:

$$\begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \bullet \\ \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_j \end{array} \approx \begin{array}{c} \bullet \quad \bullet \\ \swarrow \quad \searrow \quad \swarrow \quad \searrow \\ \circ \quad \circ \\ \swarrow \quad \searrow \quad \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_j \quad \triangleleft_i \quad \triangleleft_j \end{array} \quad \begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \bullet \\ \swarrow \quad \searrow \\ \triangleleft_i \quad \triangleleft_j \end{array} \approx \begin{array}{c} \circ \quad \circ \end{array}$$

Finally, any subgroup contains the unit of the group, so the classical subgroup must contain the unit of the \bullet -phase group. Thus, the unit of the grey phase group is a \circ -basis state, and hence:

$$\begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \bullet \end{array} \approx \begin{array}{c} \bullet \quad \bullet \end{array}$$

□

Convention 9.78 We will use Greek letters κ, κ' , etc. to denote phase states that are in the classical subgroup, whereas we stick to $\alpha, \beta, \gamma, \dots$ for general phases. Hence the phase groups and their classical subgroups for the two colours are depicted respectively as:

$$\left\{ \begin{array}{c} \circ \\ \vec{\kappa} \end{array} \right\} \subset \left\{ \begin{array}{c} \circ \\ \vec{\alpha} \end{array} \right\}_{\vec{\alpha}}$$

and:

$$\left\{ \begin{array}{c} \bullet \\ \vec{\kappa} \end{array} \right\} \subset \left\{ \begin{array}{c} \bullet \\ \vec{\alpha} \end{array} \right\}_{\vec{\alpha}}$$

In particular, for a classical phase state the colour always indicates the spider for which it is a phase, as opposed to the colour of the spider that copies it.

From Theorem 9.77, we get another alternative characterisation of strong complementarity: the copiable states of one colour form a subgroup of the phase group of the other colour. Indeed, since basis states and copiable states are one and the same, the following corollary is an immediate result.

Corollary 9.79 For \circ and \bullet strongly complementary, and for:

$$\left\{ \begin{array}{c} \bullet \\ \vec{\kappa} \end{array} \right\}_{\vec{\kappa}} \quad \text{and} \quad \left\{ \begin{array}{c} \circ \\ \vec{\kappa} \end{array} \right\}_{\vec{\kappa}}$$

the basis states for \circ and \bullet , respectively, we have:

$$\begin{array}{c} \circ \\ \bullet \\ \vec{\kappa} \end{array} \approx \begin{array}{c} \bullet \\ \vec{\kappa} \end{array} \begin{array}{c} \bullet \\ \vec{\kappa} \end{array} \quad \begin{array}{c} \bullet \\ \circ \\ \vec{\kappa} \end{array} \approx \begin{array}{c} \circ \\ \vec{\kappa} \end{array} \begin{array}{c} \circ \\ \vec{\kappa} \end{array} \quad (9.84)$$

We call this the κ -copy rule.

Example 9.80 In the particular case of qubits we have:

$$\begin{array}{c} \circ \\ \bullet \\ \pi \end{array} \approx \begin{array}{c} \bullet \\ \pi \end{array} \begin{array}{c} \bullet \\ \pi \end{array} \quad (9.85)$$

This now allows us to give a diagrammatic derivation of the fact that:

$$\begin{array}{c} \circ \quad \bullet \\ \hline \bullet \quad \circ \end{array} \quad (9.86)$$

is indeed the quantum CNOT-gate on \circ basis states. We have:

$$\begin{array}{c} \circ \quad \bullet \\ \hline \bullet \quad \circ \end{array} \approx \begin{array}{c} \bullet \\ \bullet \\ \hline \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \end{array}$$

hence:



So what is:



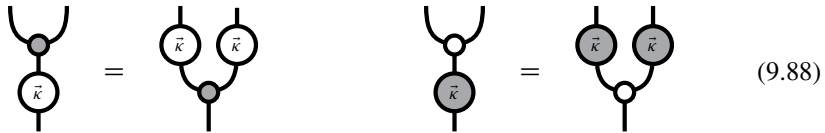
here? Since we have:



it follows that (9.87) is the *quantum NOT-gate* on \circ basis states, and so (9.86) is indeed the quantum CNOT-gate. The same argument with thin wires of course also does the trick for the classical CNOT-gate.

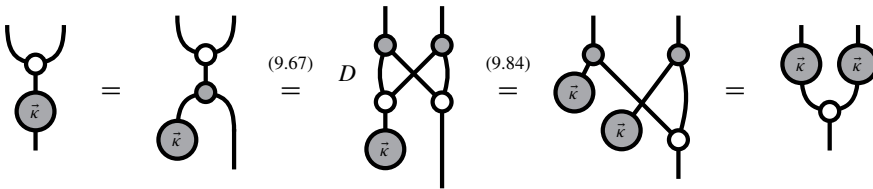
Equation (9.84) involves copy spiders and phase states. We can lift it to one involving copy spiders and phase maps.

Proposition 9.81 For \circ and \bullet strongly complementary, we have:



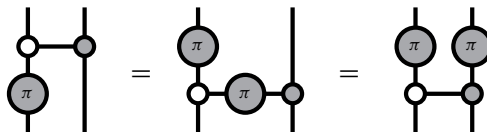
We call this the κ -map-copy rule.

Proof We have:

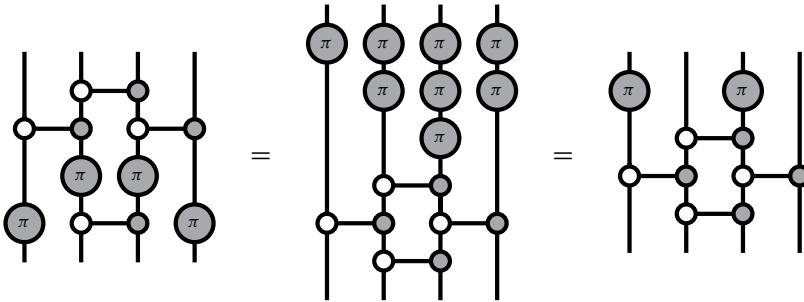


Note that this equation holds on the nose, because the doubled version of (9.67) introduces a factor of D , whereas the on-the-nose counterpart to (9.84) introduces a factor of $1/D$. \square

Example 9.82 By (9.88) a NOT-gate can be pushed past a CNOT-gate:



Hence, in a circuit consisting only of NOT-gates and CNOT-gates, NOT-gates can all be pushed to one end of the circuit:



Equations (9.84) involve undecorated spiders of one colour and phase gates of the other colour. We can transform these into an equation just involving phase gates of two colours.

Proposition 9.83 For \circ and \bullet strongly complementary, we have:

$$\begin{array}{c} \circ \\ \bullet \end{array} = \frac{1}{\sqrt{D}} \begin{array}{cc} \circ & \bullet \\ \bullet & \circ \end{array} \quad (9.89)$$

or equivalently, via doubling:

$$\begin{array}{c} \circ \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \circ \end{array} \quad (9.90)$$

We call this the κ - κ' -commute rule.

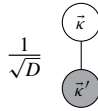
Proof First, note that:

$$\begin{array}{c} \vec{\kappa} \\ \vec{\alpha} \end{array} = \begin{array}{c} \vec{\kappa} \\ \bullet \\ \vec{\alpha} \end{array} \stackrel{(9.84)}{=} \frac{1}{\sqrt{D}} \begin{array}{cc} \vec{\kappa} & \vec{\kappa} \\ \vec{\alpha} & \bullet \end{array} \quad (9.91)$$

We rely on the undoubled version of (9.88), which can easily be shown to hold on the nose (i.e. with no global phase):

$$\begin{array}{c} \vec{\kappa} \\ \vec{\kappa}' \end{array} = \begin{array}{c} \vec{\kappa} \\ \circ \\ \vec{\kappa}' \end{array} \stackrel{(9.88)}{=} \begin{array}{c} \vec{\kappa} \\ \bullet \\ \vec{\kappa}' \end{array} \stackrel{(9.91)}{=} \frac{1}{\sqrt{D}} \begin{array}{cc} \vec{\kappa} & \vec{\kappa} \\ \vec{\kappa}' & \bullet \end{array} = \frac{1}{\sqrt{D}} \begin{array}{c} \vec{\kappa} \\ \vec{\kappa}' \end{array}$$

For the doubled version, we need to show that:



is a global phase, which is indeed the case:

$$\text{double} \left(\frac{1}{\sqrt{D}} \begin{array}{c} \text{white circle } \vec{\kappa} \\ \text{grey circle } \vec{\kappa}' \end{array} \right) = \frac{1}{D} \begin{array}{c} \text{white circle } \vec{\kappa} \\ \text{grey circle } \vec{\kappa}' \end{array} \stackrel{(9.40, 9.42)}{=} D \begin{array}{c} \text{triangle } j \\ \text{triangle } i \end{array} \stackrel{(9.38)}{=} \boxed{\phantom{\rule{1cm}{1cm}}}$$

□

Exercise 9.84 Show that (9.64), (9.84), (9.88), (9.90), and (9.92) are all equivalent. (Hint and warning: for some of the proofs one will need to rely on the fact that when two maps agree on a basis, then they are equal. But, as explained in Remark 5.11, in this case numbers do matter!)

Corollary 9.85 Each of the equations (9.84), (9.88), (9.90), and (9.92) – when paired with the equations in (9.65) – provides an alternative definition for strong complementarity.

Remark* 9.86 Note that we chose to include equation (9.89) in undoubled form, which includes a non-trivial complex phase. The fact that the phase maps in (9.89) only commute up to a phase is a version of the *canonical commutation relations* (the *Weyl relations*, to be precise). The canonical commutation relations were the first tool that physicists used to probe complementarity in quantum theory.

In the proof of Proposition 9.83 we discovered another consequence of strong complementarity, namely that phase states in the classical subgroup are ‘immune’ to phase states of the other colour.

Proposition 9.87 For \circ and \bullet strongly complementary, we have:

$$\begin{array}{c} \text{white circle } \vec{\alpha} \\ \text{grey circle } \vec{\kappa} \end{array} = \text{white circle } \vec{\kappa} \qquad \begin{array}{c} \text{white circle } \vec{\alpha} \\ \text{grey circle } \vec{\kappa} \end{array} = \text{grey circle } \vec{\kappa} \qquad (9.92)$$

We call this the κ -eliminate rule.

Proof Simply double and reflect equation (9.91). □

Proposition 9.83 has a big brother, too, which states that phase maps in the classical subgroup can pass by phases of the other colour.

Exercise 9.88 Show that for \circ and \bullet strongly complementary, we have:

$$\begin{array}{c} \circlearrowleft \\ \vec{\alpha} \\ \circlearrowleft \\ \vec{\kappa} \end{array} = \begin{array}{c} \circlearrowleft \\ \vec{\kappa} \\ \circlearrowleft \\ \vec{\kappa}(\vec{\alpha}) \end{array} \quad \begin{array}{c} \circlearrowleft \\ \vec{\alpha} \\ \circlearrowleft \\ \vec{\kappa} \end{array} = \begin{array}{c} \circlearrowleft \\ \vec{\kappa} \\ \circlearrowleft \\ \vec{\kappa}(\vec{\alpha}) \end{array} \quad (9.93)$$

where:

$$\begin{array}{c} \circlearrowleft \\ \vec{\kappa}(\vec{\alpha}) \end{array} := \begin{array}{c} \circlearrowleft \\ \vec{\kappa} \\ \circlearrowleft \\ \vec{\alpha} \end{array} \quad \begin{array}{c} \circlearrowleft \\ \vec{\kappa}(\vec{\alpha}) \end{array} := \begin{array}{c} \circlearrowleft \\ \vec{\kappa} \\ \circlearrowleft \\ \vec{\alpha} \end{array}$$

are phase states for \bullet and \circ , respectively (as the notation suggests).

Exercise 9.89 For \circ and \bullet strongly complementary, show that for any $\vec{\kappa}$, the function $\vec{\kappa}(-)$ defined in Exercise 9.88 is a *group homomorphism*, i.e.:

$$\begin{array}{c} \circlearrowleft \\ \vec{\kappa}(\vec{\alpha} + \vec{\beta}) \end{array} = \begin{array}{c} \circlearrowleft \\ \vec{\kappa}(\vec{\alpha}) + \vec{\kappa}(\vec{\beta}) \end{array} \quad \begin{array}{c} \circlearrowleft \\ \vec{\kappa}(\vec{0}) \end{array} = \begin{array}{c} \circlearrowleft \\ \vec{0} \end{array}$$

Furthermore, show that the map:

$$\vec{\kappa} \mapsto \vec{\kappa}(-)$$

is a *group action*, i.e.:

$$\begin{array}{c} \circlearrowleft \\ \vec{\kappa} + \vec{\kappa}'(\vec{\alpha}) \end{array} = \begin{array}{c} \circlearrowleft \\ \vec{\kappa}(\vec{\kappa}'(\vec{\alpha})) \end{array} \quad \begin{array}{c} \circlearrowleft \\ \vec{0}(\vec{\alpha}) \end{array} = \begin{array}{c} \circlearrowleft \\ \vec{\alpha} \end{array}$$

Example 9.90 In the case of two dimensions, the classical subgroup has two elements, 0 and π . From Exercise 9.89, we know 0 acts trivially. We saw in Section 9.3.4 that π acts as a NOT-gate for \circ -basis elements:

$$\begin{array}{c} \bullet \\ \pi \end{array} :: \begin{array}{c} \triangle \\ 0 \end{array} \mapsto \begin{array}{c} \triangle \\ 1 \end{array}, \begin{array}{c} \triangle \\ 1 \end{array} \mapsto \begin{array}{c} \triangle \\ 0 \end{array}$$

Hence, for \circ -phase states:

$$\begin{array}{c} \bullet \\ \pi \end{array} :: \begin{pmatrix} 1 \\ e^{i\alpha} \end{pmatrix} \mapsto \begin{pmatrix} e^{i\alpha} \\ 1 \end{pmatrix} = e^{i\alpha} \begin{pmatrix} 1 \\ e^{-i\alpha} \end{pmatrix}$$

Thus, after doubling, π flips the phase, i.e.:

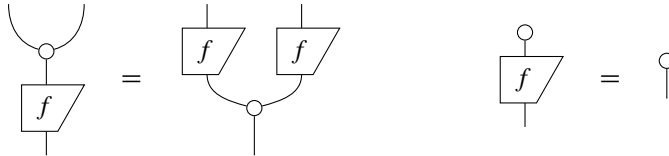
$$\begin{array}{c} \bullet \\ \pi \\ \circlearrowleft \\ \alpha \end{array} = \begin{array}{c} \circlearrowleft \\ -\alpha \end{array} \quad \begin{array}{c} \circlearrowleft \\ \pi \\ \bullet \\ \alpha \end{array} = \begin{array}{c} \bullet \\ -\alpha \end{array} \quad (9.94)$$

where the second equation comes from interchanging the roles of \circ and \bullet .

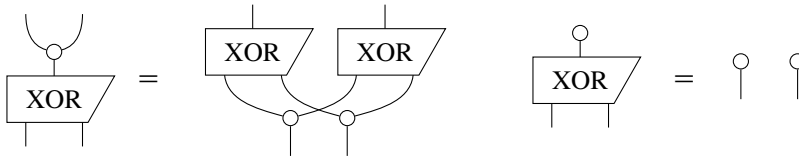
9.3.5 Parity Maps from Spiders

Spiders were initially introduced in the previous chapter as classical data operations. We will see in this section that strong complementarity gives us many more classical data operations.

In Proposition 8.19 we encountered a characterisation of function maps as linear maps f satisfying:



In Section 9.3.1 we used these equations to motivate strong complementarity equations when taking f to be XOR:



which arises (up to a number) as an X -spider (cf. Proposition 5.88). It is easily seen that this connection to function maps applies for any strongly complementary pair of spiders.

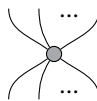
Proposition 9.91 For \circ and \bullet strongly complementary:



is a function map (up to a number) for \circ .

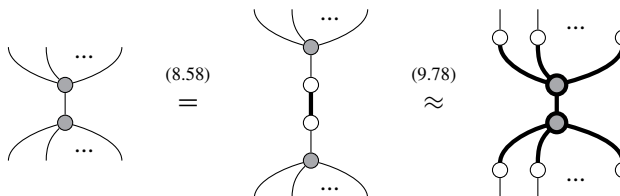
In fact, recalling that function maps are particular examples of the more general classical maps (cf Section 8.2.1), the previous proposition generalises to all \bullet -spiders.

Proposition 9.92 For \circ and \bullet strongly complementary:



is a classical process (up to a number) for \circ .

Proof We have:



The rightmost diagram consists just of \circ -measure, \circ -encode, and pure quantum maps, so by Definition 8.3, it is a cq-map, and in particular it is a classical map (i.e. a cq-map with no quantum inputs/outputs). Hence the \bullet -spider is equal up to a number to a cq-map. Since this number is positive (cf. Remark 9.36) the \bullet -spider is itself a cq-map. Causality follows from the ‘generalised copying’ equation for strongly complementary spiders:

$$\begin{array}{c} \circ \quad \circ \quad \circ \\ \vdots \\ \bullet \\ \vdots \\ \circ \quad \circ \quad \circ \end{array} = \begin{array}{c} \circ \\ \vdots \\ \bullet \\ \vdots \\ \circ \quad \circ \quad \circ \end{array} \quad (9.77) \quad \approx \quad \begin{array}{c} \circ \quad \circ \quad \circ \\ \vdots \\ \circ \quad \circ \quad \circ \end{array} \approx \begin{array}{c} \circ \quad \circ \quad \circ \\ \vdots \\ \circ \quad \circ \quad \circ \end{array}$$

□

We can get a better idea of what these new classical processes do by looking at what they do on basis states and effects in two dimensions. For this it is helpful to treat basis states/effects as elements in the classical subgroup:

$$\begin{array}{c} \downarrow \\ i \end{array} \approx \begin{array}{c} \bullet \\ \kappa \end{array} \quad \begin{array}{c} \uparrow \\ i \end{array} \approx \begin{array}{c} \bullet \\ \kappa \end{array}$$

for $\kappa \in \{0, \pi\}$, so:

$$\begin{array}{c} \triangle_{i'_1} \quad \triangle_{i'_2} \quad \dots \quad \triangle_{i'_n} \\ \vdots \\ \bullet \\ \vdots \\ \triangle_{i_1} \quad \triangle_{i_2} \quad \dots \quad \triangle_{i_m} \end{array} \approx \begin{array}{c} \bullet_{\kappa'_1} \quad \bullet_{\kappa'_2} \quad \dots \quad \bullet_{\kappa'_n} \\ \vdots \\ \bullet \\ \vdots \\ \bullet_{\kappa_1} \quad \bullet_{\kappa_2} \quad \dots \quad \bullet_{\kappa_m} \end{array} = \begin{array}{c} \sum \kappa_i + \sum \kappa'_i \end{array} \quad (9.95)$$

In order to figure out which of these are non-zero, we need to know which ‘phase numbers’ (i.e. phase spiders with no legs) taken from the classical subgroup are non-zero.

Lemma 9.93 For \circ and \bullet strongly complementary:

$$\begin{array}{c} \bullet \\ \kappa \end{array} \neq 0 \iff \kappa = 0$$

where the first 0 stands for the zero number while the second 0 stands for the unit of the phase group.

Proof Let the (classical) \bullet -phase state with phase 0 be equal, up to a number, to the first \circ -ONB state (which is also labelled ‘0’ below). Then we have:

$$\begin{array}{c} \bullet \\ \kappa \end{array} = \begin{array}{c} \bullet \\ \kappa \\ \bullet \end{array} \approx \begin{array}{c} \triangle \\ i \\ \downarrow \\ \triangle \\ 0 \end{array}$$

By orthonormality this number is only non-zero if $i = 0$, i.e. $\kappa = 0$.

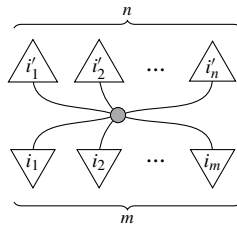
□

So, a matrix entry is non-zero if and only if we have:

$$\sum_i \kappa_i + \sum_i \kappa'_i = 0$$

In that case, it is equal to a fixed positive number p .

Exercise 9.94 What is the value of p , i.e. the number:



in terms of m and n ?

For two dimensions, the classical subgroup is \mathbb{Z}_2 (cf. Example 9.76). In that case, the group-sum is equal to 0 if and only if there are an even number of 1s, so:

$$\text{Spider} \approx \sum_{i_1 \dots i_m i'_1 \dots i'_n} \oplus (i_1 \dots i_m i'_1 \dots i'_n) \quad \begin{array}{c} \downarrow i'_1 \quad \dots \quad \downarrow i'_n \\ \uparrow i_1 \quad \dots \quad \uparrow i_m \end{array}$$

where \oplus is the *even-parity function*, i.e.:

$$\oplus(i_1 \dots i_m i'_1 \dots i'_n) := \begin{cases} 1 & \text{if number of 1s is even} \\ 0 & \text{if number of 1s is odd} \end{cases}$$

So only those terms with an even number of 1-states occur in the sum. One example is the *even-parity state*:

$$\text{Even-parity state diagram} \quad (9.96)$$

Another example of this is the *parity map*, which returns the 0-state if the number of 1-states is even, and the 1-state if it is odd:

$$\text{Parity map diagram} \quad (9.97)$$

If we decorate \bullet -spiders with a π , the parity is reversed, so we obtain:

$$\text{Decorated Spider} \approx \sum_{i_1 \dots i_m i'_1 \dots i'_n} \overline{\oplus} (i_1 \dots i_m i'_1 \dots i'_n) \quad \begin{array}{c} \downarrow i'_1 \quad \dots \quad \downarrow i'_n \\ \uparrow i_1 \quad \dots \quad \uparrow i_m \end{array}$$

where $\overline{\oplus}$ is the *odd-parity function*, i.e.:

$$\overline{\oplus}(i_1 \dots i_m i'_1 \dots i'_n) := \begin{cases} 1 & \text{if number of 1s is odd} \\ 0 & \text{if number of 1s is even} \end{cases}$$

The (classical) NOT-gate is a special case:

$$\pi = \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} + \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array}$$

since each term has precisely one 1. Another example is the *odd-parity state*:

$$\begin{array}{c} \text{...} \\ \downarrow \\ \pi \end{array} \quad (9.98)$$

Example 9.95 In the case of three systems we have:

$$\begin{array}{c} \downarrow \\ \pi \end{array} \approx \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} + \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} + \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} + \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array}$$

$$\begin{array}{c} \downarrow \\ \pi \end{array} \approx \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} + \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} + \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} + \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array}$$

These two special cases, along with the three-system parity function:

$$\begin{array}{c} \downarrow \\ \pi \end{array} :: \left\{ \begin{array}{l} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \mapsto \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \\ \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{0} \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \mapsto \begin{array}{c} \downarrow \\ \text{1} \\ \downarrow \end{array} \end{array} \right.$$

will play an important role in derivation of quantum non-locality.

In addition to the new classical maps we can build out of \bullet -spiders, we can now build even more by combining \circ -spiders and \bullet -spiders, for example, the classical CNOT-gate:



9.3.6 Classifying Strong Complementarity

In Example 9.44 we stressed how little is actually known about classifying complementary measurements. In fact establishing how many pairwise complementary measurements there are just in dimension 6 remains an open question (or, more accurately, a black hole that sucks in quantum information scientists).

So what about strong complementarity? What do we actually know? The answer is as satisfying as it ever gets: everything! We already know from Section 9.3.2 that sets of pairwise strongly complementary spiders are always of size 2. Hence, it only remains to classify these pairs. Since strong complementarity is really about the relationship between

two families of spiders, we can furthermore assume that one of the families is fixed. Hence, classifying strongly complementary pairs amounts to answering the following question:

For a fixed family of spiders \bigcirc , can we classify all spiders \bullet that are strongly complementary to \bigcirc ?

To attack this question, we should think about how much data we need to uniquely fix \bullet . But in fact, we have already answered this question! In (9.95), we saw that the \bullet -spiders, considered as parity maps, are all entirely fixed by the group-sum, which in the case of \mathbb{Z}_2 is XOR (hence ‘parity’). Furthermore, for any commutative group G of size D , we can fix a D -dimensional system and label the \bigcirc -basis states by elements $g \in G$:

$$\left\{ \begin{array}{c} \downarrow \\ \triangle \\ g \end{array} \right\}_{g \in G}$$

Then, the *generalised parity maps*:

$$\begin{array}{c} \triangle_{g'_1} \quad \triangle_{g'_2} \quad \dots \quad \triangle_{g'_n} \\ \quad \quad \quad \bullet \\ \triangle_{g_1} \quad \triangle_{g_2} \quad \dots \quad \triangle_{g_m} \end{array} := \begin{cases} \left(\frac{1}{\sqrt{D}}\right)^{m+n-2} & \text{if } \sum g_j = \sum g'_j \\ 0 & \text{otherwise} \end{cases} \quad (9.99)$$

(where ‘ \sum ’ is the group-sum from G) yield a family of spiders. Furthermore, \bigcirc and \bullet will always be strongly complementary! Hence:

Strongly complementary pairs of spiders are classified by commutative groups.

So, why did we say we ‘know everything’ about classifying strongly complementary spiders? Well, because we know everything about classifying finite commutative groups, of course!

The simplest commutative groups are *cyclic groups* \mathbb{Z}_k , whose elements are $\{0, \dots, k-1\}$, with group-sum given by addition modulo k . Then every other finite commutative group can be expressed uniquely (up to isomorphism) as a product of cyclic groups:

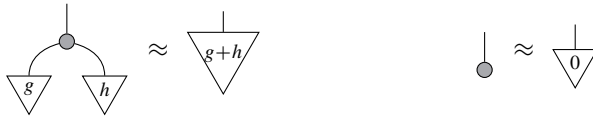
$$\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \dots \times \mathbb{Z}_{k_n}$$

where each $k_i = p_i^{n_i}$ for some prime number p_i and some integer n_i ; i.e. each of the k_i are *prime powers*. Using this characterisation, we know exactly how to build all of the strongly complementary pairs in every dimension.

Example 9.96 In dimension 2, there is only the Z/X pair, which corresponds to the ‘parity’ cyclic group \mathbb{Z}_2 , whereas in dimension 36, there are four different strongly complementary pairs, corresponding to each of the ways to factor 36 into prime powers:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \quad \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \quad \mathbb{Z}_4 \times \mathbb{Z}_9$$

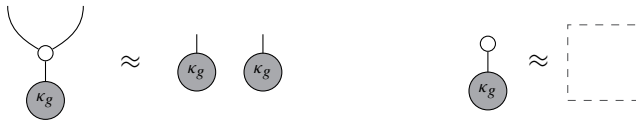
Okay, great, strongly complementary pairs are totally classified. Is this useful? Yes! Equation (9.99) implies in particular that:



where $g + h$ and 0 are the group-sum and unit in G , respectively. Hence G arises as the classical subgroup associated with the strongly complementary pair \circ/\bullet . That is, we have a set of \bullet -phases:

$$\left\{ \begin{array}{c} | \\ \triangle \\ g \end{array} \right\}_{g \in G} \cong \left\{ \begin{array}{c} | \\ \bullet \\ \kappa_g \end{array} \right\}_{g \in G}$$

which is classical for \circ (up to a number):



and encodes G via \bullet :

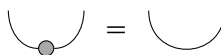


And since strong complementarity is symmetric with respect to \circ/\bullet , we also get an encoding of G in the classical subgroup of \circ -phases:



So we can totally encode this group (in two ways) using a strongly complementary pair of spiders. Now, if we want to study this group (or, better, build some quantum processes that study the group for us!), we can use this pair of spiders. This is in fact precisely what we'll do in Section 12.2.4, when we provide a quantum algorithm for solving the *hidden subgroup problem*.

Remark 9.97 A careful reader might have noticed from the definition of \bullet in (9.99) that the usual spider equation:



implies that $g = -g$ for all $g \in G$! This of course does not hold for all commutative groups, but holds only for those of the form:

$$\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_N$$

When $g \neq -g$, we still get spiders, but not necessarily ones corresponding to self-conjugate ONBs (cf. Section* 8.6.3). In this case, the linear map:

$$\begin{array}{|c} \hline \diagup \\ \hline \end{array} := \begin{array}{c} \bullet \\ \text{---} \\ \circ \end{array}$$

will be equal not to the plan wire, but rather to the function map that sends each group element to its inverse. This is discussed in detail in Section* 9.6.1.

9.4 ZX-Calculus

In this section, we will specialise the diagrammatic creatures and their interactions developed earlier in this chapter to the particular case of qubits. The two relevant questions in this context are the following:

1. Which cq-maps can we express using just phase Z- and X-spiders? In particular, can we express all of them?
2. Which equations between cq-maps can we prove using a *graphical calculus*, i.e. a fixed set of diagrammatic equations, picked from those we've already seen and maybe some new ones?

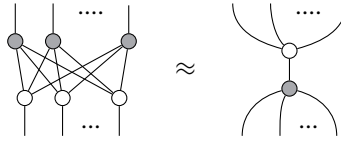
The answer to the first question is a resounding Yes! More specifically, we can build any linear map from m copies of \mathbb{C}^2 to n copies of \mathbb{C}^2 just using phase Z- and X-spiders. Hence, in particular, we can build any quantum map on qubits just by doubling, and, since we have spiders around, we can also build any cq-map on bits and qubits.

The answer to the second question, somewhat embarrassingly, is that we aren't really sure yet. But then again, it turns out to be an extremely hard question. However, if we restrict our phases to multiples of $\frac{\pi}{2}$, we obtain an important subtheory of **pure quantum maps** called **Clifford maps**. As we will show in Chapter (11), this subtheory of **Clifford maps** already provides enough quantum maps to prove that quantum theory is non-local.

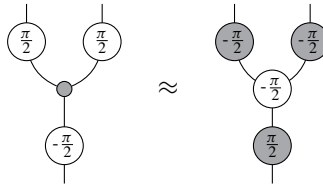
For this process theory just four equations (or technically, four families of equations) are sufficient to prove everything! The first two equations tell us how spiders of the same colour combine. These are of course just the (undoubled) spider-fusion rules we are now very familiar with:

$$\begin{array}{c} \dots \\ \dots \\ \alpha \\ \dots \\ \beta \\ \dots \\ \dots \end{array} = \begin{array}{c} \dots \\ \dots \\ \alpha + \beta \\ \dots \\ \dots \end{array} \quad \begin{array}{c} \dots \\ \dots \\ \alpha \\ \dots \\ \beta \\ \dots \\ \dots \end{array} = \begin{array}{c} \dots \\ \dots \\ \alpha + \beta \\ \dots \\ \dots \end{array}$$

The third equation tells us how spiders of different colours can commute past each other:



which via Theorem 9.71 is equivalent to strong complementarity. The fourth equation is new. It tells us how to convert spiders of one colour into spiders of the other colour:



While the other equations are generic to strongly complementary pairs in any dimension, this equation is really saying something special about qubits. Indeed, we will see in the next section that this rule is intimately connected to the geometry of the Bloch sphere.

Interestingly, the keys to answering both of the questions above, which are all about quantum picturalism, come from the literature on quantum computation! Indeed, the first question turns out to be related to the quantum gate sets required to build a universal computing device, while for the second question the proof of completeness draws from results in measurement-based quantum computation.

Remark 9.98 We are working almost exclusively with single wires in this section. This gives us our most general-purpose rules, as special cases involving quantum and bastard spiders can all be obtained by folding/unfolding quantum wires. Therefore, we will regularly use undoubled versions (thanks to Corollary 6.18) of some of the doubled equations that we established earlier in this chapter. Note that, when there can be no confusion, we still refer to the single wires resulting from undoubling as qubits.

9.4.1 ZX-Diagrams Are Universal

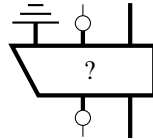
In specialising to qubits, we define a new type of diagram.

Definition 9.99 A *ZX-diagram* is a string diagram consisting of just phase Z- and X-spiders:

$$\begin{array}{c} \text{X-spider with } \alpha \end{array} := \begin{array}{c} \text{Z-spider with } 0 \end{array} \dots \begin{array}{c} \text{Z-spider with } 0 \end{array} + e^{i\alpha} \begin{array}{c} \text{X-spider with } 1 \end{array} \dots \begin{array}{c} \text{X-spider with } 1 \end{array} \quad (9.100)$$

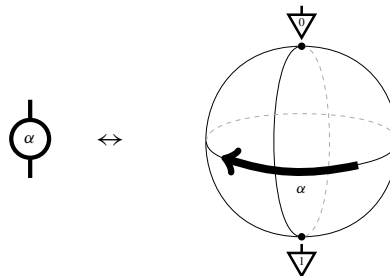
$$\begin{array}{c} \text{...} \\ \diagup \quad \diagdown \\ \text{...} \end{array} \quad \alpha \quad \begin{array}{c} \text{...} \\ \diagdown \quad \diagup \\ \text{...} \end{array} := \begin{array}{c} \downarrow 0 \quad \dots \quad \downarrow 0 \\ \uparrow 0 \quad \dots \quad \uparrow 0 \end{array} + e^{i\alpha} \begin{array}{c} \downarrow 1 \quad \dots \quad \downarrow 1 \\ \uparrow 1 \quad \dots \quad \uparrow 1 \end{array} \quad (9.101)$$

So for ZX-diagrams, we don't allow arbitrary processes, but rather just those built out of these two kinds of phase spiders. However, rather than thinking of this as removing all of the other boxes from our language, we can instead think of this as 'filling in the boxes':

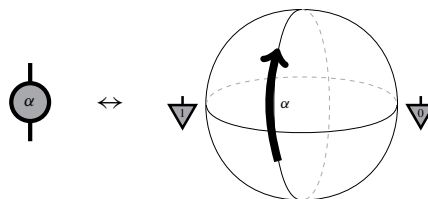


ZX-diagrams are significantly more expressive than plain string diagrams or dot diagrams, given that we have phases and two colours of spiders. In this section, we will see that this actually suffices to build any pure quantum map from qubits to qubits. If we additionally add discarding or (more generally) bastard spiders, we can build, respectively, any quantum map or any cq-map on (qu)bits.

First we show how ZX-diagrams can be used to construct arbitrary single-qubit unitaries. Recall that qubit unitaries correspond to rotations of the Bloch sphere. We already have two quite useful families of rotations: the Z-phase gates, which provide Z-axis rotations:

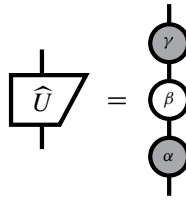


and the X-phase gates, which provide X-axis rotations:



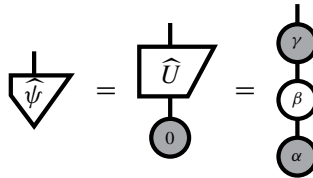
In fact, it is a standard property about spheres that any rotation can be decomposed as three rotations about a pair of orthogonal axes. Applying this to unitary quantum maps yields the following result.

Proposition 9.100 For any unitary quantum map \widehat{U} on a single qubit there exist phases α , β , and γ such that \widehat{U} can be written as:



This is called the *Euler decomposition* of \widehat{U} , and the phases α , β , and γ are called the *Euler angles*.

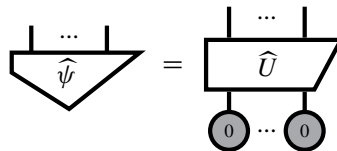
Since we can perform any unitary, it is possible to obtain any single-qubit state by just starting with some fixed state and transforming it into the state $\widehat{\psi}$ we want, now expressed as a ZX-diagram, e.g.:



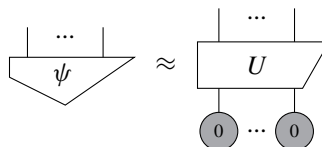
By undoubling, we can see that any state in **linear maps** of type \mathbb{C}^2 can be expressed, up to a number (namely, a global phase), as a ZX-diagram. In fact, this generalises to many-qubit states.

Proposition 9.101 Any state in **linear maps** on n copies of \mathbb{C}^2 can be expressed, up to a number, as a ZX-diagram.

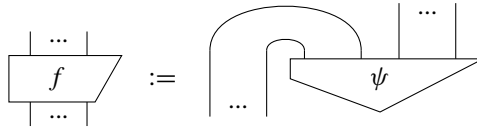
We will hold off on proving this theorem until Section 12.1.3 in the chapter on quantum computing, where we will borrow some results from the quantum circuits literature. More specifically, in Section 12.1.3 we will show that ZX-diagrams can be used to construct any unitary \widehat{U} on n qubits, and just like above, we can use this fact to obtain any n -qubit quantum state:



Undoubling this gives us any state, up to a number (cf. Corollary 6.18):

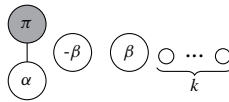


Then, just by applying process–state duality to Proposition 9.101, we can also construct any linear map whose input/output wires all are of type \mathbb{C}^2 :



Clearly if ψ is a ZX-diagram, then so too is f . Moreover, we can get all of the complex numbers back as ZX-diagrams.

Proposition 9.102 Any complex number can be expressed as a ZX-diagram of the form:



for some α , β , and k .

Proof First, note that we can obtain $\sqrt{2}$ times any complex phase via:

$$\begin{array}{c} \pi \\ \circ \\ \alpha \end{array} \stackrel{(9.46)}{=} \sqrt{2} \begin{array}{c} 1 \\ \triangle \\ \alpha \end{array} \stackrel{(9.11)}{=} \sqrt{2} e^{i\alpha}$$

So, it suffices to show that we can express any positive real number. First:

$$\begin{array}{c} (-\beta) \\ \circ \end{array} \begin{array}{c} \beta \\ \circ \end{array} \stackrel{(9.100)}{=} (1 + e^{i\beta})(1 + e^{-i\beta}) = 1 + e^{i\beta} + e^{-i\beta} + 1$$

Using the fact that $e^{i\beta} = \cos \beta + i \sin \beta$ (cf. Section 5.3.1), this reduces to:

$$\begin{array}{c} (-\beta) \\ \circ \end{array} \begin{array}{c} \beta \\ \circ \end{array} = 2(1 + \cos \beta)$$

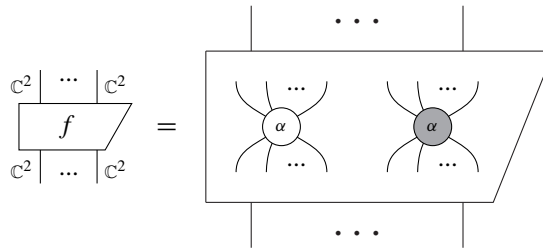
which can be any real number between 0 and 2. To get larger numbers, we simply need to add more dots:

$$\begin{array}{c} (-\beta) \\ \circ \end{array} \begin{array}{c} \beta \\ \circ \end{array} \underbrace{\circ \dots \circ}_k = 2^{k+1}(1 + \cos \beta)$$

Thus, for any positive real number r , we can fix some k such that $2^{k+1} \geq r$, then choose β accordingly. \square

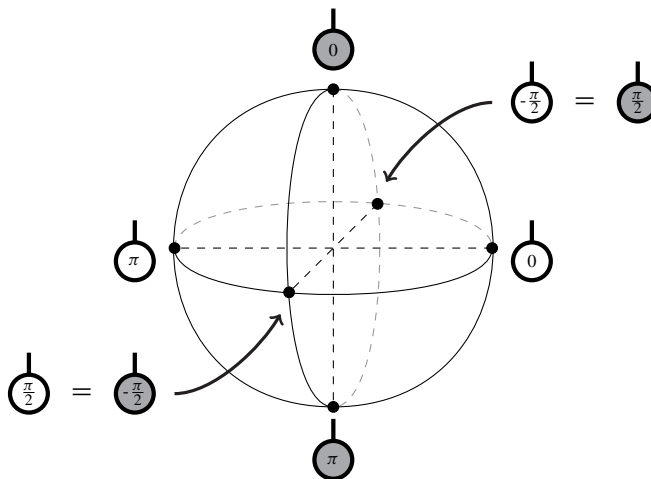
Hence we can conclude the following.

Theorem 9.103 Any linear map whose input/output wires all are of type \mathbb{C}^2 can be expressed as a ZX-diagram:



9.4.2 ZX-Calculus for Clifford Diagrams

Instead of considering the entire qubit, we can also construct lots of interesting states and processes (indeed most of those we've encountered so far!) by restricting to just six representative states on the Bloch sphere, namely, the Z-, X-, and Y-basis states, which correspond to the following phase states:



The phase groups are therefore also reduced to the four-element subgroup \mathbb{Z}_4 of $U(1)$:



Note that each of these states is representable as a Z- or X-phase state whose phase is a multiple of $\frac{\pi}{2}$. We can of course consider all such ZX-diagrams.

Definition 9.104 A *Clifford diagram* is a ZX-diagram where the phases are restricted to integer multiples of $\frac{\pi}{2}$.

In turn, these diagrams define a new process theory.

Definition 9.105 Let **Clifford maps**, be the subtheory of **pure quantum maps** obtained by doubling those linear maps that are expressible as Clifford diagrams.

As we claimed before, Clifford diagrams admit a graphical calculus for which **Clifford maps** are complete; that is, there exists a set of equations such that, whenever two Clifford maps are equal (up to a number), we can apply the equations of the graphical calculus to rewrite the diagram of one into the other.

In fact, the phase spider-fusion rules and strong complementarity already get us most of the way there. However, they cannot get us all the way there, since these rules are generic for all quantum systems, not just qubits. Hence, there has to be at least one more rule that clearly tells us that we are dealing with qubits. This final missing ingredient comes from the fact that, even though we only have Z-spiders and X-spiders in a ZX-diagram, somehow the Y-basis, and hence Y-spiders, are also hiding in there as well, by means of phases. Is there any way we can bring them out?

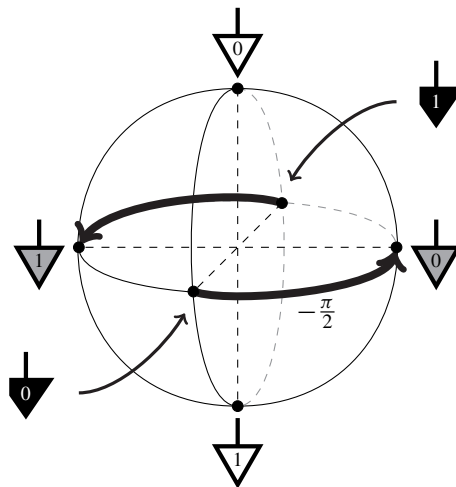
It turns out that just thinking about how to build a Y-copy spider will be enough to unlock the full power of the ZX-calculus for Clifford diagrams. In single form, the Y-basis can be written as follows:

$$\left\{ \begin{array}{l} \sqrt{2} \begin{array}{c} \downarrow \\ \text{0} \end{array} = \begin{array}{c} \circlearrowleft \\ \frac{\pi}{2} \end{array} = e^{i\frac{\pi}{4}} \begin{array}{c} \text{shaded circle} \\ -\frac{\pi}{2} \end{array} \\ \sqrt{2} \begin{array}{c} \downarrow \\ \text{1} \end{array} = \begin{array}{c} \circlearrowleft \\ -\frac{\pi}{2} \end{array} = e^{-i\frac{\pi}{4}} \begin{array}{c} \text{shaded circle} \\ \frac{\pi}{2} \end{array} \end{array} \right. \quad (9.102)$$

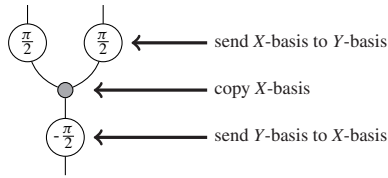
(We include the complex phases explicitly, as they'll play a role shortly.)

Exercise 9.106 Using the concrete definitions of the Y-basis and the phase Z- and X-spiders, prove the equations in (9.102) and, in particular, the complex phases are as shown.

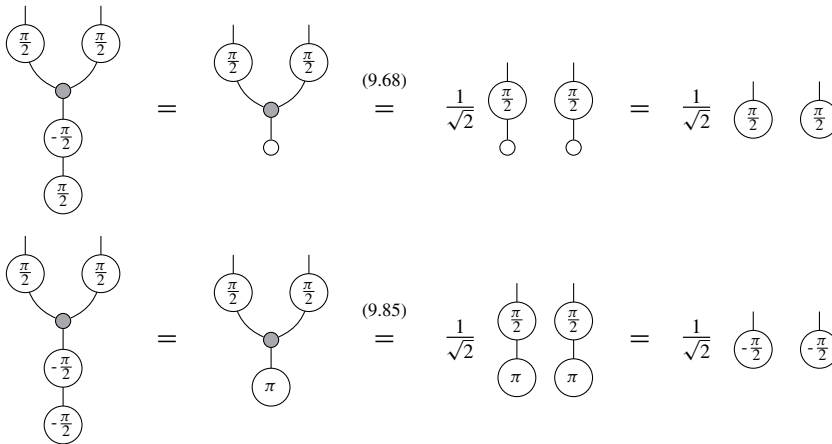
The two ways of expressing the Y-basis tell us two ways to copy it. First, a $-\frac{\pi}{2}$ rotation around the Z-axis will send the Y-basis to the X-basis:



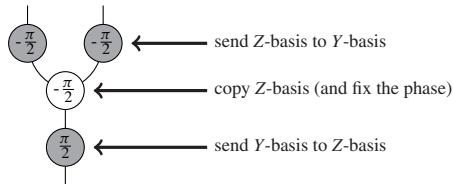
And a $\frac{\pi}{2}$ rotation will of course send the X -basis back to the Y -basis. Hence, one way to copy the Y -basis is:



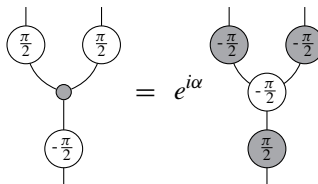
We can see this copying in action by plugging in the two Y -basis states, written as \bigcirc -phase states according to (9.102):



We can almost do the analogous thing with the colours reversed for \bullet -phases, but we need to correct the difference in the phases between the two ONB states. From (9.102), we can see these phases are $e^{i\frac{\pi}{4}}$ and $e^{-i\frac{\pi}{4}}$, respectively, so the overall difference is $\frac{\pi}{2}$. We can account for this by incorporating a $-\frac{\pi}{2}$ phase into the \bigcirc -spider:

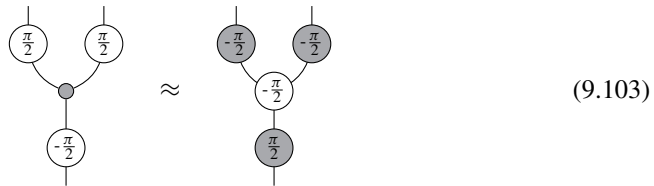


Exercise 9.107 Prove by evaluating on Y -basis states that:

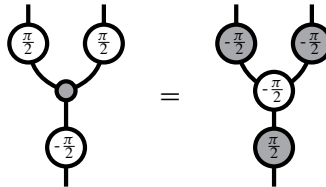


for some fixed global phase $e^{i\alpha}$.

Hence:

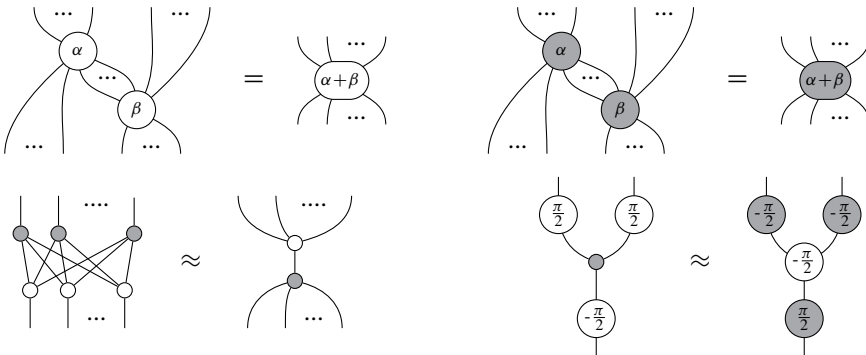


or, more accurately (since the LHS and RHS differ only by a global phase):

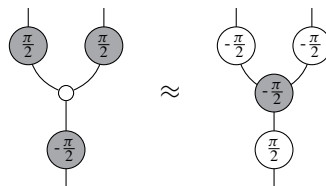


Adding this *Y-rule* to what we already know about strongly complementary pairs of spiders yields the following definition.

Definition 9.108 The *ZX-calculus for Clifford diagrams* consists of the following four rules:



A first thing that may surprise some readers is the fact that the fourth rule, in contrast to all of the other rules we have encountered so far, is not symmetric in \circ and \bullet . This asymmetry is only an artefact of going for a minimal set of rules, and in the following section we will show that the ZX-calculus is indeed colour-symmetric. That is, any rule we prove can also be proven with the colours reversed. Clearly, the colour-reverse of the first three rules holds, so this is equivalent to showing that the colour-reverse of the *Y-rule*:




holds in the ZX-calculus.

Of course, from the previous sections we already know many other things about ZX-calculus. For example, since the third rule is equivalent to strong complementarity via Theorem 9.71, we know that the initial strong complementarity equations follow:

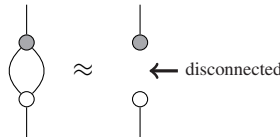


$$(9.104)$$



$$(9.105)$$

as well as the complementarity equation:



$$(9.106)$$

These special cases also show explicitly that the ZX-calculus contains some equations that make diagrams disconnect. These equations are the most important ones, because ZX-diagrams, like all of the simpler kinds of diagrams we encountered before, are still most fundamentally about ‘what is connected to what’.

As with strong complementarity, there isn’t just one way to define the ZX-calculus, but many equivalent ways. In Section 9.4.4 below we will build a version of ZX-calculus with a substantially different fourth rule. In fact, the version we presented above has never been given before. However, it is to our knowledge the smallest possible set of rules. Moreover, it is very easy to remember, since each of the rules tells us one particular thing about spiders, namely:

- how spiders of the same colour combine
- how spiders of different colours can commute past each other
- how to convert spiders of one colour into another.

In Section 9.3.4, we derived a number of rules involving phases in the classical subgroup, which in the case of qubits are 0 and π . When we first derived those rules we took as given, simply by staring at the Bloch sphere, that π -phase states for one colour are basis states for the other colour (up to a number). However, to stay true to our conviction to use only the graphical calculus to prove everything, we should really derive these just using the four defining rules of ZX-calculus. This is indeed possible, as we will demonstrate in the next section.

In addition to the ‘big four’ rules of the ZX-calculus, we also need a few little rules for eliminating non-zero numbers:

$$\circ = \bullet = \begin{array}{c} \circ \\ | \\ \bullet \\ \alpha \end{array} = \begin{array}{c} \bullet \\ | \\ \circ \\ \alpha \end{array} \approx \square \quad (9.107)$$

Using a technique similar to Exercise 9.62, we can indeed show that these numbers cannot be zero, unless every spider is already zero.

9.4.3 ZX for Dodos: Just Diagrams, Nothing Else

Now that we have fixed the ZX-calculus, our goal is to prove everything in the rest of this chapter just using those rules and nothing else. This will give a clear idea of what the ZX-calculus looks like ‘in action’. First, we’ll start with a little warmup.

Proposition 9.109 The ZX-calculus obeys:

$$\begin{array}{c} \circ \\ | \\ \bullet \\ \alpha \end{array} \approx \begin{array}{c} \circ \\ | \end{array} \quad \begin{array}{c} \bullet \\ | \\ \circ \\ \alpha \end{array} \approx \begin{array}{c} \bullet \\ | \end{array} \quad (9.108)$$

Proof The proof goes mostly just like (9.91), with a little ‘non-zero’ rule at the end:

$$\begin{array}{c} \circ \\ | \\ \bullet \\ \alpha \end{array} = \begin{array}{c} \circ \\ | \\ \bullet \\ \alpha \end{array} \begin{array}{c} \circ \\ | \end{array} \stackrel{(9.105)}{\approx} \begin{array}{c} \circ \\ | \\ \bullet \\ \alpha \end{array} \begin{array}{c} \circ \\ | \end{array} \stackrel{(9.107)}{\approx} \begin{array}{c} \circ \\ | \end{array}$$

The colour-reversed version is similar. As the use of phase spider fusion is usually self-evident, we won’t explicitly indicate its use. \square

Next we show that equations (9.102), which we used as a starting point to build the fourth rule, now pop out.

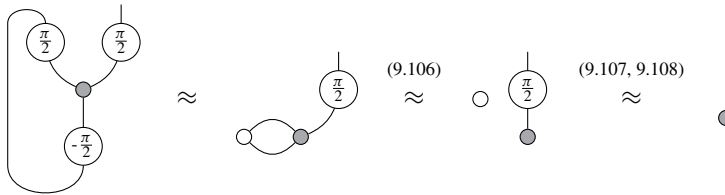
Proposition 9.110 The ZX-calculus obeys:

$$\begin{array}{c} \circ \\ | \\ \bullet \\ -\frac{\pi}{2} \end{array} \approx \begin{array}{c} \bullet \\ | \\ \circ \\ \frac{\pi}{2} \end{array} \quad \begin{array}{c} \circ \\ | \\ \bullet \\ \frac{\pi}{2} \end{array} \approx \begin{array}{c} \bullet \\ | \\ \circ \\ -\frac{\pi}{2} \end{array} \quad (9.109)$$

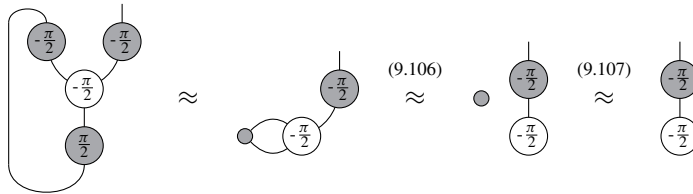
Proof After taking the partial trace of both sides of the Y-rule:

$$\begin{array}{c} \circ \\ | \\ \bullet \\ \frac{\pi}{2} \end{array} \begin{array}{c} \circ \\ | \\ \bullet \\ \frac{\pi}{2} \end{array} \begin{array}{c} \circ \\ | \\ \bullet \\ -\frac{\pi}{2} \end{array} \approx \begin{array}{c} \bullet \\ | \\ \circ \\ -\frac{\pi}{2} \end{array} \begin{array}{c} \bullet \\ | \\ \circ \\ -\frac{\pi}{2} \end{array} \begin{array}{c} \circ \\ | \\ \bullet \\ \frac{\pi}{2} \end{array} \quad (9.110)$$

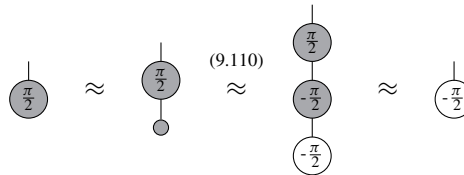
the LHS reduces to:



and the RHS to:



Then, applying a $\bullet \frac{\pi}{2}$ -phase to both sides yields the first equation in (9.109):



The second equation can then be obtained by conjugating both sides, which flips the signs. \square

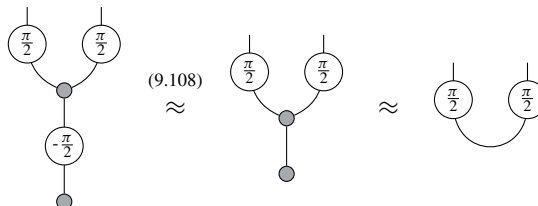
We now show that the rules involving π -phases from Section 9.3.4 can all be derived in the ZX-calculus (as long as we restrict phases to multiples of $\frac{\pi}{2}$). Most importantly, we need to show that π -phase states are indeed basis states. We start with the π -commute rule.

Proposition 9.111 The ZX-calculus obeys the π -commute rule:

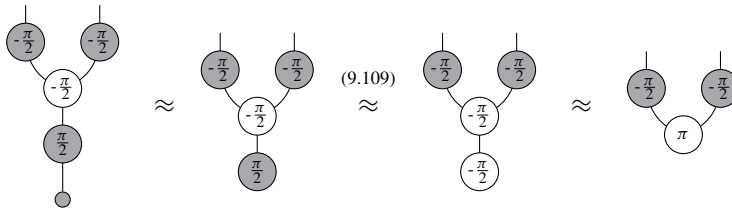


for $\alpha \in \{0, \frac{\pi}{2}, \pi, -\frac{\pi}{2}\}$.

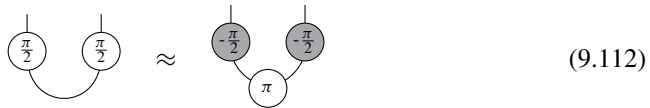
Proof By evaluating the LHS of the Y -rule on the \bullet -state we get:



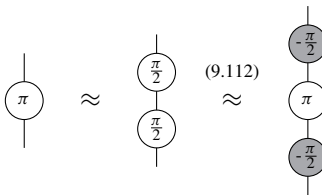
and doing the same with the RHS we get:



so we conclude:



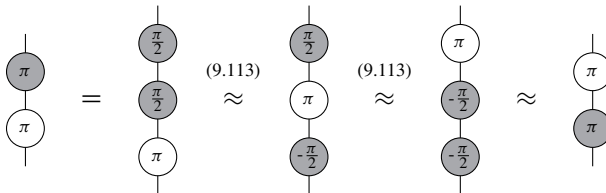
Unbending the wire yields:



Then, applying a $\bullet \frac{\pi}{2}$ -phase gate to the output gives:



i.e. (9.111) for $\alpha := \frac{\pi}{2}$. For the other angles, we can simply decompose as a series of $\frac{\pi}{2}$ gates; e.g. for $\alpha := \pi$ we have:



□

Exercise 9.112 Show that, if instead of on a \bullet -state, we evaluate on a \circ -state at the beginning of the proof above, the resulting equation is:

$$\begin{array}{c} \bullet \\ \downarrow \\ \bullet \\ \downarrow \\ \bullet \end{array} \approx \begin{array}{c} \circ \\ \downarrow \\ \bullet \\ \downarrow \\ \circ \end{array} \quad (9.114)$$

These rules give us enough to show that the ZX-calculus is colour-symmetric.

Theorem 9.113 The ZX-calculus obeys:

$$\begin{array}{c} \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \circ \\ \downarrow \\ \bullet \end{array} \approx \begin{array}{c} \circ \quad \circ \\ \diagdown \quad \diagup \\ \bullet \\ \downarrow \\ \circ \end{array} \quad (9.115)$$

Hence any equation provable in the ZX-calculus also holds with the colours reversed.

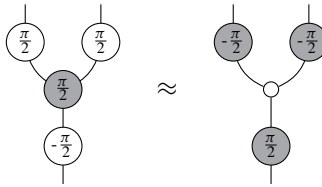
Proof Applying a series of phase gates to the LHS of the Y-rule gives:

$$\begin{array}{c} \circ \quad \circ \\ \diagdown \quad \diagup \\ \bullet \\ \downarrow \\ \circ \\ \downarrow \\ \circ \\ \downarrow \\ \bullet \\ \downarrow \\ \circ \end{array} = \begin{array}{c} \circ \quad \circ \\ \diagdown \quad \diagup \\ \bullet \\ \downarrow \\ \bullet \\ \downarrow \\ \circ \end{array} = \begin{array}{c} \circ \quad \circ \\ \diagdown \quad \diagup \\ \bullet \\ \downarrow \\ \bullet \\ \downarrow \\ \circ \end{array}$$

Applying the same phases to the RHS gives:

$$\begin{array}{c} \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \circ \\ \downarrow \\ \bullet \\ \downarrow \\ \circ \\ \downarrow \\ \bullet \\ \downarrow \\ \circ \end{array} \approx \begin{array}{c} \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \circ \\ \downarrow \\ \bullet \\ \downarrow \\ \bullet \\ \downarrow \\ \circ \\ \downarrow \\ \bullet \end{array} \approx \begin{array}{c} \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \circ \\ \downarrow \\ \pi \\ \downarrow \\ \bullet \\ \downarrow \\ \pi \end{array} \approx \begin{array}{c} \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \circ \\ \downarrow \\ \pi \\ \downarrow \\ \pi \\ \downarrow \\ \pi \end{array} = \begin{array}{c} \bullet \quad \bullet \\ \diagdown \quad \diagup \\ \circ \\ \downarrow \\ \bullet \end{array}$$

where for the first step we conjugated both sides of (9.114) to flip the signs. Hence we obtain:



and conjugating both sides completes the proof. \square

Exercise 9.114 Use the π -commute rule to prove the π -eliminate rule:

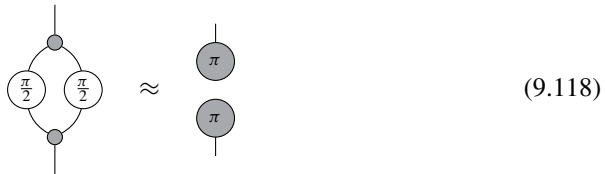


for $\alpha \in \{0, \frac{\pi}{2}, \pi, -\frac{\pi}{2}\}$. Then prove its colour-reverse:

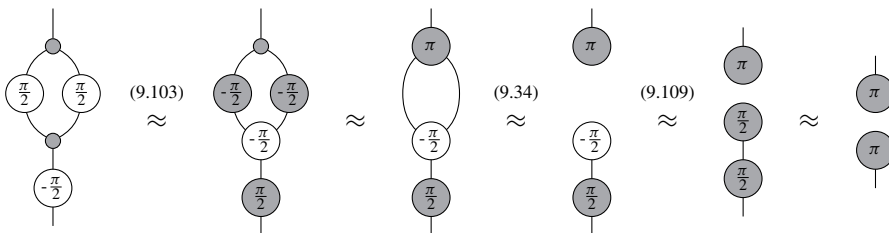


The following rule is one that we have not seen yet, but it's an important one that also disconnects diagrams.

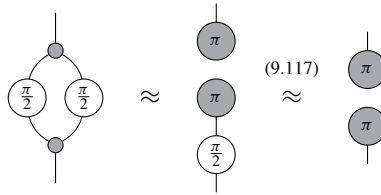
Proposition 9.115 The ZX-calculus obeys $\frac{\pi}{2}$ -supplementarity:



Proof First, we have:



Then, applying a $\circ \frac{\pi}{2}$ -phase gate gives:



□

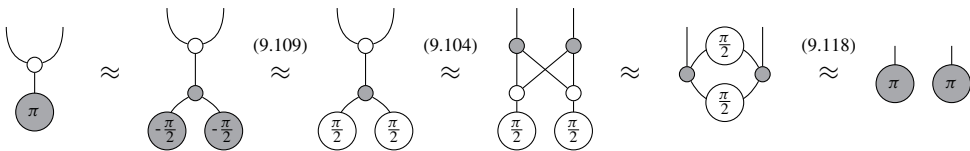
Remark 9.116 The use of the term ‘supplementarity’ above refers to the fact that $(\frac{\pi}{2}, \frac{\pi}{2})$ is a pair of *supplementary* angles, i.e. angles adding up to π (a.k.a. 180°). We’ll see a generalisation of this rule in Section 9.4.6.

Finally, we reach our goal of showing that the $\bullet \pi$ -phase state is a basis state for \circ (and vice versa via colour-reversal) using just the ZX-calculus.

Proposition 9.117 The ZX-calculus obeys the π -copy rule:



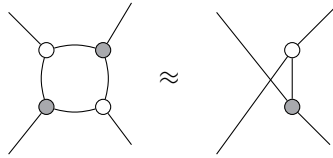
Proof We have:



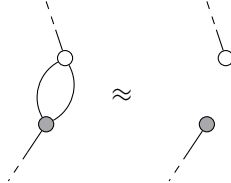
where you might need to stare at the fourth step for a bit to realise it’s just an application of \circ -phase spider fusion. □

9.4.4 ZX for Pros: Build Your Own Calculus

We’ll soon see that the four rules from Definition 9.108 suffice to prove everything for Clifford diagrams. However, that doesn’t necessarily mean they are the most convenient set of rules for someone to work with. For example, a person who is used to more traditional algebraic structures will find the many-input many-output rules very awkward and may find the Frobenius algebra rules that we discussed in Section* 8.6.1 a lot more appealing than spider fusion. (You: Are you joking? Us: No, we’re not.) That same person would also find the three defining equations of strong complementarity more appealing than the single rule in which we packaged them. Besides being corrupted by traditional algebra, one might find it more appealing simply to have a primitive rule for removing 4-cycles:

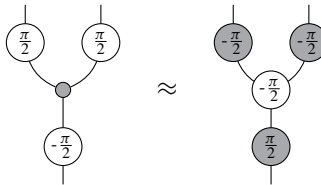


as we used to motivate strong complementarity in the first place. In a similar vein, one might wish to treat complementarity, and not strong complementarity, as a primitive:



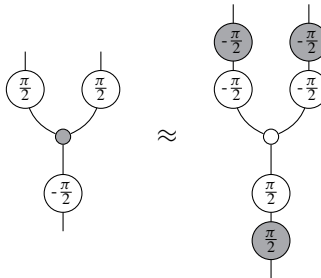
and come up with some new combination of rules that happens to imply strong complementarity. Why not? Everyone is different.

In this section, we'll derive an equivalent version of the ZX-calculus where the Y-rule:

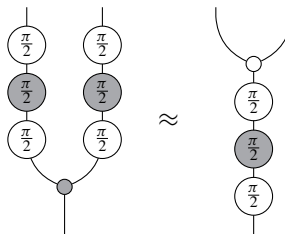


is replaced by something that is symmetric in the two colours. In the previous section, we did quite a bit of work to show that if any rule holds in the ZX-calculus, then so too does its colour-reversed version. Our new rule will show this colour-symmetry very explicitly by means of an explicit 'colour changer' that we construct out of phase gates.

First, with a bit of phase spider fusion, we have:



Then, by applying some $\frac{\pi}{2}$ phase gates to both sides, we can get rid of all the minus signs:



which at first seems like we've made everything worse. But then, if we let:

$$\square := \begin{array}{c} \circlearrowleft \frac{\pi}{2} \\ \circlearrowleft \frac{\pi}{2} \\ \circlearrowleft \frac{\pi}{2} \end{array} \quad (9.120)$$

we get:

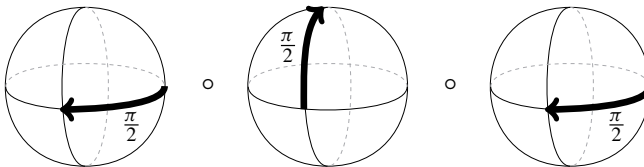
$$\begin{array}{c} \square \\ \circlearrowleft \frac{\pi}{2} \end{array} \approx \begin{array}{c} \circlearrowleft \frac{\pi}{2} \\ \square \end{array} \quad (9.121)$$

So we obtain a simple rule that tells us that the little white box passes through copy spiders and changes their colour. Aha! We seem to have found ourselves a candidate colour-changer!

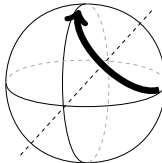
But what is this mysterious box? One way to figure this out is by using some geometry. Let's have a look at the corresponding quantum map:



As rotations of the Bloch sphere, this gives:



Those who are particularly spacially gifted will see that this amounts to the following 180° rotation:



Those who are not particularly spacially gifted are encouraged to find something ball-shaped and give it a try, or, if you happen to lack opposable thumbs, like a dodo, you can use ZX-calculus to show that the little white box sends X -basis states to Z -basis states.

Proposition 9.118 The ZX calculus obeys:

$$\begin{array}{c} \square \\ \circ \end{array} \approx \begin{array}{c} \bullet \\ \bullet \end{array} \quad \begin{array}{c} \square \\ \pi \end{array} \approx \begin{array}{c} \bullet \\ \pi \end{array} \quad (9.122)$$

Proof We have:

$$\begin{array}{c} \square \\ \circ \end{array} \approx \begin{array}{c} \pi/2 \\ \pi/2 \\ \pi/2 \end{array} \approx \begin{array}{c} \pi/2 \\ \pi/2 \\ \pi/2 \end{array} \approx \begin{array}{c} \pi/2 \\ \pi/2 \\ -\pi/2 \end{array} \approx \begin{array}{c} \pi/2 \\ \bullet \end{array} \approx \begin{array}{c} \bullet \end{array} \quad (9.109)$$

and similarly for the other basis state. \square

Since the little white box yields a 180° rotation, if we do it twice we get back to where we started, so it is self-inverse. For the dodos following along, we can again check this with the ZX-calculus.

Proposition 9.119 The ZX calculus obeys:

$$\begin{array}{c} \square \\ \square \end{array} = \begin{array}{c} | \end{array} \quad (9.123)$$

Proof One application of π -commute and some spider fusion yields:

$$\begin{array}{c} \square \\ \square \end{array} = \begin{array}{c} \pi/2 \\ \pi/2 \\ \pi/2 \\ \pi/2 \\ \pi/2 \\ \pi/2 \end{array} = \begin{array}{c} \pi/2 \\ \pi/2 \\ \pi \\ \pi/2 \\ \pi/2 \end{array} \approx \begin{array}{c} \pi/2 \\ \pi/2 \\ \pi \\ -\pi/2 \\ \pi/2 \\ \pi/2 \end{array} = \begin{array}{c} \pi/2 \\ \pi \\ \pi/2 \end{array} = \begin{array}{c} | \end{array} \quad (9.111)$$

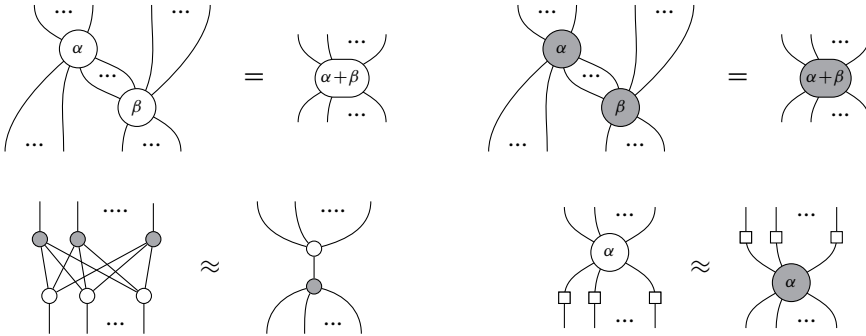
\square

So the little white box interchanges the Z- and X-basis states, and it is self-inverse. Sounds familiar? Indeed:

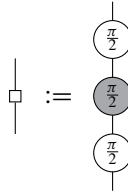
$$\begin{array}{c} \square \\ \square \end{array} = \begin{array}{c} H \\ H \end{array}$$

Our little white box and the Hadamard linear map that we first encountered back in Section 5.3.5 differ only by a global phase. Hence, we'll typically refer to either of them as the Hadamard gate, or *H-gate*. So, the punchline is as follows.

Theorem 9.120 The ZX-calculus can equivalently be presented as:



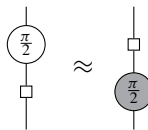
where:



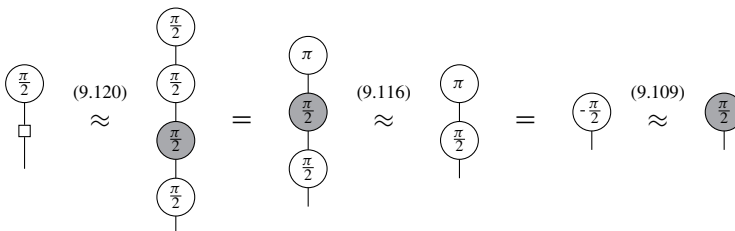
Proof Since any \circ -phase spider in a Clifford diagram can be built from just these pieces:



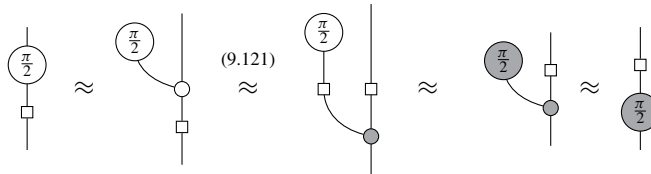
in order to change a whole \circ -phase spider to a \bullet -phase spider, all we need are rules to push *H*-gates through each of these pieces. Rules (9.121) and (9.122) together with their colour-reverses give us everything except:



To prove this, first, we have:

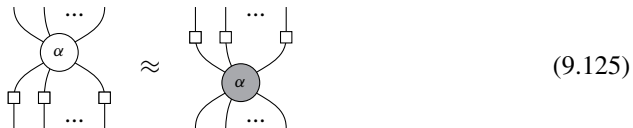


then, using the above in the third step:



Conversely, equation (9.121) arises as a special case of the colour change rule. Just by unfolding the definition of the colour-changer and doing the phase-juggling from the beginning of this section backwards, (9.121) clearly implies the *Y*-rule. \square

The new rule:



will be referred to as *colour change*.

9.4.5 ZX for the God(esse)s: Completeness

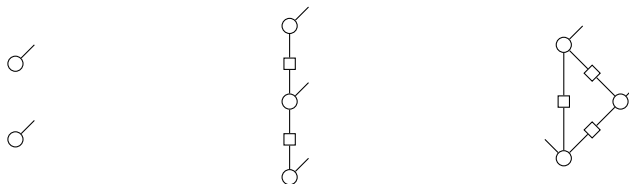
The ultimate goal of life, the universe, and everything is of course to replace horrible symbolic manipulations by diagrams. So how far are ZX-diagrams getting us towards that Final Frontier? As we already mentioned, we don't know yet. What we do know is that in the restricted case of the ZX-calculus for Clifford diagrams, we actually achieve that goal. That is, as far as deriving equations between Clifford diagrams goes, we can forget entirely that these diagrams ever had anything to do with linear maps, and simply use graphical calculus. To warp us there, our starship *Enterprise* will be the following concept.

Definition 9.121 A *graph state* is a state whose ZX-diagram consists only of (undecorated) \circ -spiders and *H*-gates where:

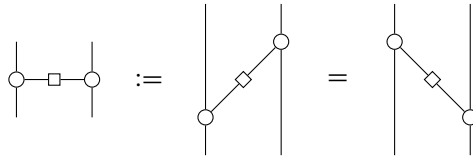
1. every \circ -spider has exactly one output, and
2. all non-output wires connect two \circ -spiders with a single *H*-gate.

Since any \circ -spider has exactly one output, we can identify quantum systems with the \circ -spiders. The edges then represent the way in which the systems are entangled with each other in the associated quantum state. We will see in Chapter 12 that *quantum graph states* obtained by doubling graph states form the basis of a *measurement-based* model of quantum computation.

Here are some examples of graph states:



Note that, for clarity, we typically don't bother to extend output wires all the way to the top, nor do we always write them vertically. Also, since an H -gate is self-transposed, there is no need to distinguish its input from its output. Thus, we can write H -gates on wires going sideways without ambiguity:



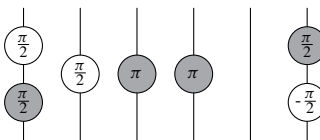
This comes in handy when drawing more elaborate graph states:



The reason we call these 'graph states' is that they are totally determined by the underlying (undirected) graph, i.e. the set of vertices connected by edges, which tells us where to add \circ -spiders and wires with H -gates:



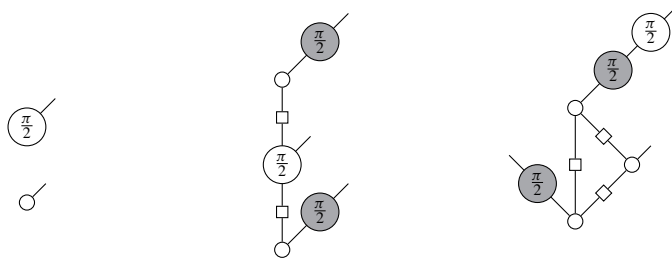
For our purposes, graph states are useful because they form the basis for a well-behaved canonical form for Clifford diagrams. This canonical form also involves *local Clifford unitaries*, i.e. unitaries expressible as parallel compositions of single-system Clifford diagrams. For example:



Remark 9.122 Since they only act on systems separately, local Clifford unitaries will not effect the entanglement between systems. Hence, when we consider graph states as an *entanglement resource*, local Clifford unitaries do not alter it in any essential way. We'll discuss this concept in detail in Section 13.3.

To obtain the canonical form, we first apply process–state duality to turn any Clifford diagram into a state. To these Clifford states we then apply the following result.

Proposition 9.123 Every Clifford state can be transformed using the ZX-calculus into a graph state, followed by local Clifford unitaries, e.g.:



This is called the *graph-form* for a Clifford diagram.

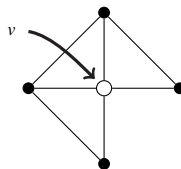
We won't give the proof of this theorem here, but it essentially goes as follows. First, the spiders in a Clifford diagram are decomposed using spider fusion into a finite set of 'little' spiders, namely those depicted in (9.124) and their \bullet counterparts. Then, the proof proceeds by induction on 'little' spiders. Whenever each type of 'little' spider is added to a Clifford diagram in graph form, the result can again be transformed into graph form.

Since we can convert every Clifford diagram into graph form, we only need to show the ZX-calculus suffices to prove equality between diagrams in graph form. Let's feed a bit of antimatter into the warp core.

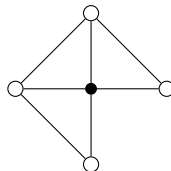
Definition 9.124 For an undirected graph G and a vertex v of G , the *local complementation* of G at v , written $G \star v$, is the graph obtained by *complementing* all the pairs w, w' of vertices adjacent to v , where by complementing we mean:

- If there is an edge connecting w and w' , remove it, and
- if there is not an edge connecting w and w' , add one.

Okay, that's a pretty tricky definition, so let's look at an example. Take this graph, with the vertex v shown in white:



The vertices *adjacent* to v are those connected to v by an edge, i.e. the ones in white here:



To do the local complementation, we delete edges between white vertices where we see them, and add them where we don't:

Again we'll omit the proof of this rather meaty theorem. However, the take-home message is: using the local complementation rule we can decide when two graph forms are equal by diagram rewriting. Combining this with Proposition 9.123, this means that if we can derive the local complementation rule in the ZX-calculus, then we can prove any equation between Clifford maps.

So, for our grand graphical finale, we'll derive the local complementation rule using the ZX-calculus. We begin with a little lemma.

Lemma 9.127 The ZX calculus obeys:

$$\text{Diagram 1} \approx \text{Diagram 2} \quad (9.127)$$

Proof First the H -gate goes up:

$$\text{Diagram 1} \stackrel{(9.125)}{\approx} \text{Diagram 2} \stackrel{(9.120)}{=} \text{Diagram 3} = \text{Diagram 4}$$

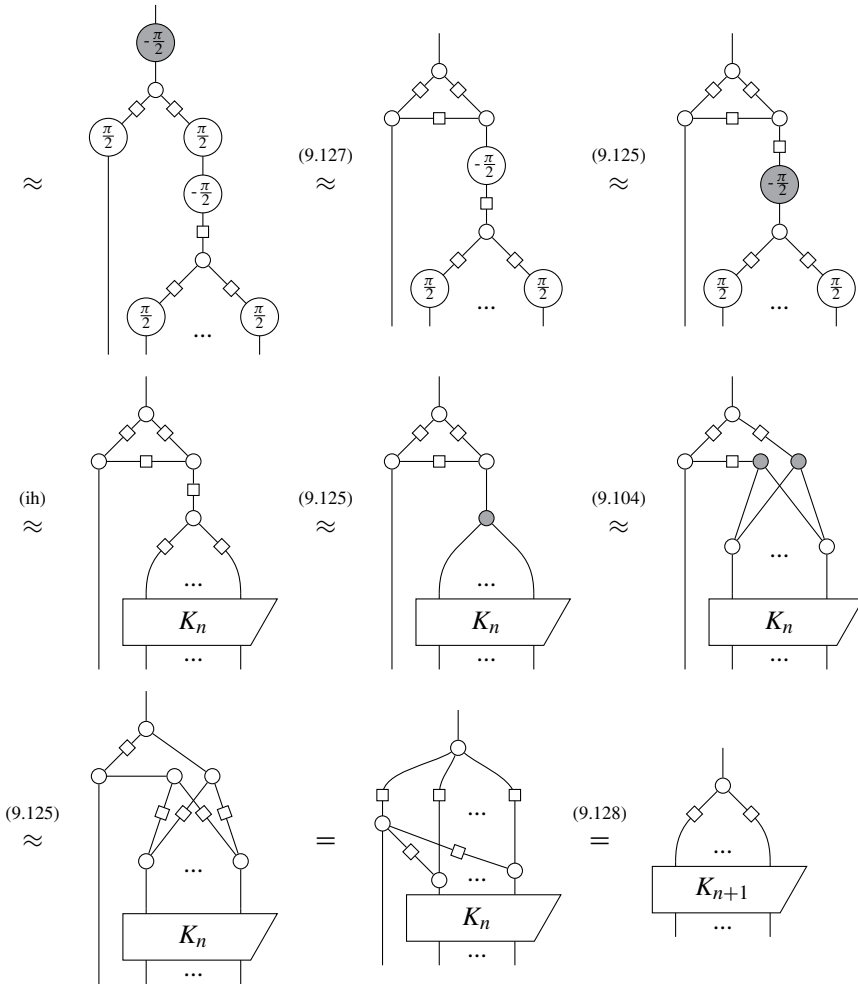
then we use some strong complementarity:

$$\text{Diagram 1} \stackrel{(9.104)}{=} \text{Diagram 2} \stackrel{(9.109)}{\approx} \text{Diagram 3} = \text{Diagram 4}$$

then the H -gate goes back down:

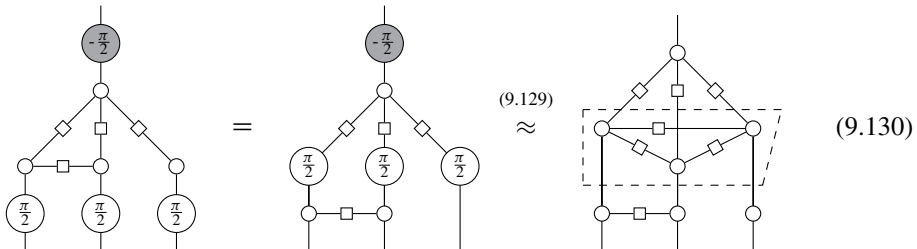
$$\text{Diagram 1} \stackrel{(9.125)}{\approx} \text{Diagram 2} \stackrel{(9.125)}{=} \text{Diagram 3}$$

□



□

So, what does this lemma say? It says that by applying a \bullet -phase gate of $-\frac{\pi}{2}$ to a node v_j in the graph state, and \circ -phase gates of $\frac{\pi}{2}$ to all of its neighbours, just like in the RHS of the local complementation rule (9.126), we introduce a new H -edge between every pair of neighbours of v_j :



But then, just like with complementary spiders, pairs of H -edges in graph states cancel out:

$$(9.131)$$

so the overall result is a local complementation around v_j :

$$(9.130)$$

Bingo! We derived the local complementation rule using nothing but the four humble rules from Definition 9.108. All together we can now conclude the following.

Theorem 9.129 The ZX-calculus is complete for **Clifford maps**. That is, for any two Clifford diagrams D, E , the following are equivalent:

- $D = E$ can be derived in ZX-calculus, and
- the associated Clifford maps $\llbracket D \rrbracket$ and $\llbracket E \rrbracket$ are equal, up to a number.

We can thus make a statement analogous to the one about string diagrams and dot diagrams, provided we interpret two Clifford diagrams as being ‘the same’ when we can rewrite one diagram into the other by means of ZX-calculus:

An equation between Clifford maps holds if and only if the Clifford diagrams are the same.

9.4.6 Where We Stand with Full ZX-Calculus

Even though Clifford maps already exhibit many quantum features, there is at least one reason one wants to consider more general ZX-diagrams. It is well known that Clifford diagrams (or, rather, their unitary cousins Clifford quantum circuits) are efficiently classically simulable. That is, if we input some fixed state into a Clifford map and measure the outputs, we can write a program on a classical computer that efficiently computes the Born-rule probabilities. Hence, if we want to build a quantum computer, Clifford maps don’t really give us anything new. We’ll discuss this more in Chapter 12.

On the other hand, if we add just one more phase to Clifford diagrams, we actually get a lot more.

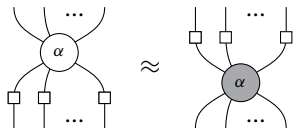
Definition 9.130 A *Clifford+T diagram* is a ZX-diagram where the phases are restricted to integer multiples of $\frac{\pi}{4}$, and **Clifford+T maps** is the corresponding subtheory of **pure quantum maps**.

The funny name comes from the fact that, in the quantum computing literature, the $\frac{\pi}{4}$ -phase gate is often called the *T gate*. Adjoining the $\frac{\pi}{4}$ phase, for practical purposes pretty much gives us everything, in the sense that we can always get arbitrarily close to what we aim for.

Theorem 9.131 Clifford+T diagrams are *approximately universal*. That is, any linear map can be approximated up to arbitrary precision by a Clifford+T diagram.

We already know that ZX-diagrams let us build any quantum process, and now we know even Clifford+T diagrams let us pretty much build any process. So, how much can we say about these richer diagrams?

If we move from Clifford diagrams to arbitrary ZX-diagrams, the first thing we notice is several of the rules we proved for $\alpha \in \{0, \frac{\pi}{2}, \pi, -\frac{\pi}{2}\}$ extend to arbitrary phases. For example, clearly applying *H*-gates to every leg of a phase spider will change its colour, regardless of the value of α . Consequently:



$$(9.132)$$

holds concretely, for all α . Similarly:



$$(9.133)$$

also holds for all α .

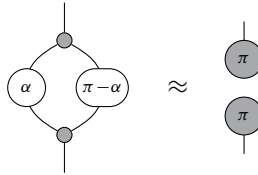
In fact, if we add the two rules above to the ZX-calculus we get a bit closer completeness for all ZX-diagrams.

Theorem 9.132 The ZX-calculus, with the addition of the rules (9.132) and (9.133), is complete for **single qubit Clifford+T maps**, i.e. maps of the form:

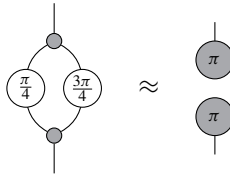


Well, that might not look like much, but it's a start. Could it be the case that with this new extended version of the ZX-calculus we have completeness with respect to all Clifford+T diagrams?

Unfortunately, no. Like the other two rules above, the $\frac{\pi}{2}$ supplementarity rule has a big brother, which holds for (almost) all phases. For all α not equal to 0 or π , we have:



That is, for any (non-trivial) pair of supplementary angles $(\alpha, \pi - \alpha)$ the diagram above separates. It turns out, even when restricting to Clifford+T diagrams, that the equation:



isn't provable from the existing rules. And that's all we know at the moment! Maybe there is a single magical rule that does the job, maybe not. So, alas, we must finish with an 'exercise'.

Exercise* 9.133 Find a complete set of rules for (Clifford+T) ZX-diagrams.

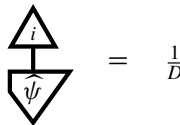
As with Exercise 7.39, if you find a solution, we'd love to hear about it! All the relevant publications will be discussed at the end of this chapter, but by the time you get to read this, probably there will be more.

9.5 Summary: What to Remember

1. The *unbiased* states for spiders are those states that satisfy:



That is, unbiased states for spiders \circ give the uniform probability distribution for \circ -measurements. In terms of the Born rule, this means for all i :



Dropping normalisation gives us *phase states*:

The *phases* that decorate these states have a clear interpretation as:

the data destroyed by the classical-quantum passage

In other words, phases constitute the stuff that is genuinely quantum. In the case of a qubit they take the following form:

2. *Phase spiders* arise as follows:

and *phase spider fusion* is:

where:

This operation provides phases with the structure of a commutative group, the *phase group*, for which the unit and the inverse, respectively, are:

An important example of phase spiders are *phase gates*:

3. Spiders \circ and \bullet are *complementary* if:

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array} \quad \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

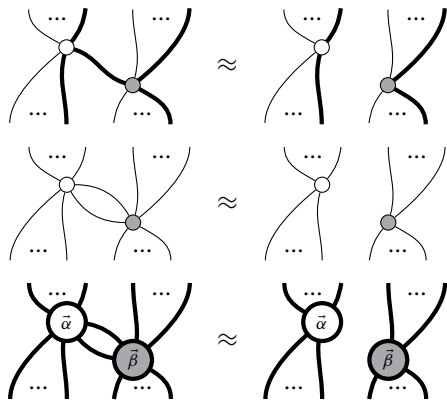
Complementarity admits the following interpretation:

(encode in \circ) THEN (measure in \bullet) = (no data flow)

Complementary is equivalent to all of the ONB-states of \circ being unbiased for \bullet and vice versa, which can be expressed in two ways:

$$\begin{array}{c} \bullet \\ | \\ \nabla_i \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \quad \begin{array}{c} \nabla_i \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \bullet \end{array}$$

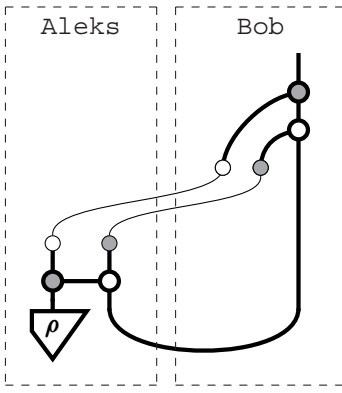
4. Complementarity induces *spider detachment rules*:



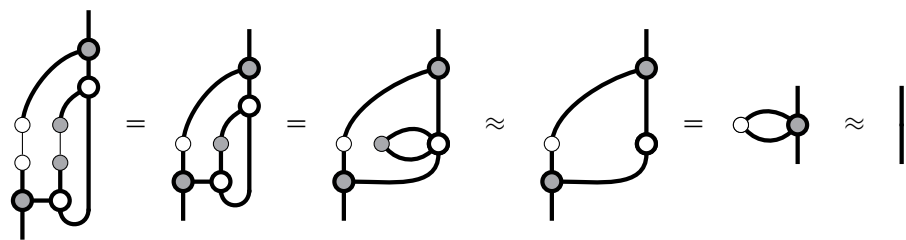
5. A complementary pair yields generalised CNOT-gates:

$$\sqrt{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \quad D \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array}$$

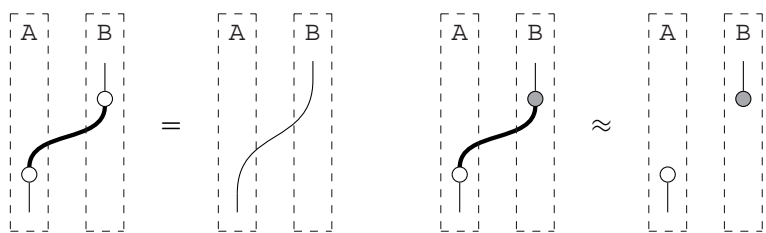
It also provides all of the pieces needed for teleportation:



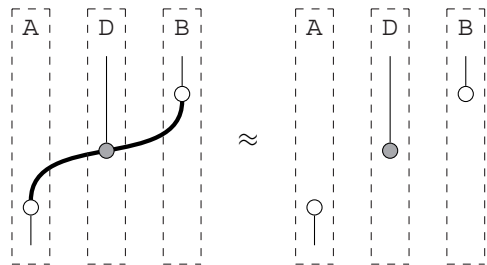
and for proving its correctness:



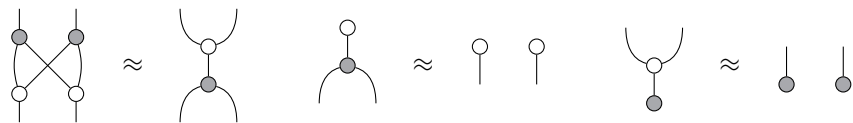
We can also do a protocol called *quantum key distribution*:



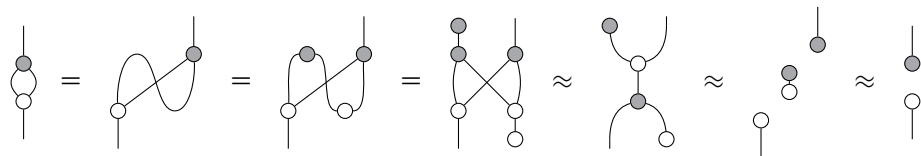
which makes it possible to detect eavesdropping on a quantum channel:



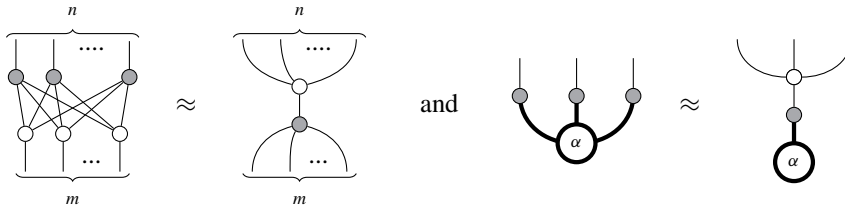
6. Strong complementarity:



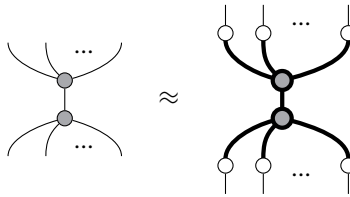
strictly implies complementarity:



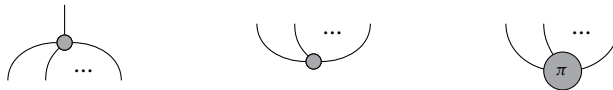
It also gives us much more rewriting power and implies, for instance:



as well as:



which shows that \bullet spiders are classical maps for \circ . Some examples of classical maps for \circ in terms of \bullet spiders are the *parity map*, the *even-parity state*, and the *odd-parity state*:



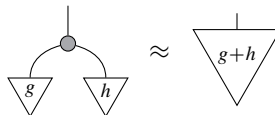
7. Strong complementarity is equivalent to the basis states of \circ forming a *subgroup* of the phase group of \bullet , and vice versa. That is, phase states satisfying:



form the following subgroups:

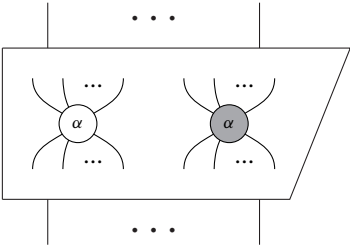
$$\left\{ \begin{array}{c} \circ \\ \vec{k} \end{array} \right\}_{\vec{k}} \subset \left\{ \begin{array}{c} \bullet \\ \vec{\alpha} \end{array} \right\}_{\vec{\alpha}} \quad \left\{ \begin{array}{c} \circ \\ \vec{k} \end{array} \right\}_{\vec{k}} \subset \left\{ \begin{array}{c} \bullet \\ \vec{\alpha} \end{array} \right\}_{\vec{\alpha}}$$

8. Strongly complementary pairs of spiders are *classified* by commutative groups. That is, for a family of spiders \circ and any finite commutative group G , there exists a unique family of spiders \bullet such that \circ/\bullet is strongly complementary and:



Conversely, all strongly complementary pairs arise in this manner.

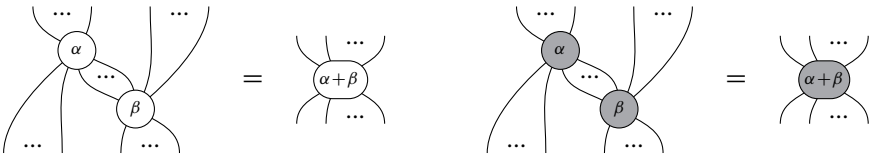
9. ZX-diagrams, i.e. diagrams made up of \circ and \bullet phase spiders:



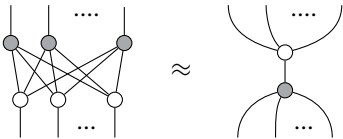
are *universal for qubits*, that is, we can express any classical-quantum map on qubits as a ZX-diagram.

10. Clifford diagrams are ZX-diagrams where the phases are restricted to integer multiples of $\frac{\pi}{2}$. The ZX-calculus, a graphical calculus for Clifford diagrams, consists of the following rules:

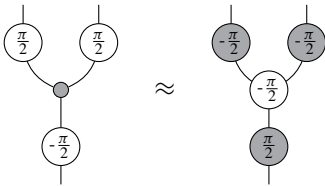
1. Two rules to combine spiders of the same colour:



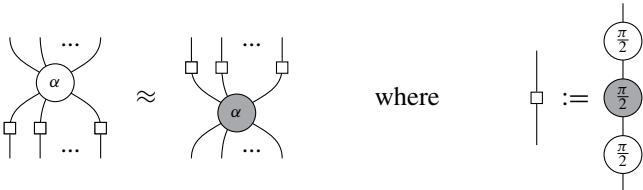
2. One rule to commute spiders of different colours past each other:



3. One rule to convert spiders of one colour into another:



Equivalently, we can replace the last rule with the *colour-change* rule:



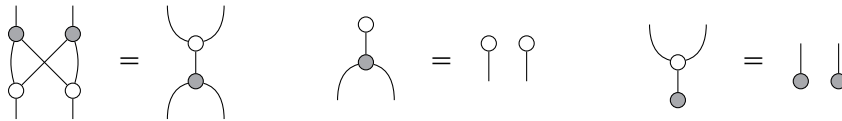
The ZX-calculus is complete for **Clifford maps**, i.e. pure quantum maps expressible as Clifford diagrams. Hence, any equation between Clifford maps can be proven just using the rules of the ZX-calculus.

9.6 Advanced Material*

9.6.1 Strongly Complementary Spiders Are Hopf Algebras*

In Section* 8.6.1 we saw that spiders have been more commonly known as (\dagger -special commutative) Frobenius algebras. Strongly complementary pairs of spiders have also been around for a long time.

Definition 9.134 A *bialgebra* on a vector space V consists of an associative algebra (\bullet, \circ) and a coassociative coalgebra (\circ, \bullet) satisfying:



A bialgebra is called a *Hopf algebra* if it additionally has a linear map:

$$\begin{array}{c} | \\ \boxed{\iota} \\ | \end{array} : V \rightarrow V$$

called the *antipode* such that:

$$\begin{array}{c} | \\ \bullet \\ \boxed{\iota} \\ | \end{array} = \begin{array}{c} | \\ \bullet \end{array} \quad (9.135)$$

That indeed looks pretty familiar. If we add the $\frac{1}{\sqrt{D}}$ -factors and let the antipode be trivial:

$$\begin{array}{c} | \\ \boxed{\iota} \\ | \end{array} := \begin{array}{c} | \end{array}$$

then we get exactly the (strong) complementarity equations.

So, what's the deal with this antipode thing anyway? Let's have a look again at the \bullet -spiders from Section 9.3.6 defined in terms of a commutative group G :

$$\begin{array}{c} | \\ \bullet \\ \swarrow \quad \searrow \\ g \quad h \end{array} \approx \begin{array}{c} | \\ \triangle \\ g+h \end{array} \quad \begin{array}{c} | \\ \bullet \end{array} \approx \begin{array}{c} | \\ \triangle \\ 0 \end{array} \quad (9.136)$$

Plugging a \circ ONB-state corresponding to a group element $g \in G$ into equation (9.135) yields:

So, if we take the group-sum of g and ι applied to g , we get 0. This means that ι encodes the group-inverse:

The antipode law of a Hopf algebra captures the fact that $g - g = 0$:

Hopf algebras that come from a group in this way are called *group algebras*. A group algebra has trivial antipode precisely when G consists only of self-inverse elements $g = -g$, like for example the parity group \mathbb{Z}_2 .

Remark 9.135 Even though we wrote the group operation as ‘+’ (which is usually done only for commutative groups), this construction works just as well for non-commutative groups. In that case the algebra \bullet becomes non-commutative, but \circ (which is still just copying) remains co-commutative. A large literature exists studying certain kinds of Hopf algebras that are neither commutative nor co-commutative, called *quantum groups*.

At this point, you might be thinking, ‘Hang on, doesn’t strong complementarity (the bialgebra equations) imply complementarity (the extra Hopf algebra equation)?’ The answer is of course Yes, but \circ and \bullet need to be spiders (a.k.a. \dagger -special commutative Frobenius algebras), not just plain old (co)algebras.

Moreover, having a careful look at the proof that strong complementarity implies complementarity:

we see that the second step relies crucially on the fact that:

$$\begin{array}{c} \circ \\ \cup \end{array} = \begin{array}{c} \cup \\ \circ \end{array} = \cup \quad \text{and} \quad \begin{array}{c} \cup \\ \circ \end{array} = \begin{array}{c} \circ \\ \cup \end{array} = \cup$$

which is only true for families of spiders that come from self-conjugate ONBs, an assumption that we make throughout this book.

In fact, we could drop this assumption, provided that we modify complementarity to:

$$\begin{array}{c} \bullet \\ \diagup \diagdown \\ \square \quad t \\ \diagdown \diagup \\ \circ \end{array} \approx \begin{array}{c} \bullet \\ | \\ \circ \end{array} \quad (9.137)$$

where we take the following antipode:

$$\begin{array}{c} \diagup \diagdown \\ \square \quad t \\ \diagdown \diagup \end{array} := \begin{array}{c} \bullet \\ | \\ \cup \\ | \\ \circ \end{array} \quad (9.138)$$

Then we indeed have:

$$\begin{array}{c} \bullet \\ \diagup \diagdown \\ \square \quad t \\ \diagdown \diagup \\ \circ \end{array} \stackrel{(9.138)}{=} \begin{array}{c} \bullet \\ | \\ \cup \\ | \\ \circ \end{array} = \begin{array}{c} \bullet \\ | \\ \cup \\ | \\ \circ \end{array} \approx \begin{array}{c} \bullet \\ | \\ \cup \\ | \\ \circ \end{array} \stackrel{(*)}{\approx} \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

Exercise 9.136 Prove the last step of this derivation marked (*). This, in particular, will require proving:

$$\begin{array}{c} \diagup \diagdown \\ \square \quad t \\ \diagdown \diagup \\ \bullet \end{array} \approx \begin{array}{c} \bullet \end{array} \quad \begin{array}{c} \circ \\ \diagup \diagdown \\ \square \quad t \\ \diagdown \diagup \\ \circ \end{array} \approx \begin{array}{c} \circ \end{array}$$

Much of what we did in this book can be extended to this more general setting, although diagrams become a bit more complicated.

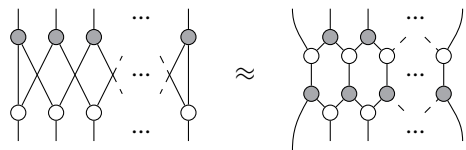
Exercise 9.137 Adapt the description of quantum teleportation using complementary spiders of Section 9.2.7 to this more general setting. Bonus points: use the ‘hairy spiders’ from Section* 8.6.3 for expressing non-self-conjugate spiders.

9.6.2 Strong Complementarity and Normal Forms*

We have already seen the following consequence of strong complementarity:

$$\begin{array}{c} \bullet \quad \bullet \quad \dots \quad \bullet \\ \diagdown \quad \diagup \quad \dots \quad \diagdown \quad \diagup \\ \square \quad \square \quad \dots \quad \square \\ \diagup \quad \diagdown \quad \dots \quad \diagup \quad \diagdown \\ \circ \quad \circ \quad \dots \quad \circ \end{array} \approx \begin{array}{c} \dots \\ \cup \\ \bullet \\ \cup \\ \dots \end{array} \quad (9.139)$$

whereby a complete bipartite graph of spiders can be replaced by a single \bullet -spider followed by a single \circ -spider. But in fact, there are many more equations of this kind one can derive; for example, this equation:



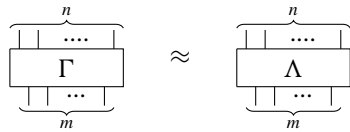
(9.140)

lets us turn large ($2N$ -long) cycles of alternating \circ - and \bullet -spiders into a bunch of connected six-cycles.

Exercise* 9.138 Prove equation (9.140).

Equations (9.139) and (9.140) are both instances of the following, much more general result.

Theorem 9.139 An equation:

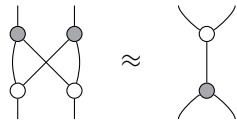


where Γ and Λ are both circuits consisting only of spiders of the form:

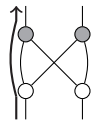


is provable using spider fusion and strong complementarity if and only if the number of (forward-directed) paths, modulo 2, connecting each input to each output is the same in Γ and Λ .

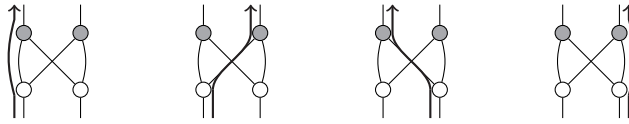
In other words, we can prove any equation that follows from strong complementarity just by path-counting. Let's see this in action for the simplest example, which is just the first strong complementarity equation itself:



If we count the number of paths from the first input to the first output, we see there is just one:



In fact, there is exactly one path for every combination of input/output:



and the same is true on the RHS:



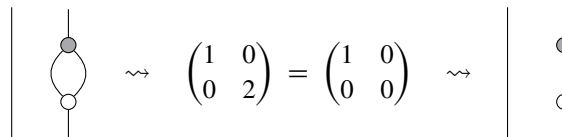
Hence we can conclude that the LHS and the RHS are equal. Checking the other two strong complementarity rules, we see they also respect the number of paths from inputs to outputs (which in those cases is always 0).

Exercise 9.140 Prove equation (9.140) using Theorem 9.139.

It is convenient to collect all of this path-counting information into the *path matrix* of a diagram. That is, a matrix \mathbf{m} where each entry \mathbf{m}_i^j gives the number of paths (modulo 2) from input i to output j . For instance, the path matrices of the diagrams above are both:



The reason we count modulo 2 is that pairs of paths can be eliminated using the complementarity rule:



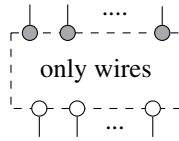
This clearly gives an equivalent statement to Theorem 9.139.

Corollary 9.141 Diagrams Γ and Λ (as in Theorem 9.139) are equal whenever they have the same path matrix.

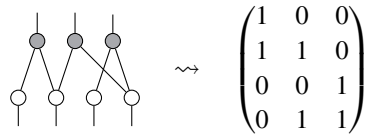
So, how do we prove it? First, note that all of the strong complementarity rules and spider fusion respect the path matrix. So, it suffices to show that we can use these rules to rewrite any diagram into a *normal form*, which is uniquely fixed by a given path matrix. These normal forms are described as follows:

- (i) No spiders of the same colour are touching;
- (ii) any pair of spiders is connected by at most 1 edge; and
- (iii) all \circ -spiders occur before \bullet -spiders.

Pictorially, these normal forms look like this:



From such a normal form, we can immediately read off the path matrix just by putting a 1 whenever we see a wire connecting the appropriate spiders. For example:

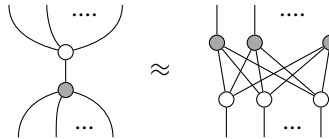


Conversely, for any path matrix, there is a unique normal form that has the correct paths from its inputs to its outputs.

So, it only remains to show that any diagram can be put into normal form. If our diagram doesn't satisfy (i) or (ii) above, we can always apply spider fusion or complementarity until it does. So, (iii) is the only tricky condition. This is where restricting to these spiders:

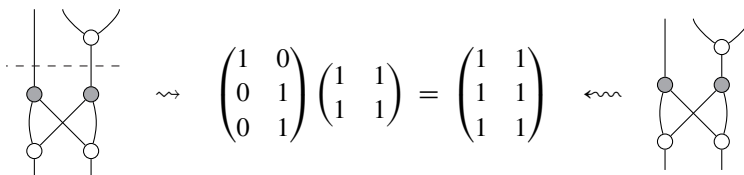


plays an important role. The only way a diagram will not satisfy (iii) is if it contains the RHS of (9.139). But then, if we just apply this equation backwards:



we can push the \circ -spider past the \bullet -spider. Since we restrict to circuit diagrams, if we do this repeatedly, all the \bullet -spiders will float to the top, while all the \circ -spiders will sink to the bottom, giving us a normal form.

Interestingly, path matrices themselves form a process theory. First note that \circ -composing two matrices yields the same result as counting paths on the composed diagram:



The \otimes -composition of diagrams does not yield the Kronecker product of path matrices, but rather the *direct sum*:

$$\left(\begin{array}{c} \text{diagram 1} \end{array} \right) \oplus \left(\begin{array}{c} \text{diagram 2} \end{array} \right) \rightsquigarrow \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \leftarrow \left(\begin{array}{c} \text{diagram 1} \end{array} \right) \left(\begin{array}{c} \text{diagram 2} \end{array} \right)$$

This is a perfectly reasonable way to compose matrices in parallel, so let **matrices** $_{\oplus}(\mathbb{Z}_2)$ be just like the process theory of matrices defined in Section 5.2.5, except that parallel composition is \oplus , not Kronecker product.

The special ‘one-to-many-legged’ spiders from Theorem 9.139 both live in this process theory:

$$\left(\begin{array}{c} \text{spider with 1 in, } \dots \text{ outs} \end{array} \right) \rightsquigarrow \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \quad \left(\begin{array}{c} \text{spider with } \dots \text{ ins, 1 out} \end{array} \right) \rightsquigarrow (1 \quad 1 \quad \dots \quad 1)$$

and the only equations that hold between diagrams of these spiders are those that come from spider fusion and strong complementary (or, equivalently, the Hopf algebra equations). This process theory is ‘the walking Hopf algebra’, in the sense that it contains a Hopf algebra and nothing else. Hence, if we really wish to study the essence of Hopf algebras, we should study this process theory. To category theorists, this is known as the *PROP for Hopf algebras*.

9.7 Historical Notes and References

The bulk of this chapter, most notably the diagrammatic notions of phase states, phase spiders, the phase group, complementarity (i.e. mutual unbiasedness), and strong complementarity, as well as all of the equivalent characterisations of Section 9.3.4, are taken from Coecke and Duncan (2008, 2011). However, in Coecke and Duncan (2008) there is a void statement, namely that, under the ‘mild’ assumption of classical subgroup closure, complementarity and strong complementarity are equivalent. Only later the authors realised that classical subgroup closure is already equivalent to strong complementarity, so it’s not so mild after all!

The usual notion of mutual unbiasedness was first introduced by Schwinger (1960). An extensive survey of what is known about them is in Durt et al. (2010), including problems concerning their classification. On the other hand, the classification of strongly complementary pairs is due to Kissinger (2012a).

The ZX-calculus was also introduced in Coecke and Duncan (2008, 2011). However, the version presented there wasn’t enough for the completeness theorem of Section 9.4.5. While the *Y*-rule is new (besides a more complex version of it having appeared in talks by Ross Duncan), the equivalent version in terms of Euler-angle decomposition of the

H -gate is due to Duncan and Perdrix (2009). Most versions of the ZX-calculus that have been around contained many redundancies, but a minimal version (from which our presentation is derived) was recently given by Backens et al. (2016).

The completeness theorem with respect to Clifford maps was proved by Backens (2014a), and the completeness theorem with respect to single qubit Clifford+T maps was also proved by Backens (2014b). A related theorem is the complete characterisation for n -qubit Clifford circuits in terms of generators and relations given by Selinger (2015).

Schröder de Witt and Zamdzhiev (2014) showed that completeness cannot be achieved with the current rules for arbitrary quantum maps on qubits, and Perdrix and Wang (2015) showed that this is also the case for Clifford+T maps. The supplementarity equation that was used for that purpose first appeared in Coecke and Edwards (2010).

Graph states, which played an important role in the completeness proof, were introduced by Hein et al. (2004). Proposition 9.125, which is due to Backens, builds further on a powerful theorem by van den Nest that states that graph states are equivalent up to local Clifford unitaries if and only they can be turned into each other via local complementation (Van den Nest et al., 2004).

The first person to realise that strong complementarity could be used to model how classical systems and quantum data interact as in example 9.74 was Quanlong (Harny) Wang, as part of the team that produced the paper by Coecke et al. (2012).

Quantum circuits were introduced by Deutsch (1989). Quantum key distribution was first introduced by Bennett and Brassard (1984), and the version obtained by ‘bending the wire’ (i.e. using an entangled state instead of sending a quantum system) is due to Ekert (1991). The protocol in Example 9.61 is due to Perdrix (2005).

The use of ZX-calculus to model quantum circuits is from Coecke and Duncan (2008), and its use for quantum key distribution as in Section 9.2.6 is from Coecke and Perdrix (2010) and Coecke et al. (2011a). Building controlled operations in the ZX-calculus as in Section 9.2.7 comes from Coecke and Duncan (2011). A similar construction, just in terms of CNOT and phase gates, appeared in Barenco et al. (1995).

A good resource for Hopf algebras and quantum groups is Street (2007). Other standard references are Kassel (1995) and Majid (2000). The ‘path counting’ characterisation, as well as the normal form for bialgebras from Section* 9.6.2, was given by Lack (2004), as an example of systematically ‘composing’ two diagrammatic theories (a.k.a. *PROPs*), namely, algebras and coalgebras. This same technique was used to compose a pair of bialgebras to obtain the entire phase-free fragment of the ZX-calculus in Bonchi et al. (2014b). Interestingly, the theory has much the same characterisation as the one we gave for bialgebras in Section* 9.6.2, but with matrices generalised to ‘linear relations’. An amusing and pedagogical account of this result involving football, LEGO, and dividing by zero is available as a blog (Sobocinski, 2015).

The phrase ‘unreasonable effectiveness of diagrammatic reasoning with spiders’ is stolen from Wigner (1995b), who argues the ‘unreasonable effectiveness of mathematics in the natural sciences’.