Quantum Processes and Computation

Assignment 6, Friday, 18 Nov

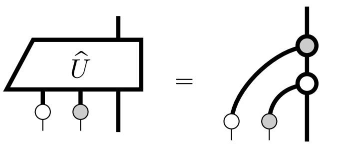
Deadline: Fri Week 7 (Groups 3 and 4), Weds Week 8 (Groups 1 and 2)

Goals: After completing these exercises you should know how to prove equalities between classical-quantum maps using the ZX-calculus, translate to and from quantum circuit notation, and do basic quantum circuit optimisations by hand.
Material covered in book: Chapters 9, 12.1

Note: Many of these exercises also appear in *Picturing Quantum Processes*, but sometimes they have been slightly modified for the problem sheet. The corresponding exercise number from the book is shown in brackets. **If you are stuck, try looking up the exercise number in the book. Usually the definitions or equations you need are nearby.**

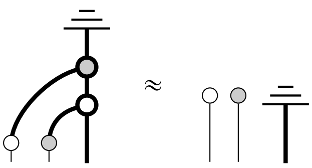
Exercise 1 (9.49, 9.58)

1. Read Section 9.2.7 about teleportation with complementary spiders. To show that it is a valid protocol we must show that the actions of both Aleks and Bob can in fact be performed, i.e. that they are causal cq-maps. We already know that Aleks's side is causal, so it remains to show that Bob's side is as well, i.e. that

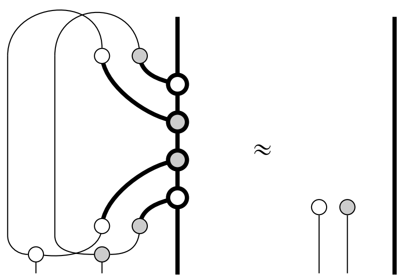


(1)

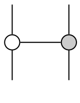
is causal, up to a number:



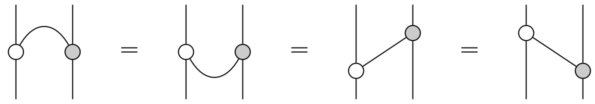
2. Show that furthermore, this map is a controlled isometry, up to a number, i.e.



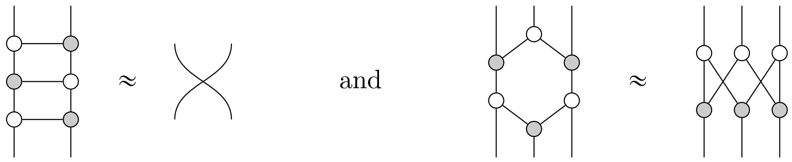
Exercise 2 (9.47): Read Section 9.2.3 about the controlled-NOT gate (CNOT):



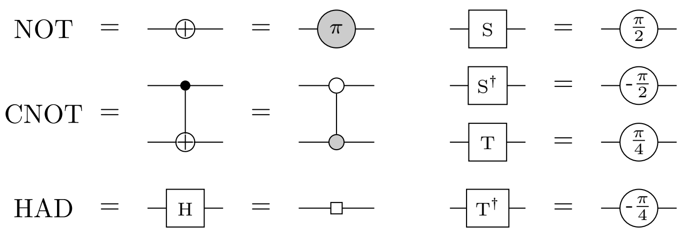
(i) Complete Lemma 9.46 by proving the remaining equalities:



(ii) Use complementarity and strong complementarity to prove that



The usage of ZX-diagrams to represent quantum circuits is not (yet) standard. A more commonly used notation is known just as *quantum circuit notation.* In this notation, the atomic building blocks are gates instead of spiders. A set of commonly used gates and their notation is:

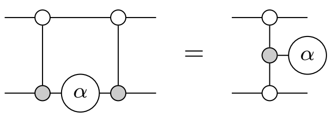


(2)

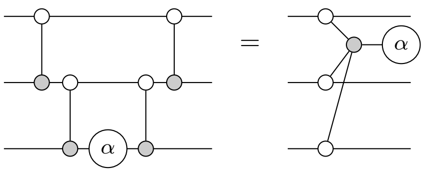
All of these gates are Clifford except for the T gate and its adjoint $\mathrm{T}^\dagger$. To make sure you get familiar with this notation, we will use it a few times throughout this exercise sheet.

Exercise 3:

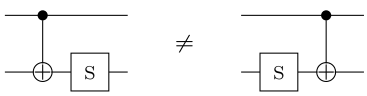
(i) In the last exercise sheet you had to find a circuit representation of the controlled-phase gate. The important part of this gate is what we call a *phase-gadget*:



Show that this equation generalises by proving the following equation in the ZX-calculus:

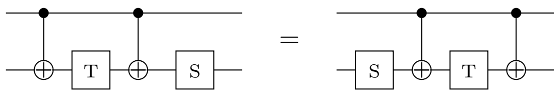


(ii) Show that a phase gate does not commute past the target of a CNOT:

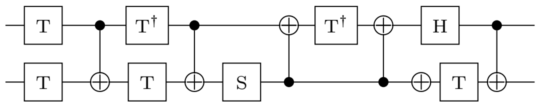


Hint: Find some input state under which the two sides aren't equal.

(iii) Show that a phase gate *does* commute past a phase-gadget:



Exercise 4: Consider the following quantum circuit:



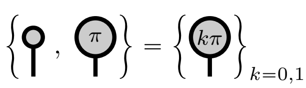
The goal is to find a more optimal implementation of this circuit. Write this circuit as a ZX-diagram, simplify it using diagrammatic reasoning, and then write it again as a quantum circuit in quantum circuit notation using the gate-set of (2). Use whatever rewrite rules you know to minimize the *T-count* of the circuit. This is the amount of T and $\text{T}^\dagger$ gates in the circuit (or in terms of a ZX-diagram, the amount of spiders that have odd multiples of $\frac{\pi}{4}$ on them). For full marks, find an equivalent circuit that has a T-count of zero.

T-count optimisation is an important problem in large-scale quantum computation as in most fault-tolerant architectures, Clifford gates are cheap to implement, while T gates can require a lot of resources and time to implement (sometimes up to 100 times more than a CNOT).

Exercise 5: This is (most of) an old exam question. It should give some idea of the size/difficulty of questions to expect.

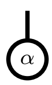
In some models of quantum computation (and particularly in fault-tolerant quantum computing), we have certain operations that come essentially for free and some that are much more expensive. For example, the following operations are often treated as free on a fault-tolerant quantum computer:

- preparing Z basis states,
- applying Clifford gates, i.e. CNOT, H, and $S := Z_{\pi/2}$, and
- performing Z basis measurements, i.e. the ONB measurement with the following outcomes (ignoring numbers):



In the questions below, "using free operations" means performing the above processes any number of times, where we are allowed classical control (i.e. choosing which gates to perform depending on measurement outcomes).

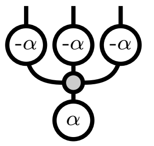
The other operations we can do on our fault-tolerant quantum computer are precious commodities! A typical example is a "magic state" of the form:

$z_\alpha :=$ 

(a) Show that, using one $z_{\pi/4}$ state, a CNOT, and a Z ONB measurement, there is a protocol that sometimes produces the Z phase gate $T := Z_{\pi/4}$ and sometimes produces $T^\dagger := Z_{-\pi/4}$.

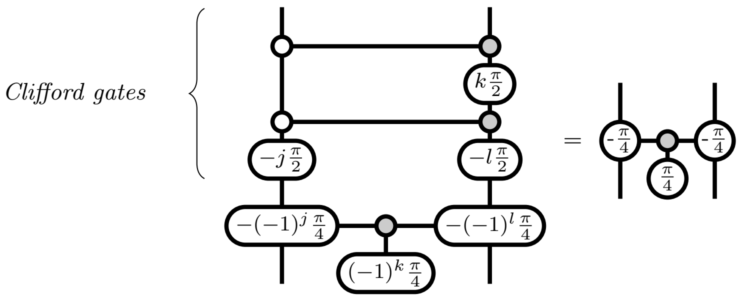
(b) By introducing another (classically controlled) Clifford gate, show that we have a protocol that always produces a T gate. In other words, show that we can turn a $z_{\pi/4}$ state into a T using just free operations.

One can think of magic states as different kinds of currency that can be exchanged using free operations. To see this, consider another kind of magic state:

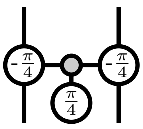
$p_\alpha :=$ 

(c) Show that we can produce a $p_{\pi/4}$ magic state using four $z_{\pi/4}$ magic states and free operations. Furthermore, show that this can be done only with Clifford gates and at most one Z ONB measurement.

(d) Show that, for any $j, k, l \in \{0, 1\}$, we have:



Using this fact (or otherwise), show that we can use a $p_{\pi/4}$ magic state and free operations to construct a controlled-S gate:

$CS :=$ 

It is not clear how we can use a $p_{\pi/4}$ state to get a $z_{\pi/4}$ state directly, but if we happen to already have a $z_{\pi/4}$ around, we can use it in the translation of $p_{\pi/4}$ to $z_{\pi/4}$, but then we get it back afterwards! This is a phenomenon called *catalysis* (cf. section 12.1.3 in the book).

(e) Show that one can convert a $p_{\pi/4}$ and a $z_{\pi/4}$ magic state into two $z_{\pi/4}$ magic states, using free operations.