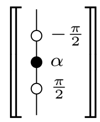
QDCS : Calcul quantique avancé et codes correcteurs

Alain Couvreur & Renaud Vilmart

TD 2 – Corrigé

1. Done in class.

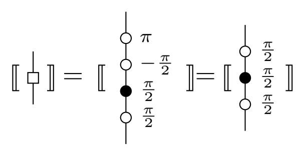
2. (a) After decomposing the black node as $HR_Z(\alpha)H$, we get (ignoring oerall scalars):



$= \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & e^{i\alpha}\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix} = \begin{pmatrix}1+e^{i\alpha} & -i(1-e^{i\alpha})\\ i(1-e^{i\alpha}) & 1+e^{i\alpha}\end{pmatrix}$. Factoring by $e^{i\alpha/2}$, and using $e^{i\alpha/2}+e^{-i\alpha/2} = 2\cos(\alpha/2)$ and $e^{i\alpha/2}-e^{-i\alpha/2} = 2i\sin(\alpha/2)$, we get $\begin{pmatrix}\cos(\alpha/2) & -\sin(\alpha/2)\\ \sin(\alpha/2) & \cos(\alpha/2)\end{pmatrix}$

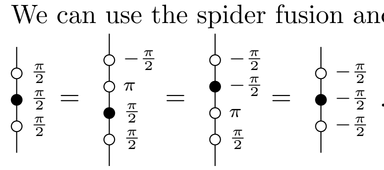
(b) I we use $\alpha = \frac{\pi}{2}$, the above matrix becomes $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$. It is not exactly H, but it can be corrected by multiplying the last column by -1, i.e. through right composition of $Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$:

$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$. Hence we have

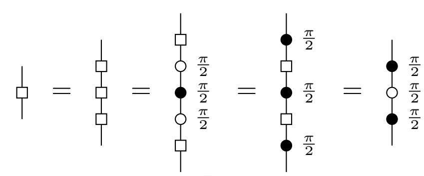


after spider fusion.

(c) We can use the spider fusion and the π-distribution to perform the following derivation:

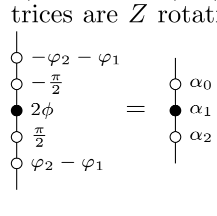


. For the colour-swapped version, we can use the fact that H is an involution, and the change-of-basis axiom:



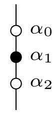
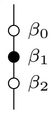
. Finally, we could do exactly the same but starting from the diagram with $-\frac{\pi}{2}$ phases everywhere, and get the same result but with all phases multiplied by -1.

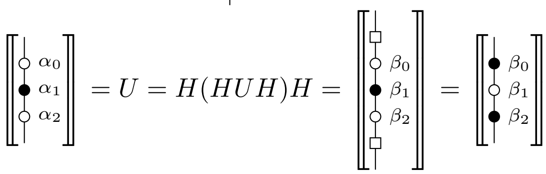
(d) We recall from the first TD that any 1-qubit unitary could be written $\begin{pmatrix}e^{i\varphi_1}\cos(\phi) & -e^{-i\varphi_2}\sin(\phi)\\ e^{i\varphi_2}\sin(\phi) & e^{-i\varphi_1}\cos(\phi)\end{pmatrix} = \begin{pmatrix}\cos(\phi) & -e^{-i(\varphi_2+\varphi_1)}\sin(\phi)\\ e^{i(\varphi_2-\varphi_1)}\sin(\phi) & e^{-2i\varphi_1}\cos(\phi)\end{pmatrix}$ up to colinearity. We can decompose it as $\begin{pmatrix}1 & 0\\ 0 & e^{i(\varphi_2-\varphi_1)}\end{pmatrix}\begin{pmatrix}\cos(\phi) & -\sin(\phi)\\ \sin(\phi) & \cos(\phi)\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & e^{-i(\varphi_2+\varphi_1)}\end{pmatrix}$. Notice that the leftmost and rightmost matrices are Z rotations, and the middle one is a rotation from 2a. It can hence be represented by

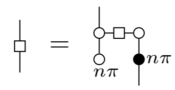
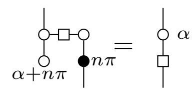


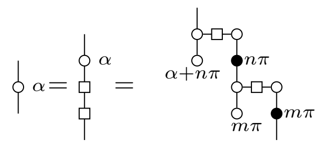
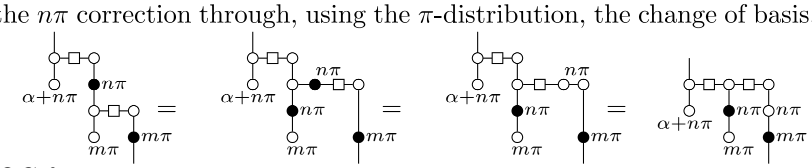
with $\alpha_0 = -\varphi_2-\varphi_1-\frac{\pi}{2}$, $\alpha_1 = 2\phi$ and $\alpha_2 = \varphi_2-\varphi_1+\frac{\pi}{2}$ after spider fusion.

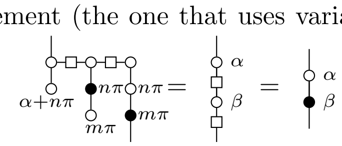
(e) $(U_1U_0)^\dagger(U_1U_0) = U_0^\dagger U_1^\dagger U_1 U_0 = U_0^\dagger U_0 = id$. Similarly $(U_1U_0)(U_1U_0)^\dagger = id$ so U_1U_0 is unitary.

(f) By composition of unitaries, the diagram  denotes a unitary U. By involution of H, we have $U = H^2UH^2 = H(HUH)H$. Again by composition of unitaries, HUH is unitary, so by 2d it can be decomposed as  . Putting everything back together, we get:

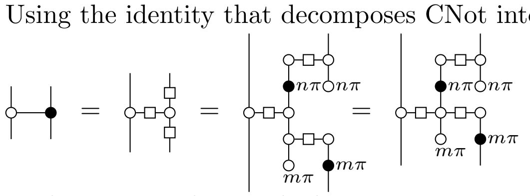


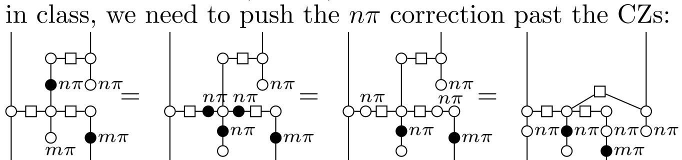
3. (a) We recall the MBQC decomposition of H seen in class:  . If instead on measuring in $\{|\pm\rangle\}$ we measure in $\{|\pm_\alpha\rangle\}$ we get  .

(b) Again, we use the H involution, as follows:  . Though physically allowed, this is technically not in MBQC-form as given in class, as a measurement (the one with variable n) is performed *in-between* entanglements of qubits (used to build the graph-state). We can however push the $n\pi$ correction through, using the π-distribution, the change of basis, and the spider fusion rules:  . This is now in proper MBQC-form.

(c) Performing the second measurement (the one that uses variable m) in the $\{|\pm_\beta\rangle\}$ basis, we can convince ourselves that we get:  .

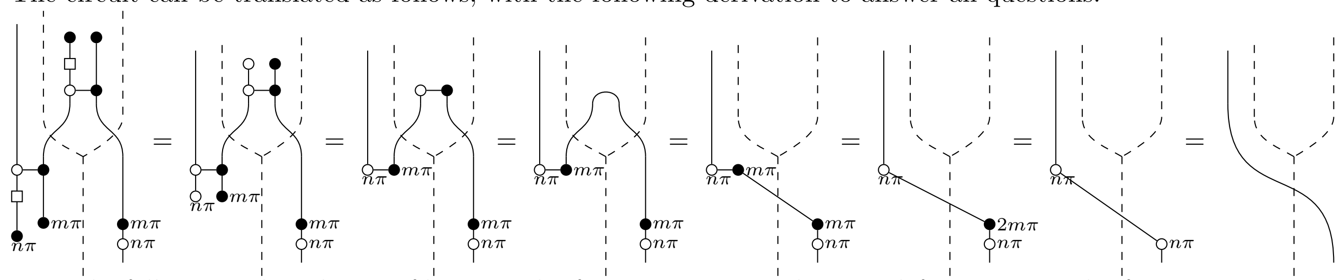
(d) Using the identity that decomposes CNot into CZ, and replacing H by its MBQC-form, we get:

 . Again this is not exactly in the MBQC form seen in class, we need to push the $n\pi$ correction past the CZs:

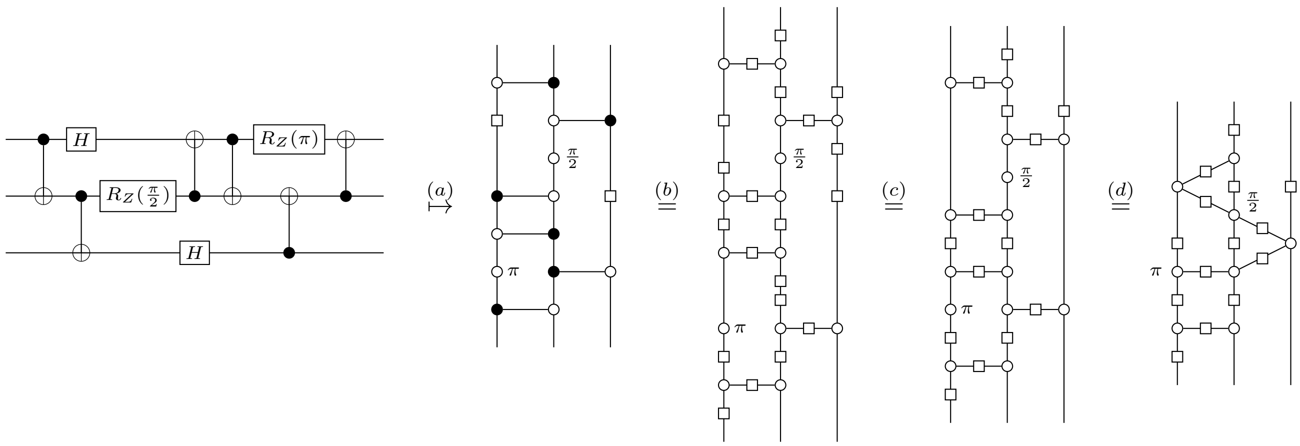
 . This is now indeed in the form of an open graph state, followed by a sequence of two measurements.

(e) By universality of the gate set $\langle \text{CNot}, H, R_Z(\alpha)\rangle$, any unitary can be decomposed as a composition of them. Each of them can be implemented in MBQC, and composition of processes in MBQC form gives a new process, which is in MBQC form, sort of. We still have the "problem" of having measurements before CZs that constitute the graph state of subsequent gates. However it can be proven, using π-distribution, change of basis and spider fusion, that an X gate (one of the two considered corrections) applied on an input of an open graph state can be pushed, resulting in Z gates (the other possible corrections) on outputs that are neighbours of the input. The situation is easier with Z gates, which simply commute with CZ gates.

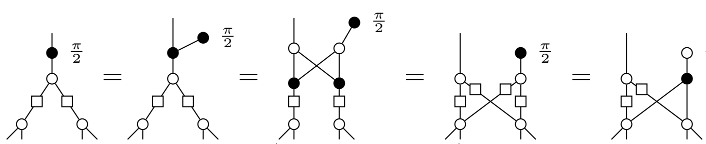
4. The circuit can be translated as follows, with the following derivation to answer all questions:

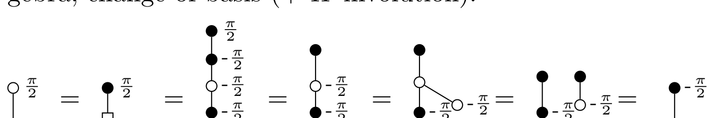


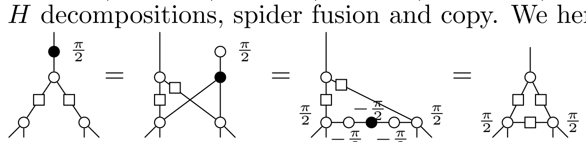
using the following rules: change of basis; spider fusion; 0-rotation; diagram deformation; spider fusion; 0-rotation; bis repetita.

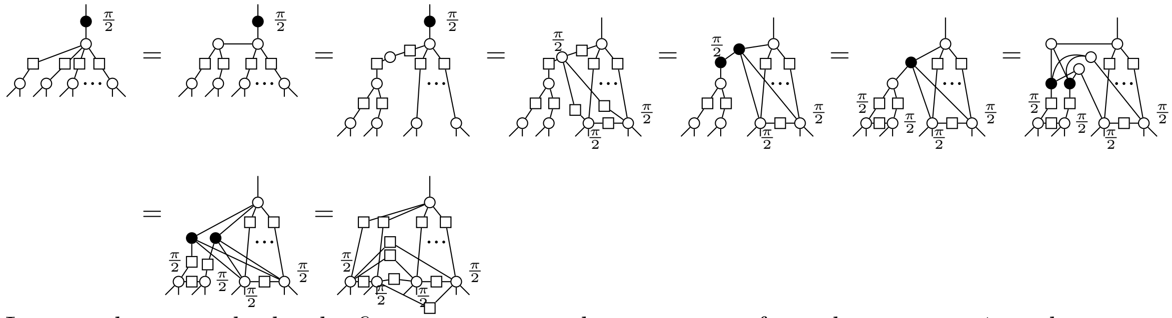
5. 

6. (a) The case $n = 1$ is simply a change of basis (with an H-involution)

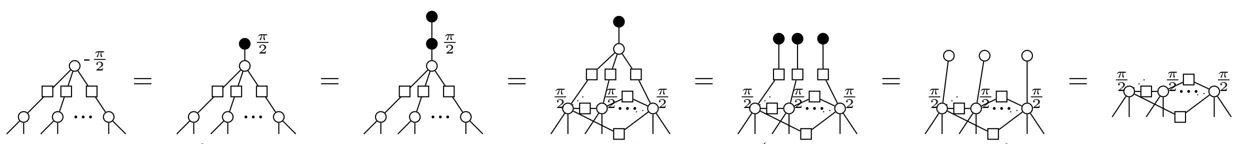
(b)  using in turn: spider fusion, bialgebra, change of basis (+ H involution).

(c)  using the change of basis, one of the H decompositions, spider fusion and copy. We hence get:

 using 6b, 6c, spider fusion and a H decomposition.

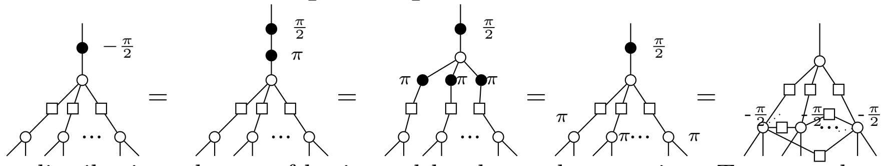
(d) 

Let us take a step back: the first two steps are here to get us from the case $n+1$ to the case n, on which we can use the induction hypothesis. To do so, we use spider fusion, H involution and 0-rotation, creating an intermediary node. After applying the induction hypothesis, we get a clique on the right part, with the left intermediary node linked to all the bottom right white nodes. We then change the colour (with the change of basis) of the intermediary node, so we can use the $n = 2$ case. It then remains to remove the intermediary node, which is possible using the generalised bialgebra rule from 1. Recall that it creates a complete bipartite graph between "white-linked" wires and "black-linked" wires. We then use the change of basis and the spider fusion to get to the final form. At the end, all bottom nodes are linked to the top one, we had a clique on the right, with the two left nodes connected together and each connected to all nodes of the clique on the right. This clique together with the two left nodes hence also form a clique.

(e) 

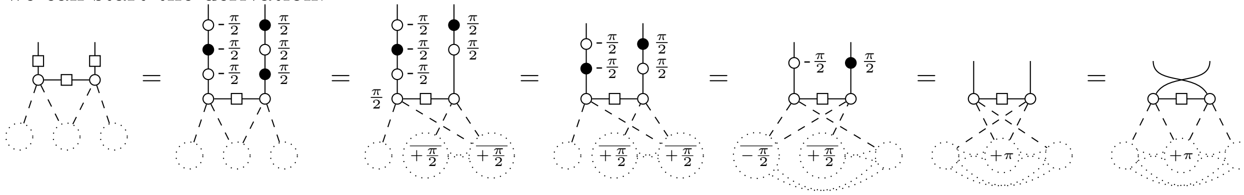
using 6c, spider fusion, local complementation, generalised copy (also a special case of the generalised bialgebra 1) and change of basis.

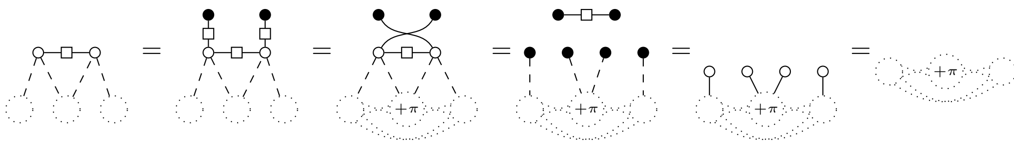
(f) We could redo the whole derivation with negated angles, or we can deduce it from the local complementation using $-\frac{\pi}{2} = \pi + \frac{\pi}{2}$ together with properties of the π-phase:

 using spider fusion, π-distribution, change of basis, and local complementation. To prove the previous identity with negated phases, it suffices to adapt the proof with a colour-swapped 6c.

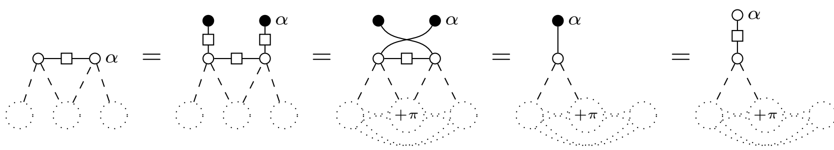
Side note: we call this operation local complementation, because when taken as a graph, we are complementing the neighbourhood of a node (the top one in our case), i.e. we add an edge between each pair of neighbours of the node if they are not connected, and we remove the edge if they were already connected. This last step can be seen as applying the Hopf law from 1 to remove pairs of edges between nodes.

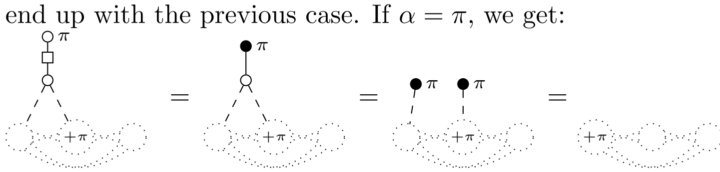
7. (a) We are going to use the following notations to deal with the blobs: When the subgraph that is the blob is complemented, we note it: $-$, when all the nodes in the blob get an additional angle of α, we note it: $+\alpha$, and when we complement two blobs (i.e. we add an edge mod 2 between each pair (u, v) where u is from the first blob and v from the second), we write: . Now we can start the derivation:



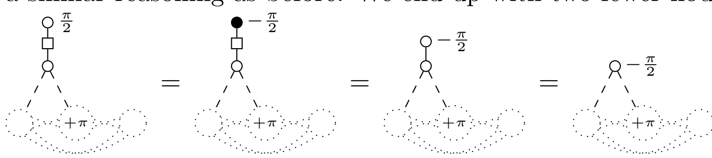
(b)  .

We performed pivoting, then generalised copy, then change of basis (recall that dashed lines represent H-edges), and finally spider fusion (because there the top white nodes are directly linked to the white nodes in the blobs).

(c)  . So far we have only removed edges, but no white nodes. However, the special cases $k\frac{\pi}{2}$ can simplify. First if $\alpha = 0$, we end up with the previous case. If $\alpha = \pi$, we get:

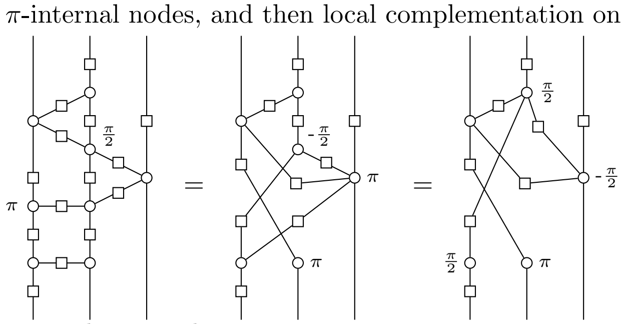


using the π-copy (generalised) and a similar reasoning as before. We end up with two fewer nodes. Next, if $\alpha = \frac{\pi}{2}$:

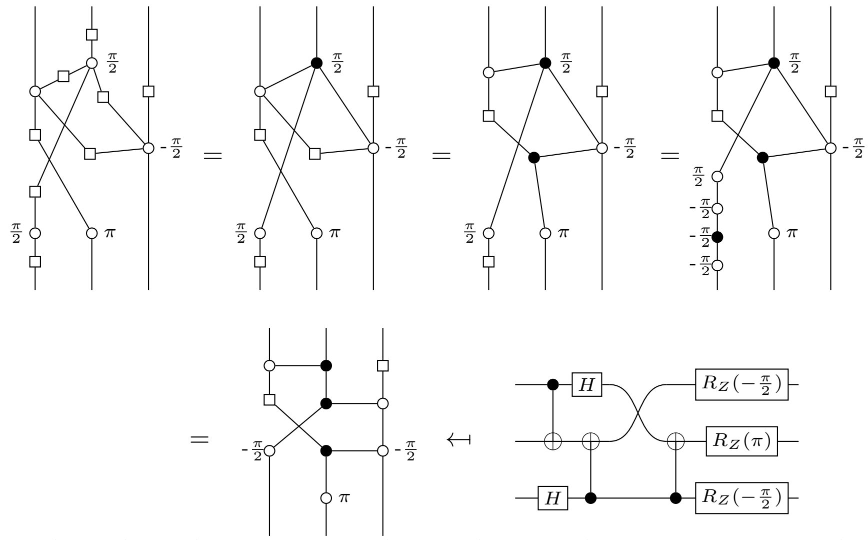


using 6c, change of basis and spider fusion. The case $\alpha = -\frac{\pi}{2}$ is similar. In these two cases, we end up with one ewer node.

8. (a) You can play around with the rules, but you should notice that what works well for diagram reduction, is the application of the two previous identities on *internal nodes*, i.e. nodes that are only linked to other nodes through H-edges. Hence, applying first pivoting on the two 0 and π-internal nodes, and then local complementation on the internal $\frac{\pi}{2}$-phase, we end up with:



From there, in this case, we can recover a circuit. We could try to translate patterns as quantum gates directly, which would give a decent result. Instead I am going to do a few on-the-nose simplifications:



In the end, we do get a circuit that implements the same operator as the one we started with in 5, but which is simplified.

(b) First, any ZX-diagram can be put in "graph-like" form, using the procedure of 5. Then, using pivoting on any adjacent pair of 0- or π-phase internal nodes reduces the node count by 2. More generally, any internal node with phase 0 or π can be removed by pivoting with an adjacent node (whatever its phase), and any internal node with phase $\pm\frac{\pi}{2}$ can be removed by local complementation. Since Clifford diagrams are only constituted of nodes with phase a multiple of $\frac{\pi}{2}$, all internal nodes will be removed with this procedure. What remains afterwards is a graph state where each node is either connected to an input or an output (or both), and potentially with some binary node between the boundary and the vertex.
Let n be the number of nodes in the graph state. Each rewrite step is bounded by $O(n^2)$ graph operations (indeed complementation scales quadratically in the worst case), and we have at most n of those, so we get an overall complexity of $O(n^3)$. The size of the resulting diagram is bounded by $O(b^2)$ with b the number of boundaries of the diagram, and the intermediary diagrams stay bounded by $O(n^2)$. Importantly, the size of the result does not depend on n but only on b.
All in all, Clifford diagrams can be put in (pseudo) normal form in polynomial time, and this normal form is itself of polynomial size.