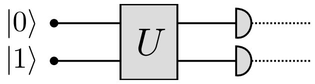
Seminar: Disentangling quantum matter with quantum information theory - Prof. Dr. D. Gross, Prof. Dr. S. Trebst - University of Cologne - July 25, 2016

Entanglement as a Resource for Quantum Computation

Jan Attig - jattig@thp.uni-koeln.de

Quantum gate model

The quantum gate model is the most common description of a quantum computer. It is derived by translating all components of a classical computer into quantum objects.

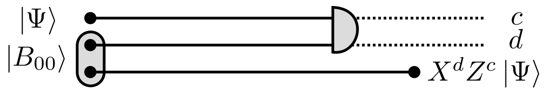


For any computation, qubits (e.g. spins, in general quantum two-level systems) are evolved unitarily in time by so-called (quantum-)gates. These gates can act on many qubits and are the components determining the calculation. To obtain an output, the qubits are being measured.

Teleportation based quantum computation

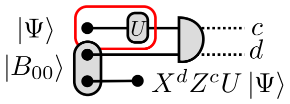
Teleportation

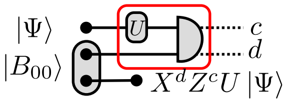
To teleport a qubit $|\Psi\rangle$, one has to perform a joint measurement with one qubit of a Bell basis state $|B_{00}\rangle$ in a two-particle measurement in the Bell basis. After the measurement, the leftover qubit from the Bell state spin will remain in the state $X^dZ^c|\Psi\rangle$ and can be transformed to the desired state $|\Psi\rangle$.



Teleportation of quantum gates

If one wants to apply a gate U to a qubit and teleport the result (left figure), one can instead let the gate act on the measurement and teleport the qubit by the modified measurement (right figure). The advantage of this procedure is to implement the gate solely by rotation of the measurement basis.





This process can be generalized for multi-qubit gates and thus lays the basic principle to build a quantum computer without unitary time evolution.

Adaptive measurements

To apply a chain of gates via teleportation, one has to deal with the Pauli-prefactors Z^cX^d. Instead of applying a gate $\mathbf{V}$ after applying another gate $\mathbf{U}$, one uses $Z^cX^d\mathbf{V}Z^{-c}X^{-d}$ with c and d known from the previous Bell measurement. In this way one obtains the following desired state:

$$\begin{aligned} &Z^{c'}X^{d'}(Z^cX^d\mathbf{V}Z^{-c}X^{-d})Z^cX^d\mathbf{U}|\Psi\rangle \\ =\ &Z^{c'}X^{d'}Z^cX^d\mathbf{V}\mathbf{U}|\Psi\rangle \end{aligned}$$

Building a universal quantum computer

Looking closer on the process of two-qubit measurements, one can decompose these into a two-qubit entanglement gate and single-qubit measurements. By grouping all entanglement gates and Bell states while leaving the single-qubit measurements untouched, one obtains the so-called *One-way quantum computer*. On this machine all quantum codes can be implemented as single-qubit measurements in some basis.

Such computer can only be used once since running a quantum code means performing measurements on an entangled quantum ground state. Afterwards a new state has to be used to run the next code.

Conclusions

Conclusions to be drawn from the existence of a quantum computer based on local adaptive measurements:

1 - The power of a quantum computer originates in the *entanglement* between different qubits, unitary time evolution can be substituted by measurements

2 - A possible *experimental realization* of a quantum computer can be achieved by putting spins in optical lattices

3 - Classical algorithms on classical computers *cannot efficiently calculate* local measurements on entangled groundstates, otherwise they would simulate a quantum computer

References

[1] Richard Jozsa. An introduction to measurement based quantum computation. *NATO Science Series, III: Computer and Systems Sciences. Quantum Information Processing-From Theory to Experiment*, 199:137–158, 2006.