Introduction to Quantum Computing

Einar Pius (e.pius@sms.ed.ac.uk)
Vedran Dunjko (vd51@hw.ac.uk)

May 1, 2012

Dear students, it was our pleasure and an honour to give the Introduction to Quantum Computing course at your University. Being students ourselves, any feedback from you on what you thought of the course would be greatly appreciated - praise us, scold us, all will be taken in good will! In the case you have any course related questions feel free to contact us via email.

At your University you also have the opportunity to contact our local host prof. Dominique Unruh, who is an excellent interdisciplinary scientist bridging between the classical and quantum worlds with ease. He can help guide you in case you catch the quantum fever and realise it is the funnest research you could ever do!

Unfortunately, this being a course and all, we are obliged to give you additional assignments to help build up the grade you already earned through the lecture attendance and the discussions/questions.

Below you will find the list of assignments, and we hope they will not be too painful.

You are allowed to/should:

1. Use any and all literature at your disposal. We will give you hints where to locate the information you will need to answer the questions, and we chose it from the public domain. However Nielsen and Chuang's Quantum Computation and Quantum Information [1] is still a very useful resource if you can get your hands on it.
2. You are GREATLY encouraged to discuss your solutions and the problems themselves with the colleagues who attended the course along side you, your professors, friends, moms and dads, Santa, whoever you want. Working in teams is a very important and useful skill.
3. You can ask us anything you wish about the questions, which includes the questions of the type 'I think the solution is this, is this right?'. But, even if you make a mistake in your final submission, we will point you in the right direction, and give you an extra try. For us, it only matters you understand the answers at the end of the story... Please, do not overuse the emailing just for gags!
4. While teamwork is encouraged, please submit individual solutions, preferably restated in your own words. We would appreciate this.
5. The solutions should be emailed to us, and we accept (in order of preference):
   (a) LaTeXgenerated pdf
   (b) any other LaTeXgenerated format, including source
   (c) pdf scans of hand written solutions (if you have better penmanship than us!)
   (d) any format in the public domain (open source)
   (e) any format not in the public domain which we can convert to something reasonable

We will give you the exact deadlines for the submissions as soon as the University forwards them to us, but you shouldn't be stressed about this, we will be as flexible as possible.

Assignments

Following are the homework assignments. Each student should choose any three out of the five questions to answer and send the answers to either of us by email.

1. Approximate Universal Quantum Computing (QC)

In the Quantum world, computational universality is defined as the ability to implement any unitary transformation on a quantum register containing the input quantum state. As we have mentioned, a curious and very important property is that to achieve (exact) universality one only needs to perform sequences of a single 2-qubit gate (CNOT) and any arbitrary single qubit unitary. However, asking for the ability to perform a *continuum* of single qubit gates is a bit unrealistic. Luckily, it turns out, a fixed finite set of single qubit gates is enough, as using them suffices for *approximate* universality - we are capable of approximating any single qubit unitary to arbitrary precision, starting from a small set.

Stop and think for a second. Is this enough to consider approximate universality sufficient for useful quantum computation? Recall, QC is only interesting if it is *efficient*. Would QC be feasible even in theory if the approximation procedure itself took exponentially many gates in terms of the desired levels of the *quality* of the approximation? Reflect on this topic and state the relevant theorem which resolves the issue with a brief explanation of what the theorem actually means and what the consequences on QC are in your opinion. The relevant information can be found in the textbook [1], chapter 4.5.3 and Appendix 3, also presented in an algorithmic form in the paper [2].

2. Optimality of Grover's algorithm

In the course we talked about the Grover's algorithm and mentioned its optimality at $O(\sqrt{N})$ queries. Imagine for a second that there existed quantum algorithm, a *supergrover*, on quantum computers which solved the same problem as Grover but in $O(\log(N))$ queries. What consequences would such a result have on the relationship between the classical and quantum complexity classes? In particular what could we say about the classical class NP and BQP augmented with the *supergrover*?

Clearly, the optimality of Grover's algorithm is an important result. Can you explain the basic idea of the proof of optimality, without the need to go into technical details?

For the first question you should look up the original paper by Lov Grover [3], whereas the latter question is explained in simple terms in [4], section 2. However, both questions are also addressed in the textbook [1], chapter 6.

3. Quantum Counting

During the course we presented the Grover's search algorithm for finding one of M solutions amongst N elements. The bounds for the number of queries needed were given assuming M is known. We mentioned that the number of solutions can be found efficiently (in N) using the quantum counting algorithm. The quantum counting makes use of the Grover's iterations and Quantum Phase Estimation, both of which were covered in the course. Describe the basic idea of quantum counting in simple terms and give the algorithm to estimate the number of solutions for the Grover's search algorithm. The algorithm can be found in chapter 6.3 in the textbook [1] or in the paper [5] section 4.

4. From Measurement Based Quantum Computing to Quantum Circuits

In this course we have covered the basics of two distinct computational models capturing the power of quantum computers: Quantum Circuits (QCirc) and Measurement-based Quantum Computation (MBQC).

There is a simple way to translate computations defined in the MBQC model to quantum circuits, which still uses ancillary qubits. Explain briefly how this works, perhaps accompanied with a short example. The required information (and a lot more!) can be found in the paper [6] (section 7.2) and related information can also be found in the paper [7]. Can we translate MBQC to circuits as well?

5. Grant Proposal

'Selling' your ideas is crucial in the life of a scientist. Imagine for a second you are the principal investigator of a very capable group of experimentalists and theorists working on Quantum Computing. You are pitching the importance of Quantum Computing to a group of investors who are (as it is often the case) clueless about the topic. Write a short (0.5 page) grant proposal explaining what amazing things one could do with quantum computers in theory and practice alike, justifying your request for an obscene amount of money.

In such 'blue skies' pitches use the following rule: it is more important to be interesting than correct or accurate. Since you are actually pitching to us, we add additional guideline: creativity and humour is a bonus!

References

[1] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, January 2000.

[2] Christopher M. Dawson and Michael A Nielsen. The Solovay-Kitaev algorithm. May 2005. http://arxiv.org/abs/quant-ph/0505030.

[3] Lov K. Grover. A fast quantum mechanical algorithm for database search. May 1996. http://arxiv.org/abs/quant-ph/9605043.

[4] Christof Zalka. Grover's quantum searching algorithm is optimal. *Physical Review A*, 60(4):2746–2751, October 1999. http://arxiv.org/abs/quant-ph/9711070.

[5] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum Counting. May 1998. http://arxiv.org/abs/quant-ph/9805082.

[6] Anne Broadbent and Elham Kashef. Parallelizing quantum circuits. *Theoretical Computer Science*, 410(26):2489–2510, 2009. http://arxiv.org/abs/0704.1736.

[7] Vincent Danos and Elham Kashefi. Determinism in the one-way model. *Physical Review A*, 74(5):052310, November 2006. http://arxiv.org/abs/quant-ph/0506062.