Some revision advice

**Bookwork:** exam questions in this course often have a substantial bookwork component. You should be able to clearly state definitions given in the course, and give an account of the steps in principal algorithms, and sketch proofs of the results in the lecture notes (stating clearly without proof, ingredients from other areas of mathematics that are used), except anything marked ‘optional’.

In addition to any part of the lecture notes that’s not marked ‘optional’, all exercise sheets are examinable too, except Sheet 1 Q7 and Sheet 3 Q3.

**Relevance of past exam papers:** the topics of HSP and HHL are new to the course for this year but PhEst, AmplAmpl and HamSim have all been lectured before. Not all exam questions from previous years are relevant - only those on PhEst, AmplAmpl and HamSim. Previous years also included other topics not done this year (measurement based computing, lower bounds on query complexity). Also, previous years included detailed exposition of Grover’s and Shor’s algorithms which are now in the Part II course (and for us are prerequisite starting material for AmplAmpl and HSP respectively).

Many of the relevant questions from past papers have already been taken/adapted for use on this year’s exercise sheets.

If you have any question/doubt about possible relevance of any past exam question, please ask (email) me.

Some revision questions

*Please also bring any questions you may have to the class, for possible discussion!*

(1) Explain how the Quantum Fourier transform QFT on a finite abelian group $G$ is constructed, and show that it is unitary. You may use results from group representation theory without proof but they should be clearly stated. Construct explicitly the QFT for $G = \mathbb{Z}_N$.

Suppose we are given an oracle for a function $f : \mathbb{Z}_N \to \mathbb{Z}_N$ which is promised to be periodic and 1-to-1 in each period. Outline how the period may be determined with any high constant level of probability $1 - \epsilon$ ($\epsilon > 0$) by use of only $O(\log \log N)$ queries to the oracle.

(2) For any matrix $M$ and analytic function $f(x) = \sum_{n=0}^{\infty} a_n x^n$, $f(M)$ is defined by $f(M) = \sum_{n=0}^{\infty} a_n M^n$. Show that for any invertible matrix $A$, $f(AMA^{-1}) = Af(M)A^{-1}$.

Suppose now that $f$ is a function such that for a given unitary $U$, $f(U)$ is unitary too. Using phase estimation or otherwise show how we may implement the operation $f(U)$ on any given state $|\alpha\rangle$, in terms of the gates controlled $U$, controlled $U^\dagger$, and other gates that are independent of $U$. You may ignore any issues of precision, and assume that all needed quantities may be adequately represented in $O(n)$ bits.

(3) State the amplitude amplification theorem (thereby also introducing the ingredients needed in its statement).

Let $Q$ be a positive integer and $m$ be an integer such that $2^m > Q$. Suppose we are able to implement any 1-qubit gate and also the $CX$ gate. You may assume that this total gate set is an exactly universal set (i.e. it suffices to represent any unitary exactly via a circuit of its gates).
Using amplitude amplification, show how the state $|\xi\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} |k\rangle$ may be constructed exactly and with certainty, in a register of $m$ qubits (with integers being represented via their binary representations), using a circuit of 1- and 2-qubit gates.

**(4)** (Review the steps of the HHL algorithm and conditions needed for it to apply).

State the Chernoff-Hoeffding bound as applied to estimate the probability value $p_1$ of a binary random variable (with values 0,1) to within $\pm \epsilon$ and with any constant level of probability $C$.

In the theory of mean-variance analysis in financial portfolio management we need to compute (actually minimise) an expression of the form $\Omega = w^T \Sigma^{-1} w$ where $w = (w_i) \in \mathbb{R}^N$ are weights for portfolio assets and the matrix $\Sigma$ of size $N \times N$ is the covariance matrix of asset return rates. Classical algorithms involve direct calculation of $\Omega$ and take $\text{poly}(N)$ time. Write $n = \text{poly}(N)$. Assume now that $\Sigma$ is sparse, $W^2 = \sum_i w_i^2$ can be computed in $\text{poly}(n)$ time, and the state $|\hat{w}\rangle$ of $n$ qubits with amplitudes $\hat{w}_i = w_i/W$ can be implemented in $\text{poly}(n)$ time. Show how the HHL algorithm enables $\Omega$ to be computed to accuracy $\epsilon = O(1/\text{poly}(n))$ with any constant level of probability $C$, exponentially faster than the classical time above. You may assume that any other conditions needed for the HHL algorithm to apply are satisfied (but they should be stated).