QC revision questions

Otto Pyper

1. What is the time complexity of the fastest classical factoring algorithm?
2. What is the time complexity of Shor's algorithm?
3. Describe the Quantum Periodicity Determination Problem.
4. How is the quantum orcale represented as a gate?
5. What is the query complexity of an algorithm?
6. Fastest possible classical periodicity algorithm?
7. Describe the Quantum Period Finding Algorithm.
8. How does QFT act on a state $|x\rangle$?
9. State the Coprimality Theorem.
10. State the 'Probability Lemma'.
11. QFT maps which basis to the standard basis? Describe the states.
12. Describe the eigenvalues of the above basis states.
13. What is $[QFT]_{k\ell}$?
14. Describe the Hidden Subgroup Problem.
15. What time complexity do we aim for in the HSP?
16. What form of a solution do is acceptable for HSP?
17. Express periodicity as an HSP.
18. Express the Discrete Logarithm Problem as an HSP.
19. Describe the Graph Isomorphism Problem.
20. Express the Graph Isomorphism Problem as a non-Abelian HSP.
21. Who found a quasi-polynomial time classical algorithm for GI, when, and what is its runtime?
22. Describe another problem that can be rephrased as an HSP.
23. What is a representation of G? What property does a represenation have when G is abelian?
24. Prove that any value $\chi(g)$ is a $|G|^{\text{th}}$ root of unity.
25. State (and prove *) Schur's Lemma (Orthogonality).
26. Enumerate the different representations of G.
27. What is the trivial irrep?
28. What are the shift operators?

29. What is the state $|\chi_k\rangle$?
30. How are these states acted on by shift operators? Prove this.
31. What is QFT? [Again.]
32. What is $[QFT^{-1}]_{gk}$?
33. What is $[QFT]_{kg}$?
34. What is $QFT|G\rangle$?
35. What is QFT on $G = \mathbb{Z}_M$?
36. Describe the Quantum Algorithm for Finite Abelian HSP.
37. What is the output for the above algorithm?
38. How do we use said output to determine the hidden subgroup?
39. For non-abelian G, what is the problem with the QFT construction?
40. What is an irreducible representation for a non-abelian group G?
41. What is a complete set of irreps?
42. State the generalisation of the previous representation theorem for non-abelian groups.
43. How is QFT defined on such a G?
44. Why does the same algorithm not work for non-abelian HSP?
45. How can we modify it to obtain *some* information about K?
46. How efficiently must we be able to implement QFT to use it here?
47. Under what circumstances does efficient implementation of QFT suffice to solve HSP?
48. For general non-abelian HSP, how many random coset states suffice to determine K?
49. Why is this not enough to solve HSP?
50. What is the Phase Estimation problem?
51. What extra gates do we need for PE? How do they act?
52. Given U as a formula or circuit distribution, how can we implement C-U?
53. What further information do we need to control U if it is given as a black box?
54. Why is this further information necessary?
55. Given this information, draw a diagram to implement C-U.
56. Now what gate do we actually need?
57. Construct this gate with a diagram.
58. How does this gate act on $|\xi\rangle = |v_\varphi\rangle$?
59. Describe (with the aid of a diagram) the Quantum Phase Estimation Algorithm.
60. State and prove Theorem (PE).
61. How many lines do we need to calculate φ to accuracy m bits with probability $1 - \eta$?
62. How does implementing $C - U^{2^k}$ impact the algorithm?

63. What happens if you do PE to an arbitrary state $|\xi\rangle$?
64. What is the precision issue in the above process?
65. What is the reflection operator $I_{|\alpha\rangle}$?
66. How does $I_{|\alpha\rangle}$ interact with unitaries?
67. How does this generalise to a k-dimensional subspace $A \subseteq \mathcal{H}_d$ with onb $|a_i\rangle : i \leq k$?
68. That is, define P_A and I_A.
69. Describe the context for using Grover's Algorithm. Which problems are these closely related to?
70. Write down the Grover iteration operator and describe its terms.
71. State Grover's Theorem (1996).
72. Describe Grover's Algorithm.
73. Approximately how many iterations are required in the algorithm?
74. What sort of speed-up does Grover's Algorithm give on the classical case?
75. Write down the generalisation of the Grover operator used in AA.
76. State and prove the Amplitude Amplification Theorem.
77. Describe the Amplitude Amplification Algorithm, including the number of iterations required.
78. What is the approximate accuracy of the AA process?
79. Implementation of which gates are sufficient for AA?
80. What conditions are sufficient to be able to compute I_G? Prove this.
81. How is $I_{|\psi\rangle}$ implemented?
82. How does AA affect the distribution of $|\psi\rangle$ restricted to the good subspace?
83. What is the above particularly useful for?
84. How can AA be made exact?
85. Describe how AA solves Grover search with one or more 'good' items.
86. Describe how AA gives a square-root speedup of general quantum algorithms.
87. Describe the use of both AA & PE in Quantum Counting.
88. Write down the time-independent Schrodinger equation (in units where $\overline{h} = 1$) and its solution.
89. What is the Hamiltonian Simulation problem?
90. What the the operator norm/spectral norm of operator A?
91. What properties does it have?
92. What is meant by '$\tilde{U}$ approxiamtes U to within ε'?
93. What constraints are we aiming for in HamSim?
94. Define a k-local (Hamiltonian) operator.
95. Why are we able to work better with k-local Hamiltonians?
96. Write down the Ising Model operator.

97. Write down the Heisenberg Model operator.
98. State the Solovay-Kitaev Theorem.
99. State and prove the lemma describing error accumulation under the operator norm.
100. Prove that for any k-local H with commuting H_js, e^{-iHt} can be efficiently approximated.
101. State and prove the Lie-Trotter Product Formula.
102. What is the overall circuit size for k-local HamSim?
103. How is this changed if we instead want to use a standard universal set?
104. What levels of complexity in t can be achieved by refining Lie-Trotter?
105. What is HHL used for?
106. What type of solution do we aim to output?
107. What are some common applications of HHL?
108. What is the best known classical runtime for solving systems of linear equations?
109. What is the condition number of a matrix?
110. State an intermediate issue immediately faced by trying to compute properties of large systems.
111. State three conditions on a matrix A necessary for applying HHL, defining any terms.
112. Define 'row-sparse' and 'row-s-sparse'.
113. Define 'row-computable'.
114. State the Hamiltonian Simulation Property.
115. Give an example of a class of matrices which are row-sparse & row-computable.
116. State the conditions on b required for HHL.
117. State the conditions required on M for efficient computation of $x^\dagger M x$.
118. How do you get around one of the above conditions failing?
119. What is the best-known classical runtime achieving the same output as HHL?
120. What is the runtime of HHL to produce output state within ε of $|\hat{x}\rangle$?
121. In the regime with $\varepsilon = 1/(\mathrm{poly}(\log N))$, how does HHL compare to classical runtime?
122. Describe the HHL algorithm, including how AA can be used to improve runtime.
123. State the Chernoff-Hoeffding bound.
124. How can PE be modified to give improved accuracy?
125. What is the worst source of accuracy in HHL?
126. Which method can be used to replace this? What else can this method be used for?
127. Define weak simulation of QC.
128. Define strong simulation of QC.
129. Demonstrate that efficient simulation is possible if we have a product state promise.
130. Define the n-qubit Pauli group, $\mathcal{P}_n$.

131. Define a Clifford operation, and the Clifford group.
132. How does the Clifford group relate to the Pauli group?
133. State some important applications of the Pauli group & Clifford group.
134. Give five examples of Clifford operators.
135. State a theorem characterising all Clifford circuits.
136. Define 'Clifford computation'.
137. State the Gottesman-Knill Theorem (variant).
138. An alternative proof of GK uses which formalism? What was it introduced for?
139. Prove the GK Theorem.
140. Define Adaptive and Non-adaptive Clifford circuits.
141. State a theorem about adaptive/non-adaptive Clifford circuits.
142. Prove (roughly) the non-adaptive case (demonstrate the critical idea).
143. Define the T-gate.
144. State a fact about T-gates and Clifford circuits.
145. Define a 'magic state' $|A\rangle$.
146. Implement a T-gate using an adaptive Clifford circuit and $|A\rangle$.
147. Explain how this proves the seconnd part of the theorem.
148. Give a full characterisation of adaptive/non-adaptive Clifford circuits.
149. State an ingredient that elevates classically limited power to full quantum power.
150. Why is this potentially alarming?