

Here is a fragment of a study guide for Exam B. Disclaimers: It does not necessarily sample from every topic that might be on our exam. Some of the questions are obviously incomplete. I have not attempted to balance them for difficulty. In short, this document does not constitute any kind of promise about the exam.

A. Here are routine calculations and definitions.

A.A. Given an  $N \times N$  matrix  $A$  and an  $M \times M$  matrix  $B$ , compute  $A \otimes B$ . (On an exam, I would give you specific  $A$  and  $B$  — or not?)

A.B. Write out  $H^{\otimes 3}$ .

A.C. Suppose that you have a system of  $n + m$  qbits. Describe precisely how partial measurement of the last  $m$  qbits works. (By “precisely” I mean that an answer consisting of plain English and drawings is not sufficient. You’re going to need mathematical notation.)

B. Maybe there will be TRUE/FALSE/PUNT questions. Write two of these questions, while a friend writes a different two. Trade. Answer your friend’s questions and critique them. (Writing your own questions is one of the most intense ways to study for an exam.)

C. Here are some basic questions about Bernstein-Vazirani’s problem and algorithm.

C.A. What problem does the algorithm solve?

C.B. What is the running time of the algorithm?

C.C. What’s the deal with that upside-down CNOT explanation? What’s that all about?

D. Let’s talk about Simon’s problem and algorithm.

D.A. All of the quantumness of the Simon algorithm is in a certain subroutine. What does this subroutine do? I’m looking for interface, not implementation. That is, I want to know how the subroutine interacts with the rest of the algorithm, rather than how the internals of the subroutine work.

D.B. Okay, now tell me about the internals of the subroutine.

D.C. What is the expected running time of the Simon algorithm? You do not need to derive it mathematically, but do explain what the minimum running time is, and why the expected running time is larger than that.

E. Finally Grover.

E.A. In the original version of Grover’s algorithm, where we know that  $m = 1$ , what exactly is the problem? What is the classical running time? What is Grover’s quantum running time?

E.B. Suppose that we continue to know  $m$ . As  $m$  increases, does the problem get easier or harder? (A good answer is multifaceted.)

E.C. Give a practical application, in which  $m$  is known. What is the best classical running time (as far as you know)? Is Grover better or worse?