There are five pages including this cover page. You have 70 minutes. No notes, books, calculators, computers, etc. are allowed.

Some problems explicitly declare that no explanation is necessary. On all other problems, show your work, in as organized a manner as possible. Incorrect answers with solid work often earn partial credit. Correct answers without explanatory work rarely earn full credit. Perform as much algebraic simplification as you can.

You may cite without proof any result discussed in class, the assigned textbook sections, or the assigned homework.

Good luck. :)

Oh, and the following matrices were used in our 7-qbit error-correcting code.

$$\begin{aligned} M_0 &= X_0 X_4 X_5 X_6, \\ M_1 &= X_1 X_3 X_5 X_6, \\ M_2 &= X_2 X_3 X_4 X_6, \\ N_0 &= Z_0 Z_4 Z_5 Z_6, \\ N_1 &= Z_1 Z_3 Z_5 Z_6, \\ N_2 &= Z_2 Z_3 Z_4 Z_6. \end{aligned}$$

And $|0\rangle$ and $|1\rangle$ were encoded as

$$\begin{aligned} |\bar{0}\rangle &= 2^{-3/2}(I + M_0)(I + M_1)(I + M_2) |0000000\rangle, \\ |\bar{1}\rangle &= 2^{-3/2}(I + M_0)(I + M_1)(I + M_2) X^{\otimes 7} |0000000\rangle. \end{aligned}$$

And in the context of this code Y is defined as $Y = ZX$.

A. Fill in the blanks. No explanation is needed, as long as your syndromes are clear.

A.A. If U is an n-qbit gate, then controlled-U or cU is an ____________-qbit gate defined by

$$\alpha |0\rangle |\psi\rangle + \beta |1\rangle |\phi\rangle \mapsto \underline{\hspace{8cm}}.$$

A.B. The subroutine in Shor's algorithm outputs an integer y such that, with probability about 0.4, y is

____.

A.C. $\mathcal{O}$(____________) primitive gates are required to implement the n-qbit Fourier transform.

A.D. In this course (not necessarily other quantum theory courses), an *observable* is a matrix A such that

____.

A.E. A code for correcting single-qbit X, Y, or Z errors must have at least ____________ qbits.

A.F. In our 7-qbit code, if the error Y_2 happens, then the syndrome is ________________________.

A.G. If the error X_5 happens, then the syndrome is ________________________.

A.H. If the error Z_1 happens, then the syndrome is ________________________.

B. The quantum Fourier transform is the $2^n \times 2^n$ complex matrix U defined by $U_{kj} = 2^{-n/2} e^{i\pi(2/2^n)kj}$. Prove that U is unitary.

C.A. Regarding our 7-qbit error-correcting code, draw a circuit that measures N_1.

C.B. What is the 7-qbit gate $\bar{Z}$? Prove that $\bar{Z}\,|\bar{0}\rangle$ and $\bar{Z}\,|\bar{1}\rangle$ have the desired values.

D.A. Draw the circuit for the crucial quantum subroutine in Shor's algorithm. Label all inputs.

D.B. How does computing the period r of some $f(k) = b^k \bmod N$ help you factor N?