Phys 571 Quantum Computation **Fall 2009**

Homework Problem 1.2 **Due Thursday, September 3**
(10 points) **(at lecture)**

1.2 **Three-bit reversible classical gates.**

The most general three-bit classical gate can be written as

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longrightarrow \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \oplus M \begin{pmatrix} x \\ y \\ z \end{pmatrix} \oplus N \begin{pmatrix} yz \\ xz \\ xy \end{pmatrix} \oplus \begin{pmatrix} p \\ q \\ r \end{pmatrix} xyz \ ,$$

where M and N are 3×3 matrices, and all the constants and entries in the matrices can be either 0 or 1. Notice that a three-bit gate is specified by 24 binary parameters, giving $2^{24} = (2^3)^{2^3}$ gates, as required. We introduce a vector notation,

$$\mathbf{M}_j = \begin{pmatrix} M_{1j} \\ M_{2j} \\ M_{3j} \end{pmatrix} \qquad \mathbf{N}_j = \begin{pmatrix} N_{1j} \\ N_{2j} \\ N_{3j} \end{pmatrix} \qquad \mathbf{p} = \begin{pmatrix} p \\ q \\ r \end{pmatrix} \ ,$$

where the vectors $\mathbf{M}_j$ and $\mathbf{N}_j$ are the columns of the matrices M and N. In this problem we consider the restrictions imposed by requiring that the gate be reversible.

(a) *Show* that to be reversible, the three columns of M must be linearly independent or be the three nonzero vectors in a two-dimensional subspace.

Throughout the following, we will concentrate on the first of these cases; i.e., we will assume that the columns of M are linearly independent.

(b) *Show* that $\mathbf{p} = 0$. (Hint: Think in terms of the vectors $\mathbf{V}_1 = \mathbf{M}_2 \oplus \mathbf{M}_3$, $\mathbf{V}_2 = \mathbf{M}_1 \oplus \mathbf{M}_3$, $\mathbf{V}_3 = \mathbf{M}_1 \oplus \mathbf{M}_2$, and $\mathbf{V}_4 = \mathbf{M}_1 \oplus \mathbf{M}_2 \oplus \mathbf{M}_3$.)

(c) *Characterize* the seven classes of transformations that can be produced by the columns of N. [Hint: Think in terms of permutations of the vectors introduced in part (c).]

(d) *Show* how FREDKIN and TOFFOLI fit into your characterization from part (c).