Ph/CS 219, Fall 2003 **Quantum Computation** **Prof. Alexei Kitaev**	**Problem set #3** **Due Wednesday, November 24, 2004**

1. Positivity vs. complete positivity (10 points) This problem has been moved from the previous set to the current one.

Let $T : \mathbf{L}(\mathbb{C}^2) \to \mathbf{L}(\mathbb{C}^2)$ be a superoperator defined by the equations

$$TI = I, \qquad T\sigma_x = x\sigma_x, \qquad T\sigma_y = y\sigma_y, \qquad T\sigma_z = z\sigma_z, \tag{1}$$

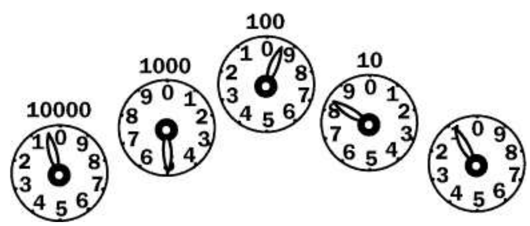
where x, y, z are some real numbers.

a) Find a necessary and sufficient condition for T being positive.

b) Find a necessary and sufficient condition for T being completely positive. **Hint:** Use the matrix representation.

2. Measurement decoding. (Strange as it sounds, this problem has important applications in quantum computation. We will use the algorithm in class!)

Some electricity meters look like this:



Apparently, it takes a special skill to read them quickly. Let us consider a mathematical version of the meter reading problem. We will assume that the dials have eight digits instead of ten and rotate at speeds that differ by powers of 2. The meter may roll over the highest value, which is equal to 1.

Let x be a real number *modulo* 1, i.e., we do not distinguish between numbers that differ by an integer. We may also think of x as a point on the circle that is obtained from the interval $[0,1]$ by identifying the points 0 and 1. However, the actual value of x is unknown. Instead, we are given individual dial readings $s_0, \ldots, s_{n-1} \in \{0,1,2,3,4,5,6,7\}$ such that

$$2^j x \in \left(\frac{s_j - 1}{8}, \frac{s_j + 1}{8}\right) \pmod 1 \qquad \text{for } j \in \{0, \ldots, n-1\}, \tag{2}$$

where the notation $(a,b) \pmod 1$ stands for the interval from a to b on the circle. Assuming that the data are consistent, we need to find a number $y = \overline{.y_1 \ldots y_{n+2}} = \sum_{j=1}^{n+2} 2^{-j} y_j$ (where $y_j \in \{0,1\}$) such that

$$x - y \in \left(-2^{-(n+2)}, 2^{-(n+2)}\right) \pmod 1. \tag{3}$$

a) (10 points) Construct a circuit of size $O(n)$ for the solution of this problem. (Describe the circuit in reasonable detail, e.g., as a composition of elementary blocks. You don't have to go down to Boolean gates.)

b) (Extra credit: 10 points) Construct a circuit of size $O(n)$ and depth $O(\log n)$.

3. Quantum PSPACE **coincides with classical** PSPACE**.** It is shown in the textbooks that BQP $\subseteq$ PSPACE, i.e., polynomial-size quantum circuits can be simulated classically in polynomial space. A definition of quantum PSPACE is somewhat tricky. Intuitively, a polynomial space machine may run for exponentially long time, repeating the same operations. Translating this to the circuit language, one may be tempted to only limit the circuit width and depth. However, such a definition does not make sense. In fact, Barrington showed that even classical circuits of *constant* width are very powerful and can compute anything (see problem 2.19 in the book by Kitaev, Shen, and Vyalyi). Roughly, the problem is that one can encode the truth table of any Boolean function in the circuit design if the circuit is sufficiently large (even though it is narrow). Thus, we must only allow circuits with sufficiently regular structure. More specifically, we will consider circuits of the form U^{2^n}, where U has polynomial size and can be constructed efficiently by a classical Turing machine. Let us omit the exact definition. Note that Watrous has even considered quantum polynomial-space computation in *doubly exponential time*, but the result has turned out to be the same.

a) (10 points) These preliminaries dispensed with, let U be a matrix of size $2^n \times 2^n$. Given j and k, the matrix element u_{jk} can be computed with sufficient precision in $s(n) = \mathrm{poly}(n)$ space. Find a polynomial space algorithm to compute $\langle 0|U^{2^n}|0\rangle$ with a constant precicion.

b) (Extra credit: 5 points) How many precision bits of u_{jk} do we need to keep? How much space is actually needed for this computation? (Give estimates as powers of n.)