Midterm

This exam is due in class on November 8. There is **no late policy** for the midterm. Start early.

Some edits to the notes at the end on 10/30/2012, 8pm

Work with $m \geq 3$ in Problem 3. 11/06/2012, 11am

1. [10/100] Suppose that you are interested in constructing a 1-qubit unitary operator U with the properties that

$$U|0\rangle = -|1\rangle$$
$$U \cdot \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) = |0\rangle$$

   Does such a unitary operator exist? If so describe it as a 2×2 unitary matrix, if not give an example of a quantum state which, according to the above rules, is mapped to something that is not a valid quantum state.

2. [30/100] (In this problem, all operations are in the vector space $\mathbb{F}_2^n$. See the note at the end of the exam if you are not familiar with linear algebra in finite fields.)

   Let $f : \{0,1\}^n \to \{0,1\}^n$ be a function such that there exists distinct and non-zero $a, b \in \{0,1\}^n$ with the property that for all $x, y \in \{0,1\}^n$ we have

$$f(x) = f(y) \Leftrightarrow \exists \alpha, \beta \in \{0,1\}. y = x + \alpha a + \beta b$$

   Note that this is a "two-dimensional generalization" of the assumption in Simon's algorithm.

   Suppose that we run Simon's algorithm on f:

   (a) [20/100] Describe the distribution of outcomes of the measurement at the last step

(b) [10/100] Show that by running the algorithm $O(n)$ times it is possible to reconstruct the set $\{a, b, a + b\}$.

3. [30/100] Let $M = 2^m$ be a power of two, $m \geq 3$. The period-finding algorithm of lecture 8 is able to recover the period r of a function $f : \{0, \ldots, M - 1\} \to \{0, \ldots, M - 1\}$ if $r \leq \sqrt{M}$, but for much larger periods the measurement at the last step does not always give enough information to accurately reconstruct r. In some cases, however, one can still get non-trivial information about r even for very large r.

   Show that there is an algorithm that runs one iteration of the period-finding algorithm and, after seeing the outcome of the measurement at Step 4 decides whether to *accept* or *reject* and:

   (a) if f has period $r = M/2$, then the algorithm accepts with probability 1

   (b) there is a constant $p < 1$ (independent of M) such that if f has period $r = M/2 - 1$, then the algorithm accepts with probability $\leq p$.

4. [30/100] Use Grover's algorithm to prove that the 3-coloring problem can be solved in time $O(2^{n/2} \cdot n^{O(1)})$ on a quantum computer, where n is the number of vertices.

   [Hint: show that a valid 3-coloring can be encoded using $n + O(1)$ bits.]

Linear Algebra mod 2. $\mathbb{F}_2^n$ is the n-dimensional vector space over the field $\mathbb{F}_2$. The field $\mathbb{F}_2$ has elements $\{0, 1\}$ and operations of addition and multiplication mod 2. Linear algebra in $\mathbb{F}_2^n$ works mostly in the same way as in $\mathbb{R}^n$: a vector $x = (x_1, \ldots, x_n)$ is simply an n-bit string; the sum of two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ is $x + y := (x_1 + y_1 \bmod 2, \ldots, x_n + y_n \bmod 2)$; the multiplication of a vector $x = (x_1, \ldots, x_n)$ by a scalar $\alpha \in \{0, 1\}$ is $\alpha x := (\alpha x_1, \ldots, \alpha x_n)$; a linear combination of vectors $x^{(1)}, \ldots, x^{(k)}$ using coefficients $\alpha_1, \ldots, \alpha_k$ is $\alpha_1 x^{(1)} + \cdots + \alpha_k x^{(k)}$; a linear combination is non-trivial if not all coefficients are zero, and a collection of vectors is linearly independent if all their non-trivial linear combinations are non-zero; k linearly independent vectors span a k-dimensional subspace, and a k-dimensional subspace has precisely 2^k elements; k linearly independent homogeneous linear equations over n variables have precisely 2^{n-k} solutions, forming a $(n-k)$-dimensional subspace, and so on. One thing to pay attention to: if, by analogy with linear algebra over the reals, you try to define an inner product as $\langle x, y \rangle := \sum_i x_i y_i \bmod 2$ then what you get is not an inner product, because you can have non-zero vectors v, for example $v = (1, 1)$ such that $\langle v, v \rangle = 0$, and you can have vectors $v_1, \ldots, v_k$ such that $\langle v_i, v_j \rangle = 0$ for all $i \neq j$ even though the vectors v_i are not linearly independent, for example, consider $(1, 1, 1, 1), (1, 1, 0, 0), (0, 0, 1, 1)$.