Due: Thursday November 17, 2005

1. Consider the proof that IP = PSPACE from Sipser's textbook *Introduction to the Theory of Computation*. In this proof, the verifier does not have a polynomial-sized representation of the polynomials $f_0, f_1, \ldots$ because the new interpolation "quantifier" R doubles the length of each polynomial and we can have $O(m)$ of these R quantifiers in a row. Intuitively, the R quantifier is used to rename the variables in much the same way that Shamir's original proof converted quantified boolean formulas into "simple" formulas.

   Look over this proof and make sure that you understand why the verifier does not need write down $f_0, f_1, \ldots$ in any form. In particular, explain the role of r in Phase i of the protocol:

   $$f_{i-1}(r_1 \cdots, r) = (1-r)f_i(r_1 \cdots, 0) + r f_i(r_1 \cdots, 1) \quad \mathsf{S} = R$$

   (on page 366 of the first edition and page 399 of the second edition). What is this value r? How does it change from phase to phase? Note that the formula would typically have long sequences of R quantifies.

2. A function $g : \mathbb{Z}^n \to \mathbb{Z}$ is *multilinear* if its restriction to any single variable is linear. That is, for all i, $1 \leq i \leq n$ and for all $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \in \mathbb{Z}$, the function $h(y)$ on one variable defined by

   $$h(y) = g(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n)$$

   must be a linear function.

   Consider any Boolean function $f : \{0,1\}^n \to \{0,1\}$. Argue that f has a *unique* multilinear extension in $\mathbb{Z}^n$. That is, there exists a unique multilinear function $g : \mathbb{Z}^n \to \mathbb{Z}$ such that for all $\alpha \in \{0,1\}^n$, $g(\alpha) = f(\alpha)$.