CS 1511 Homework 17

Mathew Varughese, Justin Kramer, Zach Smith

Friday, March 22

32.)

The language QNR = { (a, p) | a is not a quadratic residue modulo p where p is a prime.}

From Euler's criterion, we know that there are (p+1)/2 quadratic residues and (p-1)/2 quadratic nonresidues.

In the private coin protocol, the verifier takes a random number r mod p and a random bit b $\in$ {0,1} and sends the prover r^2 mod p if b = 0 and sends the prover ar^2 mod p if b = 1.

If a is a quadratic residue, then the prover has a 1/2 chance of guessing b correctly. Otherwise, the prover is certain of the value of b.

We know from Euler's criterion that if a is not a quadratic residue, then $\mid S \mid$ will be equal to (p-1)/2. If it is a quadratic residue, $\mid S \mid$ will be equal to (p+1)/2. With the set S being the set of quadratic or non-quadratic residues.

To solve this problem, we can use several iterations of the set lower bound protocol run in parallel. In this instance of the protocol, we will have both our prover and verifier know a number K. The prover will try to convince the verifier that $\mid S \mid$ is $\geq$ K and the verifier should reject with good probability if $\mid S \mid \leq K/2$. Let k be an integer such that $2^{k-2} < K \leq 2^{k-1}$.

Verifier: Randomly pick a function h : $\{0,1\}^m -> \{0,1\}^k$ from a pairwise independent hash function collection $H_{m,k}$. Pick y $\in_R \{0,1\}^k$. Send h,y to prover.

Prover: Try to find an x $\in$ S such that H(x) = y. Send such an x to Verifier, together with a certificate that x $\in$ S.

Verifier output: If h(x) = y and the certificate validates that x $\in$ S then accept, otherwise reject.

If run for several iterations where the verifier accepts iff the traction of accepting iterations was least 5/16, which is the mean of 3/8 and 1/4. The Chernoff bound shows that a constant number of iterations will ensure completeness probability of at least 2/3. These iterations are run in parallel by sending several choices of h,y at once to the prover.

This is the public coin interative protocol for the language QNR.