Handout 5: One-Way Permutations, Number Theory

Boaz Barak

Total of 120 points.
Exercises due October 25th, 2005 1:30pm.

Exercise 1 (50 points). The Goldreich-Levin theorem says that we can transform every one-way permutation $f(\cdot)$ into a one-way permutation $f'(\cdot)$ such that $f'$ has a hard-core bit $h(\cdot)$. The transformation is the following:

- Given $f : \{0,1\}^n \rightarrow \{0,1\}^n$, define $f' : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ as follows: for $x, r \in \{0,1\}^n$ define $f'(x \circ r) = f(x) \circ r$. (Where $\circ$ denotes concatenation.)
- The function $h : \{0,1\}^{2n} \rightarrow \{0,1\}$ is defined as follows: $h(x \circ r) = \sum_{i=1}^n x_i r_i (\text{mod } 2)$. This is also sometimes called the inner product of $x$ and $r$ modulo 2, and we’ll denote $h(x \circ r)$ by $\langle x, r \rangle$.

1. Prove that if $f(\cdot)$ is a one-way permutation then so is $f'(\cdot)$.

2. The main part of the Goldreich-Levin theorem is the following lemma:

**Lemma 1 (GL Lemma).** Let $x \in \{0,1\}^n$ be some string and $\epsilon > 0$ some number, and let $A : \{0,1\}^n \rightarrow \{0,1\}$ be a function such that for a random $r \leftarrow_R \{0,1\}^n$, the probability that $A(r) = \langle x, r \rangle$ is at least $\frac{1}{2} + \epsilon$.

Then, there exists a polynomial in $n$ time algorithm $B$ that given black-box access to $A$ outputs $x$ with probability at least $\frac{\epsilon^2}{n}$.

Assuming Lemma 2, prove that the function $h(\cdot)$ is indeed a hard-core for $f'(\cdot)$.

Do this by proving that if there’s a $T$-time algorithm $A$ such that

$$\Pr_{x,r \in \{0,1\}^n}[A(f'(x, r)) = h(x, r)] \geq \frac{1}{2} + \epsilon$$

Then there is an algorithm $A'$ with running time polynomial in $T$ and $n$ such that

$$\Pr_{x \in \{0,1\}^n}[A(f(x)) = x] \geq \epsilon'$$

Where $\epsilon'$ is polynomial in $\epsilon$ and $n$.

**Hint:** Define “good” $x$’s to be $x$’s such that $\Pr_{r \leftarrow_R \{0,1\}^n}[A(r) = h(x, r)] \geq \frac{1}{2} + \frac{\epsilon^2}{100}$. Show that there are not too few good $x$’s and use the lemma to give an algorithm $A'$ that inverts $f$ on these good $x$’s.

3. Prove the following “toy version” of Lemma 2:
Lemma 2 (GL Lemma - probability 1 case). Let \( x \in \{0,1\}^n \) be some string. There exists a polynomial in \( n \) time algorithm \( B \) that given black-box access to the function \( r \mapsto \langle x, r \rangle \) outputs \( x \).

4. Prove the following “reduced version” of Lemma 2:

Lemma 3 (GL Lemma - probability 0.9 case). Let \( x \in \{0,1\}^n \) be some string and let \( A : \{0,1\}^n \to \{0,1\} \) be a function such that for a random \( r \leftarrow \{0,1\}^n \), the probability that \( A(r) = \langle x, r \rangle \) is at least 0.9.

Then, there exists a polynomial in \( n \) time algorithm \( B \) that given black-box access to \( A \) outputs \( x \) with probability at least 0.1.

Exercise 2 (20 points). Recall that an Abelian group \( G \) is a set of elements with an operation \( \ast \) that satisfies the following properties:

- Associativity: for all \( a, b, c \in G \), \( (a \ast b) \ast c = a \ast (b \ast c) \).
- Commutativity: for all \( a, b \in G \), \( a \ast b = b \ast a \).
- Identity: there exists an element \( e \in G \) such that for all \( a \in G \), \( a \ast e = e \ast a = a \). (We’ll often denote the identity element by 1.)
- Inverse: for every \( a \in G \), there exists an element \( a' \) such that \( a \ast a' = a' \ast a = e \) where \( e \) is an identity element. (We’ll often denote \( a' \) by \( a^{-1} \).)

Prove that for every \( n \), the set of numbers \( x < n \) with \( \gcd(x, n) = 1 \) with the operation \( a \ast b = a \cdot b \mod n \) is an Abelian group. (You can take for granted properties of normal (non-modulo) multiplication such as associativity and commutativity.)

We denote this group by \( \mathbb{Z}_n^\ast \) and denote its size by \( \phi(n) \). Note that clearly for every prime \( p \), \( \phi(p) = p - 1 \).

Exercise 3 (15 points). Let \( G \) be an Abelian group of finite size \( n \), and let \( a \in G \). Prove that there exists a number \( k \) such that \( a^k = 1 \) (where \( a^k = a \ast a \ast \cdots \ast a \) \( k \) times). Hint: As a first step, show that there must be numbers \( \ell < j \) such that \( a^\ell = a^j \).

The smallest such \( k \) is called the order of \( a \) and it turns out that it’s always the case that \( k | n \) and thus it’s always the case that \( a^n = 1 \).

Exercise 4 (20 points). Let \( G \) be an Abelian group with an operation \( \ast \) and let \( G' \) be the subset of \( G \) where \( y \in G' \) if and only if \( y = x^2 \) for some \( x \in G \). Prove that \( G' \) with the operation \( \ast \) is also an Abelian group.

We note that \( G' \) is called the subgroup of quadratic residues of \( G \).

Exercise 5 (15 points). Let \( G \) be an Abelian group. \( G \) is called cyclic if there is an element \( g \in G \) such that for every \( a \in G \) there is an integer \( k \) such that \( a = g^k \) (and thus \( G \) is simply the set \( \{1 = g^0, g = g^1, g^2, \ldots, g^{n-1}\} \)).

Prove that for every cyclic group \( G \) of size \( n \) for an even number \( n \), the set of quadratic residues of \( G \) is exactly the set \( \{g^{2k} \mid k = 0, 1, 2, \ldots, n/2 - 1\} \).