T-79.503 Fundamentals of Cryptology Additional material (Handout 3) for lectures October 21 and 28, 2004

1 Euler Phi-Function

In section 1.1.3 of the text-book, Definition 1.3, the Euler phi-function is defined as follows.

Definition 1.3 (Stinson) Suppose $a \ge 1$ and $m \ge 2$ are integers. If gcd(a, m) = 1 then we say that a and m are relatively prime. The number of integers in \mathbb{Z}_m that are relatively prime to m is denoted by $\phi(m)$.

We set $\phi(1) = 1$. The function

$$m \mapsto \phi(m), \ m \ge 1$$

is called the Euler phi-function, or Euler totient function. Clearly, for m prime, we have $\phi(m) = m - 1$. Further, we state the following fact without proof, and leave the proof as an easy exercise.

Fact. If m is a prime power, say, $m = p^e$, where p is prime and p > 1, then $\phi(m) = m(1 - \frac{1}{p}) = p^e - p^{e-1}$.

Next we prove the multiplicative property of the Euler phi-function.

Proposition. Suppose that $m \ge 1$ and $n \ge 1$ are integers such that gcd(m, n) = 1. Then $\phi(m \times n) = \phi(m) \times \phi(n)$.

Proof. If m = 1 or n = 1, then the claim holds. Suppose now that m > 1 and n > 1, and denote:

$$A = \{a \mid 1 \le a < m, \ \gcd(a, m) = 1\}$$

$$B = \{b \mid 1 \le b < n, \ \gcd(b, n) = 1\}$$

$$C = \{c \mid 1 \le c < m \times n, \ \gcd(c, m \times n) = 1\}.$$

Then we have that $|A| = \phi(m)$, $|B| = \phi(n)$, and $|C| = \phi(m \times n)$. We show that C has equally many elements as the set $A \times B = \{(a, b) | a \in A, b \in B\}$, from which the claim follows.

Since gcd(m,n) = 1, we can use the Chinese Remainder Theorem, by which the mapping

$$\pi: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \ \pi(x) = (x \bmod m, x \bmod n)$$

is bijective. Now we observe that $A \subset \mathbb{Z}_m$, $B \subset \mathbb{Z}_n$, and $C \subset \mathbb{Z}_{m \times n}$. Moreover, it holds that $x \in C$ if and only if $\pi(x) \in A \times B$, which we see by writing the following chain of equivalences:

$$gcd(x, m \times n) = 1 \iff gcd(x, m) = 1 \text{ and } gcd(x, n) = 1$$
$$\Leftrightarrow gcd(x \mod m, m) = 1 \text{ and } gcd(x \mod n, n) = 1.$$

As a corollary, we get Theorem 1.2 of the textbook.

Theorem 1.2 Suppose

$$m = \prod_{i=1}^{k} p_i^{e_i},$$

where the integers p_i are distinct primes and $e_i > 0, 1 \le i \le k$. Then

$$\phi(m) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i-1}).$$

2 More About Finite Fields

This section contains complementary material to Section 5.2.3 of the text-book. It is not entirely self-contained but must be studied in companion with the text-book. For the used notation we refer to the text-book. We also use the same numbering of the theorems whenever applicable. The new theorems and fact are marked by an asterisk (*). We start by sketching a proof of Theorem 5.4.

For a finite multiplicative group G, define the *order* of an element $g \in G$ to be the smallest positive integer m such that $g^m = 1$. Similarly, in an additive group G, the *order* of the element $g \in G$ is the smallest positive integer m such that mg = 0, where 0 is the neutral element of addition. An example of a finite additive group is a group formed by the points on an elliptic curve to be discussed later. For simplicity, we shall use the multiplicative notation in the rest of this section.

Theorem 5.4. (Lagrange) Suppose (G, \cdot) is a multiplicative group of order n, and $g \in G$. Then the order of g divides n.

Proof. Denote by r the order of g, and consider the subset of G formed by the r distinct powers of g. We denote it by H. Thus $H = \{1, g, g^2, \ldots, g^{r-1}\}$. It is straightforward to verify that H is a subgroup of G. Then we can define a relation in G by setting

$$f' \sim f \Leftrightarrow f' \in fH = \{f, fg, \dots, fg^{r-1}\}.$$

This relation is reflexive, symmetric, and transitive, hence it is an equivalence relation, and therefore, divides the elements of G into disjoint equivalence classes which can be given as follows fH, $f \in G$. Clearly, |fH| = r, for all $f \in G$. Consequently, r divides the number |G| of all elements in G.

Corollary 5.5 If $b \in \mathbb{Z}_n^*$ then $b^{\phi(n)} \equiv 1 \pmod{n}$. **Proof.** Recall that

$$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \, | \, gcd(a, n) = 1 \}$$

is a multiplicative group. The Euler ϕ -function is defined as

$$\phi(n) = |\{x \in \mathbb{Z} \mid 0 < x < n, \ \gcd(x, n) = 1\}|,$$

for a positive integer *n*. Thus $|\mathbb{Z}_n^*| = \phi(n)$. Let $b \in \mathbb{Z}_n^*$. By Theorem 5.4 the order *r* of *b* divides $\phi(n)$. Since $b^r \equiv 1 \pmod{n}$, the claim follows.

Corollary^{*}. (Euler's theorem.) Let \mathbb{F} be a finite field, which has q elements, and let $b \in \mathbb{F}^*$. Then the order of b divides q - 1 and $b^{q-1} = 1$.

Proof. (\mathbb{H}^*, \cdot) is a multiplicative group with q-1 elements.

Corollary 5.6 (Fermat) Suppose p is prime and $b \in \mathbb{Z}_p$. Then $b^p \equiv b \pmod{p}$. **Proof.** \mathbb{Z}_p is a finite field with p elements. For b = 0, the congruence holds. If $b \neq 0$, then $b \in \mathbb{Z}_p^*$, and the claim follows from Euler's theorem.

Proposition 1^{*} Suppose G is a finite group, and $b \in G$. Then the order of b divides every integer such that $b^r = 1$.

Proof. Let d be the order of b. Hence $d \leq r$. If r is divided by d, let t be the remainder, that is, we have the equality $r = d \times s + t$, with some s, where $0 \leq t < d$. Then

$$1 = b^r = b^{ds+t} = (b^d)^s b^t = b^t.$$

Since t is strictly less than d, this is possible only if t = 0.

Proposition 2^{*} Suppose G is a finite group and $b \in G$ has order equal to r. Let k be a positive integer, and consider an element $a = b^k \in G$. Then the order of $a = b^k$ is equal to

$$\frac{1}{\gcd(k,r)}$$

Proof. Since

$$(b^k)^{\frac{r}{\gcd(k,r)}} = (b^r)^{\frac{k}{\gcd(k,r)}} = 1,$$

it follows from Proposition 1 that the order of $a = b^k$ divides the integer $\frac{r}{\gcd(k,r)}$. To prove the converse, denote the order of a by t. Then

$$1 = (b^k)^t = b^{k \times t}$$

hence r divides $k \times t$. Then it must be that $\frac{r}{\gcd(k,r)}$ divides t, which is the order of $a = b^k$.

For positive integers k, n, we denote k|n if k divides n.

Proposition 3^{*} For any positive integer n,

$$\sum_{k|n} \phi(k) = n,$$

where ϕ is the Euler phi-function.

Proof. Let integer d be such that d|n, and denote

$$A_d = \{ r \,|\, 1 \le r \le n, \, \gcd(r, n) = d \},\$$

or what is the same,

$$A_d = \{r \mid r = \ell \times d, \ 1 \le \ell \le \frac{n}{d}, \ \gcd(\ell, \frac{n}{d}) = 1\}.$$

Hence it follows that $|A_d| = \phi(\frac{n}{d})$. On the other hand, we have that $A_d \cap A_{d'} = \emptyset$, if $d \neq d'$. Also,

$$\bigcup_{d|n} A_d = \{r \mid 1 \le r \le n\}.$$

It follows that

$$n = \sum_{d|n} |A_d| = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{\frac{n}{d}|n} \phi(\frac{n}{d}) = \sum_{k|n} \phi(k).$$

Proposition 4^{*} Suppose that \mathbb{F} is a finite field of q elements. Let d be a divisor of q-1. Then there are $\phi(d)$ elements in \mathbb{F} with order equal to d.

Proof. Let $a \in \mathbb{H}^*$ such that the order of a is equal to d. Then d|(q-1). Denote

$$B_d = \{ x \in \mathbb{F}^* \mid \text{order of } x = d \}.$$

Then by Proposition 2, we have $\{a^k \mid \gcd(k,d) = 1\} \subset B_d$. On the other hand, $\{1, a, a^2, \ldots, a^{d-1}\} \subset \{x \in \mathbb{H}^* \mid x^d = 1\}$. Since the set on the left hand side has exactly *d* elements, and the set on the right hand side has at most *d* elements, it follows that these sets must be equal. Hence we have

$$B_d \subset \{x \in \mathbb{F}^* \, | \, x^d = 1 \} = \{1, a, a^2, \dots, a^{d-1} \}.$$

It follows that $B_d = \{a^k \mid \gcd(k, d) = 1\}$ and that $|B_d| = \phi(d)$. Suppose now that d is an arbitrary divisor of q - 1. If $B_d = \emptyset$, then $|B_d| = 0$. If $B_d \neq \emptyset$, then we know from above that $|B_d| = \phi(d)$. It follows that

$$q-1 = |\mathbf{F}| = \sum_{d|(q-1)} |B_d| \le \sum_{d|(q-1)} \phi(d).$$

But Proposition 3 states that

$$\sum_{d|(q-1)}\phi(d) = q - 1.$$

Consequently,

$$\sum_{d|(q-1)} \phi(d) = \sum_{d|(q-1)} |B_d| = q - 1,$$

and this happens exactly if, $|B_d| = \phi(d)$, for all divisors d of q - 1.

Definition^{*} A group G is cyclic, if there is $g \in G$ such that for all $h \in G$ there is an integer k such that $h = g^k$. Then we say that g is a generating element of G, or what is the same, G is generated by g.

Corollary^{*} Suppose that \mathbb{F} is a finite field. Then the multiplicative group (\mathbb{F}^*, \cdot) is a cyclic group.

Proof. Denote $|\mathbf{F}| = q$. By Proposition 4 there are $\phi(q-1)$ elements of order q-1 in \mathbf{F}^* . Clearly, each such element is a generator of \mathbf{F}^* .

Definition. Suppose that \mathbb{F} is a finite field. An element in \mathbb{F}^* with maximal order that is equal to $|\mathbb{F}| - 1 = |\mathbb{F}^*|$, is called a primitive element. A finite field \mathbb{F} has $\phi(|\mathbb{F}| - 1)$ primitive elements.

Example. Consider the field \mathbb{Z}_{19} . Then the number 2 is primitive modulo 19, which we can verify, for example, as follows. The factorization of the integer 19 -1 = 18 is $18 = 2 \times 3 \times 3$. By exercise 5.4 of the textbook it suffices to check that that

$$2^9 = 512 \neq 1 \pmod{19}$$
 and $2^6 = 64 \neq 1 \pmod{19}$.

Hence

$$\mathbb{Z}_{19}^* = \{2^k \mod 19 \, | \, k = 0, 1, \dots, 17\}.$$

Next we determine the syclic subgroups of \mathbb{Z}_{19}^* . The number of elements of a cyclic subgroup of \mathbb{Z}_{19}^* must be a divisor of 18. By Euler's theorem, the following numbers are possible: 1, 2, 3, 6, 9 and 18. We denote by S_r the cyclic subgroup of r elements. Below, we list the exponents k such that $2^k \in S_r$, for all divisors r of 18.

r	k	S_r
18	$k=0,1\ldots,17$	1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10
9	k even	1, 4, 16, 7, 9, 17, 11, 6, 5
6	$\frac{18}{6}$ divides k	1, 8, 7, 18, 11, 12
3	$\frac{18}{3}$ divides k	1, 7, 11
2	9 divides k	
1	k = 0	1

3 Algebraic Normal Form of a Boolean function

Let us now consider a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. Such a function is called a Boolean function of n variables. A Boolean function of n variables x_1, \ldots, x_n has a unique representation in its algebraic normal form

$$g(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus \dots$$
$$\dots \oplus a_{(n-1)n} x_{n-1} x_n \oplus a_{123} x_1 x_2 x_3 \oplus \dots \oplus a_{12\dots n} x_1 x_2 \cdots x_n.$$

with coefficients $a_{i_1,\ldots,i_k} \in \mathbb{Z}_2$.

Given the values of the function f, its algebraic normal form ANF(f) can be derived using the following algorithm:

ANF Algorithm.

- 1. Set $g(x_1, \ldots, x_n) = f(0, 0, \ldots, 0)$
- 2. For k = 1 to $2^n 1$, do
- 3. use the binary representation of the integer k, $k = b_1 + b_2 2 + b_3 2^2 + \dots + b_n 2^{n-1}$
- 4. if $g(b_1, b_2, \dots, b_n) \neq f(b_1, b_2, \dots, b_n)$ then set $g(x_1, \dots, x_n) = g(x_1, \dots, x_n) \oplus \prod_{i=1}^n (x_i)^{b_i}$

5.
$$ANF(f) = g(x_1, ..., x_n)$$

Example 4.

k	b_3	b_2	b_1	$f(b_1, b_2, b_3)$	$g(b_1,b_2,b_3)$
	0	0	0	0	0
1	0	0	1	0	0
2	0	1	0	1	x_2
3	0	1	1	0	$x_2 \oplus x_1 x_2$
4	1	0	0	1	$x_2 \oplus x_1 x_2 \oplus x_3$
5	1	0	1	1	$x_2 \oplus x_1 x_2 \oplus x_3$
6	1	1	0	0	$x_2 \oplus x_1 x_2 \oplus x_3$
7	1	1	1	1	$x_2 \oplus x_1 x_2 \oplus x_3$

Now the values of f given in the third column of the table can also be calculated from the expression $f(x_1, x_2, x_3) = x_2 \oplus x_3 \oplus x_1 x_2$.

4 Non-linearity of Boolean Functions

4.1 Correlations

Let $x = (x_1, \ldots, x_m) \in \mathbb{Z}_2^m$. The Hamming weight of x is defined as

$$H_W(x) = |\{i \in \{1, 2, \dots, m\} \mid x_i = 1\}|.$$

For two vectors $x = (x_1, \ldots, x_m) \in \mathbb{Z}_2^m$ and $y = (y_1, \ldots, y_m) \in \mathbb{Z}_2^m$ the Hamming distance is defined as

$$d_H(x,y) = H_W(x \oplus y) = |\{i \in \{1, 2, \dots, m\} \mid x_i \neq y_i\}|.$$

Given two Boolean functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and $g : \mathbb{Z}_2^n \to \mathbb{Z}_2$ the Hamming weight of f is defined as

$$H_W(f) = |\{x \in \mathbb{Z}_2^n \,|\, f(x) = 1\}|,\$$

and the Hamming distance between f and g is

$$d_H(f,g) = |\{x \in \mathbb{Z}_2^n \,|\, f(x) \neq g(x)\}|.$$

A Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is balanced if $H_W(f) = 2^{n-1}$, which happens if and only if

$$|\{x \in \mathbb{Z}_2^n \,|\, f(x) = 1\}| = |\{x \in \mathbb{Z}_2^n \,|\, f(x) = 0\}|.$$

Example 5. Let $f_{00} : \mathbb{Z}_2^4 \to \mathbb{Z}_2$ be the Boolean function defined as the first outputbit of the s-box S_1 of the DES, when the first and the last (sixth) input bits are set equal to zero. Then f_{00} has the following values

$$f_{00} = (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$$

arranged in the *lexicographical order* with respect to the input (x_2, x_3, x_4, x_5) . Clearly, f_{00} is balanced, that is, $H_W(f_{00}) = 8$. Further we see that

$$d_H(f_{00}, s_5) = 6$$
, and $d_H(f_{00}, s_2) = 10$,

where we have denoted by s_i the *i*th input bit to S_1 as a Boolean function of the four middle input bits. That is, $s_i(x_2, x_3, x_4, x_5) = x_i$, for i = 2, 3, 4, 5.

Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and $g : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be two Boolean functions. The *correlation* between f and g is defined as

$$c(f,g) = 2^{-n}(|\{x \in \mathbb{Z}_2^n \mid f(x) = g(x)\}| - |\{x \in \mathbb{Z}_2^n \mid f(x) \neq g(x)\}|)$$

= 2⁻ⁿ(2ⁿ - 2|\{x \in \mathbb{Z}_2^n \mid f(x) \neq g(x)\}|) = 1 - 2^{1-n}d_H(f,g).

A Boolean function $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ is *linear* if it has an ANF of the form

$$f(x) = a \cdot x = a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n$$

for some $a = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_2^n$. Then f is just a linear combination of its input bits. In such a case we denote $f = L_a$. A Boolean function is *affine* if it has an ANF of the form $f(x) = a \cdot x \oplus 1$.

Nonlinearity of a Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is defined as its minimum distance from the set consisting all affine and linear Boolean functions

$$\mathcal{N}(f) = \min_{L \text{ linear}} \{ \min\{d_H(f, L), d_H(f, L \oplus 1) \} \}.$$

Example 5(continued)

From $d_H(f_{00}, s_5) = 6$ and $d_H(f_{00}, s_2) = 10$, it follows that the nonlinearity of f is at most 6. Further we see that

$$c(f_{00}, s_5) = 1 - \frac{1}{8} \cdot 6 = \frac{1}{4}$$
, and
 $c(f_{00}, s_2) = 1 - \frac{10}{8} = -\frac{1}{4}$.