DD2448 Foundations of Cryptography
Lecture 5

Douglas Wikström
KTH Royal Institute of Technology
dog@kth.se

February 19, 2016

Entropy

Let us turn this expression into a definition.

Definition. Let X be a random variable taking values in $\mathcal{X}$. Then the **entropy** of X is

$$H(X) = -\sum_{x \in \mathcal{X}} \mathrm{P}_X(x) \log \mathrm{P}_X(x) \quad .$$

Examples and intuition are nice, but what we need is a theorem that states that this is **exactly** the right expected length of an optimal code.

Conditional Entropy

Definition. Let (X, Y) be a random variable taking values in $\mathcal{X} \times \mathcal{Y}$. We define **conditional entropy**

$$H(X|y) = -\sum_x \mathrm{P}_{X|Y}(x|y) \log \mathrm{P}_{X|Y}(x|y) \quad \text{and}$$

$$H(X|Y) = \sum_y \mathrm{P}_Y(y) H(X|y)$$

Note that $H(X|y)$ is simply the ordinary entropy function of a random variable with probability function $\mathrm{P}_{X|Y}(\cdot|y)$.

Properties of Entropy

Let X be a random variable taking values in $\mathcal{X}$.

Upper Bound. $H(X) = \mathrm{E}\left[-\log \mathrm{P}_X(X)\right] \leq \log |\mathcal{X}|$.

Chain Rule and Conditioning.

$$\begin{aligned} H(X, Y) &= -\sum_{x,y} \mathrm{P}_{X,Y}(x, y) \log \mathrm{P}_{X,Y}(x, y) \\ &= -\sum_{x,y} \mathrm{P}_{X,Y}(x, y) \left(\log \mathrm{P}_Y(y) + \log \mathrm{P}_{X|Y}(x|y) \right) \\ &= -\sum_{y} \mathrm{P}_Y(y) \log \mathrm{P}_Y(y) - \sum_{x,y} \mathrm{P}_{X,Y}(x, y) \log \mathrm{P}_{X|Y}(x|y) \\ &= H(Y) + H(X|Y) \leq H(Y) + H(X) \end{aligned}$$

Elementary Number Theory

Greatest Common Divisors

Definition. A common divisor of two integers m and n is an integer d such that $d \mid m$ and $d \mid n$.

Definition. A greatest common divisor (GCD) of two integers m and n is a common divisor d such that every common divisor d' divides d.

Greatest Common Divisors

Definition. A common divisor of two integers m and n is an integer d such that $d \mid m$ and $d \mid n$.

Definition. A greatest common divisor (GCD) of two integers m and n is a common divisor d such that every common divisor d' divides d.

- **The** GCD is the **positive** GCD.

Greatest Common Divisors

Definition. A common divisor of two integers m and n is an integer d such that $d \mid m$ and $d \mid n$.

Definition. A greatest common divisor (GCD) of two integers m and n is a common divisor d such that every common divisor d' divides d.

- **The** GCD is the **positive** GCD.
- We denote the GCD of m and n by $\gcd(m, n)$.

Properties

- $\gcd(m, n) = \gcd(n, m)$
- $\gcd(m, n) = \gcd(m \pm n, n)$
- $\gcd(m, n) = \gcd(m \bmod n, n)$
- $\gcd(m, n) = 2 \gcd(m/2, n/2)$ if m and n are even.
- $\gcd(m, n) = \gcd(m/2, n)$ if m is even and n is odd.

Euclidean Algorithm

EUCLIDEAN(m, n)
(1) **while** $n \neq 0$
(2) $t \leftarrow n$
(3) $n \leftarrow m \bmod n$
(4) $m \leftarrow t$
(5) **return** m

Steins Algorithm (Binary GCD Algorithm)

```
Stein(m, n)
    if m = 0 or n = 0 then return 0
    s ← 0
    while m and n are even
        m ← m/2, n ← n/2, s ← s + 1
    while n is even
        n ← n/2
    while m ≠ 0
        while m is even
            m ← m/2
        if m < n
            Swap(m, n)
        m ← m − n
        m ← m/2
    return 2^s n
```

Bezout's Lemma

Lemma. There exists integers a and b such that

$$\gcd(m, n) = am + bn \quad .$$

Bezout's Lemma

Lemma. There exists integers a and b such that

$$\gcd(m, n) = am + bn \ .$$

Proof. Let $d > \gcd(m, n)$ be the smallest positive integer on the form $d = am + bn$. Write $m = cd + r$ with $0 < r < d$. Then

$$d > r = m - cd = m - c(am + bn) = (1 - ca)m + (-cb)n \ ,$$

a contradiction! Thus, $r = 0$ and $d \mid m$. Similarly, $d \mid n$.

Extended Euclidean Algorithm (Recursive Version)

ExtendedEuclidean(m, n)
(1) **if** $m \bmod n = 0$
(2) **return** $(0, 1)$
(3) **else**
(4) $(x, y) \leftarrow$ ExtendedEuclidean$(n, m \bmod n)$
(5) **return** $(y, x - y\lfloor m/n \rfloor)$

If $(x, y) \leftarrow$ ExtendedEuclidean(m, n) then
$\gcd(m, n) = xm + yn$.

Coprimality (Relative Primality)

Definition. Two integers m and n are coprime if their greatest common divisor is 1.

Fact. If a and n are coprime, then there exists a b such that $ab = 1 \bmod n$.

Coprimality (Relative Primality)

Definition. Two integers m and n are coprime if their greatest common divisor is 1.

Fact. If a and n are coprime, then there exists a b such that $ab = 1 \bmod n$.

Excercise: Why is this so?

Chinese Remainder Theorem (CRT)

Theorem. (Sun Tzu 400 AC) Let $n_1, \ldots, n_k$ be positive pairwise coprime integers and let $a_1, \ldots, a_k$ be integers. Then the equation system

$$\begin{aligned} x &= a_1 \bmod n_1 \\ x &= a_2 \bmod n_2 \\ x &= a_3 \bmod n_3 \\ &\vdots \\ x &= a_k \bmod n_k \end{aligned}$$

has a unique solution in $\{0, \ldots, \prod_i n_i - 1\}$.

Constructive Proof of CRT

1. Set $N = n_1 n_2 \cdot \ldots \cdot n_k$.
2. Find r_i and s_i such that $r_i n_i + s_i \frac{N}{n_i} = 1$ (Bezout).
3. Note that

$$s_i \frac{N}{n_i} = 1 - r_i n_i = \begin{cases} 1 \pmod{n_i} & \\ 0 \pmod{n_j} & \text{if } j \neq i \end{cases}$$

4. The solution to the equation system becomes:

$$x = \sum_{i=1}^{k} \left(s_i \frac{N}{n_i} \right) \cdot a_i$$

The Multiplicative Group

The set $\mathbb{Z}_n^* = \{0 \leq a < n \ : \ \gcd(a, n) = 1\}$ forms a group, since:

- **Closure.** It is closed under multiplication modulo n.
- **Associativity.** For $x, y, z \in \mathbb{Z}_n^*$:

$$(xy)z = x(yz) \bmod n \ .$$

- **Identity.** For every $x \in \mathbb{Z}_n^*$:

$$1 \cdot x = x \cdot 1 = x \ .$$

- **Inverse.** For every $a \in \mathbb{Z}_n^*$ exists $b \in \mathbb{Z}_n^*$ such that:

$$ab = 1 \bmod n \ .$$

Lagrange's Theorem

Theorem. If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof.

1. Define $aH = \{ah : h \in H\}$. This gives an equivalence relation $x \approx y \Leftrightarrow x = yh \wedge h \in H$ on G.
2. The map $\phi_{a,b} : aH \rightarrow bH$, defined by $\phi_{a,b}(x) = ba^{-1}x$ is a bijection, so $|aH| = |bH|$ for $a, b \in G$.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relatively prime to n.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relatively prime to n.

- Clearly: $\phi(p) = p - 1$ when p is prime.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relatively prime to n.

- Clearly: $\phi(p) = p - 1$ when p is prime.
- Similarly: $\phi(p^k) = p^k - p^{k-1}$ when p is prime and $k > 1$.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relatively prime to n.

- Clearly: $\phi(p) = p - 1$ when p is prime.
- Similarly: $\phi(p^k) = p^k - p^{k-1}$ when p is prime and $k > 1$.
- In general: $\phi\left(\prod_i p_i^{k_i}\right) = \prod_i \left(p_i^k - p_i^{k-1}\right)$.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relatively prime to n.

- Clearly: $\phi(p) = p - 1$ when p is prime.
- Similarly: $\phi(p^k) = p^k - p^{k-1}$ when p is prime and $k > 1$.
- In general: $\phi\left(\prod_i p_i^{k_i}\right) = \prod_i \left(p_i^k - p_i^{k-1}\right)$.

Excercise: How does this follow from CRT?

Fermat's and Euler's Theorems

Theorem. (Fermat) If $b \in \mathbb{Z}_p^*$ and p is prime, then $b^{p-1} = 1 \bmod p$.

Theorem. (Euler) If $b \in \mathbb{Z}_n^*$, then $b^{\phi(n)} = 1 \bmod n$.

Fermat's and Euler's Theorems

Theorem. (Fermat) If $b \in \mathbb{Z}_p^*$ and p is prime, then $b^{p-1} = 1 \bmod p$.

Theorem. (Euler) If $b \in \mathbb{Z}_n^*$, then $b^{\phi(n)} = 1 \bmod n$.

Proof. Note that $|\mathbb{Z}_n^*| = \phi(n)$. b generates a subgroup $\langle b \rangle$ of $\mathbb{Z}_n^*$, so $|\langle b \rangle|$ divides $\phi(n)$ and $b^{\phi(n)} = 1 \bmod n$.

Multiplicative Group of a Prime Order Field

Definition. A group G is called **cyclic** if there exists an element g such that each element in G is on the form g^x for some integer x.

Theorem. If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

Multiplicative Group of a Prime Order Field

Definition. A group G is called **cyclic** if there exists an element g such that each element in G is on the form g^x for some integer x.

Theorem. If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

Every group of prime order is cyclic. Why?

Multiplicative Group of a Prime Order Field

Definition. A group G is called **cyclic** if there exists an element g such that each element in G is on the form g^x for some integer x.

Theorem. If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

Every group of prime order is cyclic. Why?

Why is there no cyclic multiplicative group $\mathbb{Z}_p^*$, with prime p, except the trivial case $\mathbb{Z}_2^*$?

Multiplicative Group of a Prime Order Field

Definition. A group G is called **cyclic** if there exists an element g such that each element in G is on the form g^x for some integer x.

Theorem. If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

Every group of prime order is cyclic. Why?

Why is there no cyclic multiplicative group $\mathbb{Z}_p^*$, with prime p, except the trivial case $\mathbb{Z}_2^*$?

Keep in mind the difference between:

- $\mathbb{Z}_p$ with *prime order* as an *additive group*,
- $\mathbb{Z}_p^*$ with *non-prime order* as a *multiplicative group*.
- group G_p of *prime order*.