Introduction to cryptology
TD#1

2024–W5

Exercise 1: One-time pad

Q.1: One considers two independent random variables X and Y over $\{0, 1\}$. X follows a uniform distribution, and Y is arbitrary; we let $p := \Pr[Y = 0]$.

Let $Z := X \oplus Y$ over $\{0, 1\}$ be given as the XOR of X and Y. Compute:

1. $\Pr[Z = 0]$
2. $\Pr[Z = 1]$
3. $\Pr[Z = 0 \wedge Y = 0]$; deduce that Z is independent from Y.
4. $\Pr[Z = 0 \wedge X = 0]$; deduce that Z is independent from X iff. $p = 1/2$.
5. $\Pr[Y = 0 : Z = 0]$

   Hint. Use the formula of conditional probabilities:

   $$\Pr[A : B] = \frac{\Pr[B : A] \Pr[A]}{\Pr[B]}$$

   (for $\Pr[B] > 0$).
6. $\Pr[Y = 0 : Z = 0]$, now taking an arbitrary distribution for X, letting $q := \Pr[X = 0]$. Compare with the previous result.

Q.2: Recall that n random variables $X_0, \ldots, X_{n-1}$ of co-domain $\mathcal{X}_0, \ldots, \mathcal{X}_{n-1}$ are *mutually independent* iff.:

$$\forall (x_i)_{0 \leqslant i < n} \in \mathcal{X}_0 \times \cdots \times \mathcal{X}_{n-1},\ \Pr\left[\bigwedge_{0 \leqslant i < n} X_i = x_i\right] = \prod_{0 \leqslant i < n} \Pr[X_i = x_i]$$

or equivalently iff.:

$$\forall (x_i)_{0 \leqslant i < n} \in \mathcal{X}_0 \times \cdots \times \mathcal{X}_{n-1},\ \forall j \in [\![0, n-1]\!],$$
$$\Pr\left[X_j = x_j : \bigwedge_{0 \leqslant i \neq j < n} X_i = x_i\right] = \Pr[X_j = x_j]$$

We consider a random variable $X = (X_i)_{0 \leqslant i < n} \in \{0, 1\}^n$.

1. Show that X is uniform over $\{0, 1\}^n$ iff. the X_i's are mutually independent and uniform over $\{0, 1\}$.

Q.3:

1. Deduce from the previous questions that if X and Y are two independent random variables over $\{0, 1\}^n$, X uniform, then $Z := X \oplus Y$ given by the bitwise XOR of X and Y is uniform over $\{0, 1\}^n$ and independent from Y.

Remark: More generally, one may show that the above holds over any finite quasigroup.

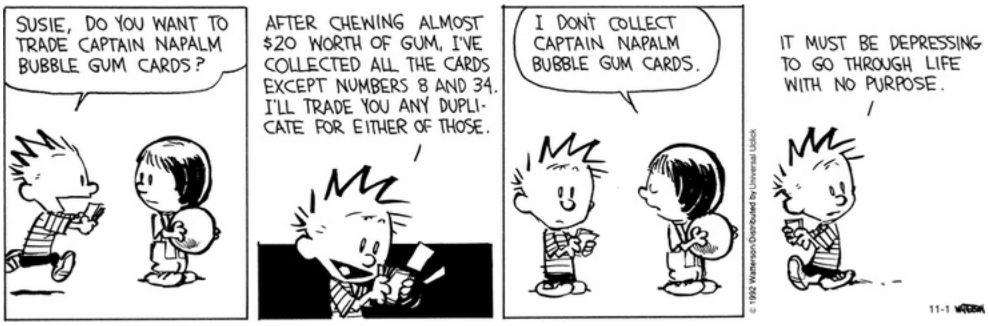

Figure 1: The coupon collector's problem: a Calvin & Hobbes illustration

Exercise 2: (multi-)collisions

In this exercise, we let $\mathcal{S}$ be an arbitrary finite set of size N, and we denote by $X \twoheadleftarrow \mathcal{S}$ the process of drawing X from $\mathcal{S}$ uniformly at random, and independently of any other process.

Let $X \twoheadleftarrow \mathcal{S}$, $Y \twoheadleftarrow \mathcal{S}$, $Z \twoheadleftarrow \mathcal{S}$.

1. Compute $\Pr[(X = x) \wedge (Y = y)]$ for any $x, y \in \mathcal{S}$.
2. Compute $\Pr[X = Y]$.
3. Compute $\Pr[X = Y = Z]$.

Exercise 3: For my birthday I got a coupon for a pair of socks

Let again $\mathcal{S}$ be an arbitrary finite set of size N, which we sample repeatedly by drawing $X_1, \ldots, X_q$ uniformly and independently. A (non-trivial) *collision* for those random variables is a pair $(X_i, X_{j \neq i} = X_i)$.

Q.1 (*Pigeonhole principle*, or *lemme des chaussettes*): How many samples q are necessary to ensure (with probability 1) that there is *at least one* collision among $X_1, \ldots, X_q$?

Q.2 (*Birthday paradox*):

1. Compute the probability p^q_{unq} that there are *no* collisions among $X_1, \ldots, X_q$.
2. Using the union bound, give an upper bound for $p^q_{\text{col}} := 1 - p^q_{\text{unq}}$, the probability that there *is* a collision.

   HINT: Introduce some new random variables $C_{i,j}$ that indicate if their corresponding pair (X_i, X_j) forms a collision.
3. Compute the expected number of collisions in function of q.

   HINT: Use the linearity of expectations.

REMARK. By suitably upper-bounding p^q_{unq}, one may show that for small enough values of q, $p^q_{\text{col}} \geqslant q(q-1)/4N$, cf. https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto/BirthdayBounds.pdf.

Q.3⋆ (*Coupon collector's problem, cf. Figure 1*):

1. For all $\alpha \in \mathbb{R}$, $\alpha > 1$, compute an upper-bound on the number of samples q necessary to ensure that the probability that there is some a in $\mathcal{S}$ s.t. none of the X_i's evaluated to a (i.e. the probability that not all coupons were collected) is less than $1/\alpha$.

   HINT: Apply the union bound to suitable random variables, and use $(1 - 1/N)^{kN} \leqslant e^{-k}$ (for $k > 1$).
2. Compute the expected number of samples q needed to collect all coupons.

   HINT: Use the linearity of expectations and the fact that the number of samples needed to pick a new coupon after k have been collected follows a geometric distribution of parameter $\frac{n-k}{n}$.