You are asked to complete the exercise(s) marked with a [★] and to send me your solutions at: nicolas.schabanel@cnrs.fr
(or drop it in my mail box at the 4th floor of Sophie Germain) on Tue. Nov. 22, 2016.

Exercise 1 (Let’s try random and derandomize by two different methods). We consider the NP-complete Max-Cut problem: Given an undirected graph \( G = (V, E) \), find a cut \( C = (S, V \setminus S) \) of maximum size, where:

\[
\text{size}(C) = \# \{ uv \in E : u \in S \text{ and } v \notin S \}.
\]

▶ Question 1.1 (★) Prove that outputting a random cut is a randomized \( \frac{1}{2} \)-approximation for the Max-Cut problem (i.e. its output cuts at least \( \text{OPT} / 2 \) edges). Which upper bound on \( \text{OPT} \) did you use? Exhibit a family of tight instances.

We now want to derandomize this algorithm by making the “best random choice” for each vertex. We consider each vertex, one after the other in an arbitrary order \( u_1, \ldots, u_n \), and place each vertex on the side of the cut which maximizes the expected number of edges in the cut given the choices already made and assuming the next choices are random.

▶ Question 1.2 (★) Let \( A_i \) and \( B_i \) denote the left and right sides of the cut \( C_i \) obtained after inserting \( u_1, \ldots, u_i \). Show that:

\[
\mathbb{E}[\text{size}(C_{i+1}) \mid A_i, B_i, u_{i+1} \in A_{i+1}] - \mathbb{E}[\text{size}(C_{i+1}) \mid A_i, B_i, u_{i+1} \in B_{i+1}] = \deg(u_{i+1}, B_i) - \deg(u_{i+1}, A_i),
\]

where \( \deg(u, A) = \# \{ v \in A : uv \in E \} \).

▶ Question 1.3 (★) Conclude that the greedy algorithm that puts each vertex on the side to which it has the less connection is a deterministic \( \frac{1}{2} \)-approximation, as it is a derandomized version of the random cut algorithm (this derandomization scheme is called the conditional expectation method).

▶ Question 1.4 (★) Give a direct analysis for the approximation ratio of this greedy algorithm.

Remark that we only need \( n \) pairwise independent uniform random bits to ensure that the analysis of the randomized algorithm works and thus to conclude that the expected value of the cut is at least \( \# E / 2 \). In the following we will describe a way to generate \( n \) pairwise independent uniform random bits \( X_1, \ldots, X_n \) using only \( \ell = \lceil \log_2 n \rceil \) “true” uniform independent random bits \( Y_1, \ldots, Y_\ell \).

▶ Question 1.5 Let \( (G, \cdot) \) be a finite group, \( X \) a random variable over \( G \) and \( U \) an independent uniform random variable over \( G \). Show that \( X \cdot U \) is an uniform random variable over \( G \) independent from \( X \).
Let \([i] = \{j : \text{\(j\)-th bit of \(i\) written in binary is 1}\} \subseteq \{1, \ldots, \ell\}\) such that \(i = \sum_{j \in [i]} 2^{j-1}\) for all \(i \in \{1, \ldots, n\}\). Consider \(Y_1, \ldots, Y_\ell\), \(\ell\) uniform independent random bits. We then set \(X_i = \bigoplus_{j \in [i]} Y_j\) for \(i = 1 \ldots n\), where \(a \oplus b\) denote the XOR of \(a\) and \(b\) (i.e. their sum modulo 2). For instance: \(13 = 1101\) in binary, thus \(X_{13} = Y_4 \oplus Y_3 \oplus Y_1\).

**Question 1.6** Show that \(X_1, \ldots, X_n\) are \(n\) pairwise independent uniform random bits.

**Question 1.7** Propose then a polynomial-time deterministic algorithm that enumerates all possible outcomes for the pairwise independent random bits \(X_1, \ldots, X_n\) to output a cut which cuts at least \(\#E/2\) edges.

We now want to generate economically \(n\) \(k\)-wise independent random variables \(X_1, \ldots, X_n\). The technics above for pairwise independent random variables does not generalize easily. We thus proceed as follows. Let \(\ell = \lceil \log_2 n \rceil\) Consider \(\mathbb{F}_{2^\ell}\) the finite field with \(2^\ell\) elements and let \(\sigma\) be any bijection from \(\{0, \ldots, 2^\ell - 1\}\) to \(\mathbb{F}_{2^\ell}\). We denote by \([i] = \sigma(i)\) the \(i\)th element of \(\mathbb{F}_{2^\ell}\). Now, let \(A_1, \ldots, A_k\) be \(k\) independent uniform random variables with values in \(\mathbb{F}_{2^\ell}\). Consider the random polynomial \(P_A(z) = \sum_{j=1}^k A_j \cdot z^{j-1}\) and set, for \(i = 1 \ldots n\), \(Z_i = P_A([i])\), the image by \(P_A\) of the \(i\)th element of \(\mathbb{F}_{2^\ell}\).

**Question 1.8** Show that \(n\) random variables \(T_1, \ldots, T_n\) are \(k\)-wise independent uniform random variables over some finite set \(\mathcal{T}\) if and only if \(\Pr\{T_{i_1} = t_1 \land \cdots \land T_{i_k} = t_k\} = 1/\#\mathcal{T}^k\) for all \(1 \leq i_1 < \cdots < i_k \leq n\) and \((t_1, \ldots, t_k) \in \mathcal{T}^k\).

Conclude that \(Z_1, \ldots, Z_n\) are \(k\)-wise independent uniform variables over \(\mathbb{F}_{2^\ell}\) if and only for all \(1 \leq i_1 < \cdots < i_k \leq n\), and all \((z_1, \ldots, z_k) \in \mathbb{F}_{2^\ell}^k\), there is exactly one outcome \((a_1, \ldots, a_k) \in \mathbb{F}_{2^\ell}^k\) of \(A_1, \ldots, A_k\) such that \(Z_{ij} = z_j\) for all \(1 \leq j \leq k\).

**Question 1.9** Show that \(Z_1, \ldots, Z_n\) are \(k\)-wise independent uniform variables over \(\mathbb{F}_{2^\ell}\).

Hint. The Vander Monde matrix \(( (\alpha_j)^q )_{j=1..k, q=0..k-1}\) is invertible in a given field if and only if \(\alpha_1, \ldots, \alpha_k\) are distinct.

**Question 1.10** Conclude with an algorithm to compute \(n\) \(k\)-wise independent uniform random bits \(X_1, \ldots, X_n\) from at most \(k\ell\) uniform random bits. How many possible outcomes for \(X_1, \ldots, X_n\) does this process generates?