1 A subsum problem

We recall the permanent lemma.

**Lemma 1.1.** Let $M$ be an $n \times n$-matrix with non-zero permanent over $\mathbb{Z}_p$ ($p$ prime). Then, for any $n$ pairs of elements $\{a_i, b_i\}$ and any vector $t \in \mathbb{Z}_p^n$, there exists $x \in \{a_1, b_1\} \times \{a_2, b_2\} \times \cdots \times \{a_n, b_n\}$ such that $M \cdot x$ differs from $t$ on all coordinates.

The goal of this exercise is to show that if $a_1 \leq a_2 \leq \cdots \leq a_{2p-1}$ is a sequence $A$ (with possible repetitions) of integers between 0 and $p-1$ (where $p$ is a prime), then there exists a subset $S \subset A$ of size $p$ that sums to a multiple of $p$.

1. Does the statement still hold for $2p-2$ instead of $2p-1$ (for all prime $p$)?

2. Show that we can assume $a_i < a_{p+i-1}$ for all $i = 1 \ldots p-1$.

3. Show that the constant $(p-1) \times (p-1)$ matrix $J$ with all values 1 has non-zero permanent over $\mathbb{F}_p$.

4. Denote $S_i = \{a_i, a_{p+i-1}\}$ for all $i = 1 \ldots p-1$. Use the permanent lemma with $J$ to show the existence of a subset $S \subset A$ which sums to 0 mod $p$.

2 Sylvester matrices

Let $K$ be a field, and $P = \sum_{i=0}^{d_P} p_i X^i$, $Q = \sum_{i=0}^{d_Q} q_i X^i$ be two polynomials in $K[X]$ of respective degree $d_P$ and $d_Q$. Put $D = d_P + d_Q$, define $v_P = (p_0, p_1, \ldots, p_{d_P}, 0, \ldots, 0) \in K^D$ and $v_Q = (q_0, q_1, \ldots, q_{d_Q}, 0, \ldots, 0) \in K^D$.

For $x = (x_0, \ldots, x_{D-1})$ a vector in $K^D$, define $C(x) = (0, x_0, \ldots, x_{D-2})$. The Sylvester matrix of $P$ and $Q$ is the matrix of size $D$ whose columns are

$$(v_P, C(v_P), \ldots, C^{d_Q-1}(v_P), v_Q, C(v_Q), \ldots, C^{d_P-1}(v_Q)).$$

It is probably better illustrated on an example: if $P$ has degree 2 and $Q$ degree 3, then we have

$$S(P, Q) := \begin{pmatrix}
p_0 & 0 & 0 & q_0 & 0 
p_1 & p_0 & 0 & q_1 & q_0 
p_2 & p_1 & p_0 & q_2 & q_1 
0 & p_2 & p_1 & q_3 & q_2 
0 & 0 & p_2 & 0 & q_3
\end{pmatrix}.$$
2.1 Solving linear systems

1. Let \( v = (v_0, \ldots, v_{d_Q-1}, w_0, \ldots, w_{d_P-1}) \in K^D \). Compute \( S(P, Q) \cdot v \) and express it in terms of the polynomials \( V = \sum v_i X^i \) and \( W = \sum w_i X^i \).

2. What is the best complexity you can achieve for computing a product \( S(P, Q) \cdot v \) using fast arithmetic?

3. If \( P, Q \) are coprime, what is the best complexity you can achieve for solving the equation \( S(P, Q) \cdot v = w \)? Or computing the inverse of \( S(P, Q) \)?

2.2 Computing \( \det(S(F, G)) \)

Recall simple facts about the resultant \( \text{Res}(F, G) \) for \( F = \text{LC}(F) \prod_i (x - u_i), G = \text{LC}(G) \prod_i (x - v_i) \) for \( u_i, v_i \in \bar{K} \), where \( \text{LC}() \) is the leading coefficient:

1. \( \text{Res}(F, G) = \text{LC}(F)^{\deg G} \text{LC}(G)^{\deg F} \prod_{i,j} (u_i - v_j) \)

2. \( \text{Res}(F, G) = \text{LC}(F)^{\deg Q} \prod_i G(u_i) \)

1. Prove that for \( F = GQ + R \):

\[
\text{Res}(F, G) = (-1)^{\deg F \deg G} \text{LC}(G)^{\deg F - \deg R} \cdot \text{Res}(G, R).
\]

2. Using the above equality deduce an algorithm to compute \( \det(S(F, G)) \) and analyse its complexity.