Encode Summer School 2025
Information Set Decoding

Exercises: ISD

Problem 1: Information sets

1. Let $\mathcal{C}$ be the code generated by $G \in \mathbb{F}_5^{2\times 4}$, given as
$$G = \begin{pmatrix} 1 & 3 & 2 & 3 \\ 0 & 4 & 4 & 3 \end{pmatrix}.$$
Determine all information sets of this code.
2. Compute the probability of a set I to be an information set.

Problem 2: Asymptotics

Let us denote by $T = \lim_{n\to\infty} t(n)/n$.

If we have multiple solutions, say x many, we assume that the cost of finding *one* solution is the usual cost$/x$.

1. Compute the asymptotic costs of the two Brute Force algorithms.
2. Show that the asymptotic number of solutions is $N = H_q(T) - (1-R)$.
3. Show that Prange's asymptotic cost is $H_q(T) - (1-R)H_q(T/(1-R))$.
4. Show that $H_q((q-1)/q) = 1$.
5. Let $T \in [(1-R)(q-1)/q, R + (1-R)(q-1)/q]$. Show that Prange's asymptotic cost $= 0$.

Problem 3: Representations

Compute the number of representations over $\mathbb{F}_q$.