Exercise 1. Prove the equivalence (by two polynomial reductions) of the following problems :

- **Problem:** ML-DECODING

  Instance: A matrix G in $GF(2)^{n\times m}$, $c \in GF(2)^m$, an integer w.

  Property: There is $x \in GF(2)^n$ such that $d_H(xG, c) \leq w$.

- **Problem:** ML-DECODING′

  Instance: A matrix H in $GF(2)^{m\times r}$, $s \in GF(2)^r$, an integer w.

  Property: There is $y \in GF(2)^m$ such that $\text{wgt}(y) \leq w$ and $yH = s$.

For that, take the same w and depending on the reduction choose H and s or G and c such that the rows of G form a basis of the left kernel of H and $cH = s$. Explain why you can do that in polynomial time.

In the rest of this exercise sheet, you have to prove the NP-completness of the 4 following problems using the given hints.

Exercise 2.

Problem: CHROMATIC NUMBER

Instance: Graph $G = (V, E)$, positive integer k.

Property: There is a function $\phi : V \to \{1, \ldots, k\}$ such that if u and v are adjacent, then $\phi(u) \neq \phi(v)$.

We will reduce 3-SAT to it. We start with an instance of 3-SAT given by r clauses $D_1, \ldots, D_r$ each consisting of at most three literals from $\{u_1, \ldots, u_m\} \cup \{\overline{u_1}, \ldots, \overline{u_m}\}$. We assume without loss of generality that $m \geq 4$. We associate to this instance the following CHROMATIC NUMBER instance:

- V is a set of $3m + r$ vertices labeled $\{u_1, \ldots, u_m\} \cup \{\overline{u_1}, \ldots, \overline{u_m}\} \cup \{v_1, \ldots, v_m\} \cup \{D_1, \ldots, D_r\}$
- $E = \{u_i, \overline{u_i}\}_i \cup \{v_i, v_j\}_{i\neq j} \cup \{v_i, u_j\}_{i\neq j} \cup \{v_i, \overline{u_j}\}_{i\neq j} \cup \{u_i, D_f\}_{u_i \notin D_f} \cup \{\overline{u_i}, D_f\}_{\overline{u_i} \notin D_f}$
- $k = m + 1$

Exercise 3.

Problem: EXACT COVER

Instance: Family $\{S_j\}$ of subsets of a set $X = \{x_1, \ldots, x_t\}$.

Property: There is a subfamily $\{T_h\} \subseteq \{S_j\}$ such that the T_h are disjoint and $\cup T_h = \cup S_j = \{x_1, \ldots, x_t\}$.

We will reduce a CHROMATIC NUMBER instance to it:

- The set of elements X is $V \cup E \cup \{(u, e, f) \mid u \text{ is incident with e and } 1 \leq f \leq k\}$.
- The sets S_j are the following
  - For each $f \in \{1, \ldots, k\}$ and each $u \in V$, $\{u\} \cup \{(u, e, f) \mid e \in E \text{ and } u \in e\}$.
  - For each $e = \{u, v\} \in E$ and each pair $f_1, f_2 \in \{1, \ldots, k\}$ such that $f_1 \neq f_2$, $\{e\} \cup \{(u, e, f), f \neq f_1\} \cup \{(v, e, g), g \neq f_2\}$.

Exercise 4.

Problem: 3 DIMENSIONAL MATCHING

Instance: A set $U \subseteq Z \times Z \times Z$ where Z is a finite set.

Property: There is a set $T \subseteq U$ such that $|T| = |Z|$ and no two elements of T agree on the same coordinates.

We will reduce EXACT COVER to it. Without loss of generality we assume $|S_j| \geq 2$ for each j. Let $Z = \{(i,j) | x_i \in S_j\}$. Let α be an arbitrary one-to-one function from $X = \{x_i\}$ into Z. Let $\pi : Z \to Z$ be a permutation such that, for each fixed j, $\{(i,j) \mid x_i \in S_j\}$ is a cycle of π.

$$U = \{(\alpha(x_i), (i,j), (i,j)) \mid (i,j) \in Z\} \cup \{(\beta, \sigma, \pi(\sigma)) \mid \forall \beta \notin \alpha(X) \text{ and } \forall \sigma\}$$

Exercise 5.

Problem: WEIGHT DISTRIBUTION

Instance: A matrix $H \in \mathrm{GF}(2)^{m \times n}$, an integer w.

Property: There is $c \in \mathrm{GF}(2)^m$ of weigth w such that $cH = 0$.

We will reduce 3 DIMENSIONAL MATCHING to it. The idea is to construct a matrix H for the weight distribution problem from the triple incidence matrix B as defined in the course. We assume its size is $t \times 3n$, ie, $|U| = t$ and $|Z| = n$. The matrix H is formed from B as shown below.

$$\begin{array}{c|cccc}
\leftarrow 3n \rightarrow & \longleftarrow & 3n \text{ copies} & & \longrightarrow \\
\hline
B & I_t & I_t & \cdots & I_t \\
\hline
\multicolumn{5}{c}{I_{3n(t+1)}}
\end{array}$$

Remark: Can you see why this reduction does not work if we just assume that the weight of c is $\leq w$?