Solution.

Exercise 1. If G, H, c and s verify the given relations we obtain the equivalence between the two properties:

- We assume $\exists x, d_H(xG, c) \leq w$. This implies $\exists y, \text{wgt}(y) \leq w, xG = c + y$. But, by construction $xGH = 0$ hence $(c + y)H = 0$ and $yH = cH = s$.
- We assume $\exists y, \text{wgt}(y) \leq w, yH = s$. Since $s = cH$, we get $(y+c)H{=}0$. This implies by construction that $\exists x, xG = y + c$ and we get the result.

From c, it is easy to take $s = cH$ and otherwise, we have to solve a linear system. If there is no solution, a y will never exists so we can just take an instance of ML-DECODING that has no solution either. The polynomial construction of G and H comes from linear algebra.

Exercise 2. To understand the reduction, you have to notice the following facts:

- Since $\{v_i, v_j\}_{i \neq j} \subseteq E$, all the v_i are of different colors. Hence we can assume that v_i is of color i, and we will call the extra color 0.
- The other elements in E not involving the D_i implies that for all i, either u_i is of color i and $\overline{u_i}$ is of color 0 or the opposite. We will interpret this by u_i is 0 (in 3-SAT) iff its color is 0 (in CN).
- Since $m \geq 4$, for each D_f there is a i such that D_f is both connected to u_i and $\overline{u_i}$. So D_f can never be of color 0 and it can only be colored if one of the literal that appear in it get one of the colors in $\{1, \ldots, n\}$.

It is now easy to check that the properties are equivalent:

- From a valid assignment of 3-SAT, we color each pair $(u_i, \overline{u_i})$ with colors i and 0 according to whether u_i is 1 or not. Then we color each clause D_f by the color of one of the literal assigned to 1 in it (which is of color different from 0). We thus get a valid color assignment for CN.
- From a valid color assignment of CN, we interpret the value of each literal as above, and it is easy to verify that we get a valid assignment for the instance of 3-SAT.

Exercise 3. To understand the reduction, you have to notice the following facts:

- The only way to cover V is by using for each $v \in V$ a subset of the first type. We will chose the one for which f correspond to the color associated to it in CN.
- The only way to cover E is by using for each $e = \{u, v\} \in E$ a subset of the second type. We will chose the one for which the colors f_1, f_2 corresponds to the colors associated to u and v.

It is now easy to check that the properties are equivalent:

- From a valid color assignment, we chose the subsets as described above. Amongst the elements of X, the ones corresponding to elements of E or V appears exactly in one subset. Hence we just have to show that it is the case for all the triplet of the form (u, e, f). But for each couple (u, e) the triplet with f equal to the color of u appear in the set S_j covering u and all the other triplet appear in the set S_j covering e.

- From a valid exact cover, we get the colors of the vertices from the set S_j of the first type. It is not possible to have an edge $e = (u, v)$ with u and v of the same color because then the set of the second type used to cover e has some common element with the one covering u or the one covering v.

Exercise 4. To understand the reduction, you have to notice the following facts:

- In the formula defining U, we have two types of subsets. Only the ones of the first type have a first coordinate in the image of α.
- In order to get a 3-DM, for a fixed j, the only way to have $|S_j|$ elements with all possible coordinates of the form (i, j) in the second and last positions is by using either none of the elements of the first type or only elements of the first type. Otherwise, if we look at the second coordinates, $\exists i$ such that (i, j) do not appear in any elements of the first type, but $\pi(i, j) = (i', j)$ does. Then, it is not possible to have (i, j) for a second coordinate of an element of the second type, because it will necessarily have as a third coordinates (i', j) which is already used by the element of the first type having (i', j) as second coordinate.

It is now easy to check that the properties are equivalent:

- From an exact cover, we use the elements of the first type to cover $\alpha(X)$ on the first coordinates and all the (i, j) on the other coordinates with j corresponding to the S_j we use in the exact cover. We then use the elements of the second types to get a 3-DM (we can since none of the $\{(i, j)\}$ for a fixed j partially appears as the second or last coordinates of the elements of the first type we used).
- From a 3-DM, the j that appear as (i, j) in the last coordinates of the elements of the first type are taken for the exact cover. From the same reason as above, if one j is taken, all the $x_i \in S_j$ are taken. We then get the exact cover property for the 3-DM property on the first coordinate.

Exercise 5. A c of weight w such that $cH = 0$ corresponds to w rows of H whose sum (coordinates-wise XOR) is equal to 0. In the following, by first part of H we mean the $(B|I_t| \dots |I_t)$ part.

- from a 3-DM solution, as in the course we will take the $|Z|$ corresponding rows of the first part of H. The sum of all theses rows will be equal to the all 1 vector on the first $3n$ coordinates and will contains $3n|Z|$ ones on the other coordinates. We will then take the $3n(|Z| + 1)$ rows of the second part of H to cancel all theses 1. The corresponding w will thus be $|Z| + 3n(|Z| + 1)$.
- Now suppose we have a WD solution with such a w. It is not possible to have less than $|Z|$ rows on the first part, because the number of rows on the second part has to be exactly equals to the number of 1 in the sum of the rows of the first part. If it is exactly $|Z|$, then the sum of the first part rows is equal to the all one vector on B and a solution to 3-DM follow as in the courses. If it is more than $|Z|$, then we have at least $3n(|Z| + 1)$ one in the sum of the first part rows. That means we need at least $3n(|Z| + 1)$ rows on the second part. But then our total weight is of at least $|Z| + 1 + 3n(|Z| + 1)$ which is 1 more than w, a contradiction.