ETH Zurich
Department of Computer Science

Discrete Mathematics
Prof. Dennis Hofheinz
Autumn Semester 2025

Exercise Sheet 11

Due: December 04, 2025

Vincent Xigu Liu (25-927-229, TA: Moeto Suzuki)

Exercise 11.2

1)

Lemma Ex. 11.2.1:

Let $\|$ denote the concatenation operation. Let $+$ denote the arithmetic sum operation. Then we have

$$\forall x \in \mathcal{C} : \left(\exists a, b \in \bigcup_{i \in \mathbb{N}*} F^i : a \| b = x\right) \to \mathrm{hw}(a) + \mathrm{hw}(b) = \mathrm{hw}(x)$$

Proof.

Let $x = (x_1, x_2, ..., x_n)$ for all sequences x. We define the indicator function:

$$k_i(x) = \begin{cases} 1 \text{ if } x_i \neq 0 \\ 0 \text{ otherwise} \end{cases}$$

Then, we have for the Hamming weight of x the following splitting:

$$k_i(x) = \begin{cases} k_i(a) \text{ if } 1 \leq i \leq |a| \\ k_{i-|a|}(b) \text{ if } |a| + 1 \leq i \leq n \end{cases}$$

which gives

$$\mathrm{hw}(x) = \sum_{i=1}^{n} k_i(x) = \sum_{i=1}^{|a|} k_i(a) + \sum_{i=|a|+1}^{n} k_{i-|a|}(b) = \mathrm{hw}(a) + \mathrm{hw}(b)$$

□

Lemma Ex. 11.2.2:

Let u be a sequence over $F^n, n \in \mathbb{N}^*$. Then,

$$\mathrm{hw}(u) = \mathrm{hw}(-u)$$

Proof. Let $u = (u_1, u_2, ..., u_n)$. Then, we have

$$-u = (-u_1, -u_2, ..., -u_n)$$

and according to the definition of Hamming weight, we have

$$\mathrm{hw}(u) = \sum_{i \in [n]} \begin{cases} 0 \text{ if } u_i = 0 \\ 1 \text{ otherwise} \end{cases}$$

and

$$\mathrm{hw}(-u) = \sum_{i \in [n]} \begin{cases} 0 \text{ if} - u_i = 0 \\ 1 \text{ otherwise} \end{cases}$$

However, according to the properties of a field, we have

$$u_i = 0 \Leftrightarrow -u_i = 0$$

so in all positions $i \in [n]$, the contribution to the Hamming weight from u_i and $-u_i$ are the same. $\square$

According to Lemma Ex. 11.2.1, as

$$x = (x_1, x_2, ..., x_n) = x_1 \parallel x_2 \parallel ... \parallel x_n$$

we have

$$\mathrm{hw}(x) = \sum_{i \in [n]} \mathrm{hw}(x_i) \wedge \mathrm{hw}(y) = \sum_{i \in [n]} \mathrm{hw}(y_i)$$
$$\Rightarrow \mathrm{hw}(x) + \mathrm{hw}(y) = \sum_{i \in [n]} \mathrm{hw}(x_i) + \sum_{i \in [n]} \mathrm{hw}(y_i) = \sum_{i \in [n]} \mathrm{hw}(x_i) + \mathrm{hw}(y_i)$$

analogously, we have

$$\mathrm{hw}(x + y) = \sum_{i \in [n]} \mathrm{hw}(x_i + y_i)$$

We notice that

$$x_i = 0 \wedge y_i = 0 \Rightarrow x_i + y_i = 0 \Rightarrow \mathrm{hw}(x_i + y_i) = 0 \wedge \mathrm{hw}(x_i) + \mathrm{hw}(y_i) = 0 + 0 = 0$$
$$x_i = 0 \wedge y_i \neq 0 \Rightarrow x_i + y_i \neq 0 \Rightarrow \mathrm{hw}(x_i + y_i) = 1 \wedge \mathrm{hw}(x_i) + \mathrm{hw}(y_i) = 0 + 1 = 1$$
$$x_i \neq 0 \wedge y_i = 0 \Rightarrow x_i + y_i \neq 0 \Rightarrow \mathrm{hw}(x_i + y_i) = 1 \wedge \mathrm{hw}(x_i) + \mathrm{hw}(y_i) = 1 + 0 = 1$$
$$x_i \neq 0 \wedge y_i \neq 0 \Rightarrow x_i + y_i \neq 0 \Rightarrow \mathrm{hw}(x_i + y_i) = 1 \wedge \mathrm{hw}(x_i) + \mathrm{hw}(y_i) = 1 + 1 = 2$$

as in all cases,

$$\mathrm{hw}(x_i + y_i) \leq \mathrm{hw}(x_i) + \mathrm{hw}(y_i)$$

we have

$$\mathrm{hw}(x + y) = \sum_{i \in [n]} \mathrm{hw}(x_i + y_i) \leq \sum_{i \in [n]} \mathrm{hw}(x_i) + \mathrm{hw}(y_i) = \mathrm{hw}(x) + \mathrm{hw}(y)$$

with which our claim is proven.

2)

1. $d_{\min}(\mathcal{C}) \leq \min_{c \in \mathcal{C} - \{0^n\}} \mathrm{hw}(c)$:

suppose that there is a $c \in \mathcal{C} - \{0^n\}$ with $\mathrm{hw}(c) < d_{\min}(\mathcal{C})$. Then, the Hemming distance between 0^n and c is exactly $\mathrm{hw}(c)$, so $d(0^n, c) < d_{\min}(\mathcal{C})$ which is a contradiction, so the opposite is proven.

2. $d_{\min}(\mathcal{C}) \geq \min_{c \in \mathcal{C}-\{0^n\}} \operatorname{hw}(c)$:

suppose that there is $a, b \in \mathcal{C}$ with $d(a, b) < \min_{c \in \mathcal{C}-\{0^n\}}$. Then, let $a_n = a + (-a) = 0$, $b_n = b + (-a)$. The hamming distance remains the same because for all positions $i \in [n]$, if $a_i = b_i$ then $a_i + (-a_i) = b_i + (-a_i)$, else $a_i \neq b_i$ implies $a_i + (-a_i) \neq b_i + (-a_i)$. So we have $d(a_n, b_n) = d(a, b) < \min_{c \in \mathcal{C}-\{0^n\}}$. However, $d(a_n, b_n) = \operatorname{hw}(b_n)$ and $b_n \in \mathcal{C} - \{0^n\}$, which is a contradiction. So the opposite is proven.

Combining 1. and 2), we have

$$d_{\min}(\mathcal{C}) = \min_{c \in \mathcal{C}-\{0^n\}} \operatorname{hw}(c)$$

3)

According to 2), we have

$$\begin{aligned} d_{\min}(\mathcal{D}) &= \min_{d \in \mathcal{D}-\{0^{2n}\}} \operatorname{hw}(d) \\ \wedge\, d_{\min}(U) &= \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u) \\ \wedge\, d_{\min}(V) &= \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v) \end{aligned}$$

so it is sufficient to prove that

$$\Rightarrow \min_{d \in \mathcal{D}-\{0^{2n}\}} \operatorname{hw}(d) = \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v)\right)$$

we prove in both directions:

1. $\min_{d \in \mathcal{D}-\{0^{2n}\}} \operatorname{hw}(d) \leq \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v)\right)$:

Case 1: $2 * \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u) \leq \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v)$

In this case, let $v = 0^n$. Then, we have $u \| u \in \mathcal{D}$ and $\operatorname{hw}(u \| u) = 2 * \operatorname{hw}(u)$. Hence, we have

$$\begin{aligned} \min_{d \in \mathcal{D}-\{0^{2n}\}} \operatorname{hw}(d) \leq \operatorname{hw}(u \| u) = 2 * \operatorname{hw}(u) = 2 * \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u) \\ = \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v)\right) \end{aligned}$$

Case 2: $2 * \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u) > \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v)$

In this case, let $u = 0^n$. Then, we have $0^n \| v \in \mathcal{D}$ and $\operatorname{hw}(0^n \| v) = \operatorname{hw}(v)$. Hence, we have

$$\begin{aligned} \min_{d \in \mathcal{D}-\{0^{2n}\}} \operatorname{hw}(d) \leq \operatorname{hw}(0^n \| v) = \operatorname{hw}(v) = \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v) \\ = \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v)\right) \end{aligned}$$

As the case distinction is complete, the claim is proven.

2. $\min_{d \in \mathcal{D}-\{0^{2n}\}} \operatorname{hw}(d) \geq \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \operatorname{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \operatorname{hw}(v)\right)$:

Suppose that there is a $d \in \mathcal{D} - \{0^{2n}\}$ with

$$\mathrm{hw}(d) < \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \mathrm{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \mathrm{hw}(v)\right)$$

Let $d = u \| (u+v)$ with $u \in \mathcal{U}, v \in \mathcal{V}$.

Case 1: $v = 0^n$

In this case, $u \neq 0^n$ because otherwise $d = 0^{2n}$. So we have

$$\mathrm{hw}(d) = \mathrm{hw}(u \| (u + 0^n)) = \mathrm{hw}(u \| u)$$
$$= 2 * \mathrm{hw}(u) \geq 2 * \min_{u \in \mathcal{U}-\{0^n\}} \mathrm{hw}(u) \geq \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \mathrm{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \mathrm{hw}(v)\right)$$

which is a contradiction.

Case 2: $v \neq 0^n$

In this case, we have

$$\mathrm{hw}(d) = \mathrm{hw}(u \| (u+v)) = \mathrm{hw}(u) + \mathrm{hw}(u+v)$$
$$= \mathrm{hw}(-u) + \mathrm{hw}(u+v) \geq \mathrm{hw}(v + u - u)$$
$$= \mathrm{hw}(v) \geq \min_{v \in \mathcal{V}-\{0^n\}} \mathrm{hw}(v) \geq \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \mathrm{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \mathrm{hw}(v)\right)$$

which is a contradiction.

As the case distinction is complete, the claim is proven.

As both directions are proven, we have

$$\min_{d \in \mathcal{D}-\{0^{2n}\}} \mathrm{hw}(d) = \min\left(2 * \min_{u \in \mathcal{U}-\{0^n\}} \mathrm{hw}(u), \min_{v \in \mathcal{V}-\{0^n\}} \mathrm{hw}(v)\right)$$

which is exactly what we wanted to show.