

Tache 4 (Décodage)

Donnée Output liste de 4 nombres dans $\{1, \dots, 8\}$ distincts

1^{er} nombre codage de d (distance minimale)

Output = $[P, D_1, D_2, D_3]$

Résultat : C nombre caché • dans le $\hat{m}$ sous-ensemble que P

$$\bullet d_+(P, C) = d \quad \left(\begin{array}{l} \text{distance minimale à décoder} \\ \text{à partir de } D_1, D_2, D_3 \end{array} \right)$$

$\cap$
 $\{1, \dots, 6\}$

- Décodage de la distance

La distance d est obtenu à partir de $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$.

On note $a < b < c$ des 3 valeurs $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ ordonnées.

Codage d'une distance : $d, a, b, c \rightarrow \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$

	d	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$
distance ①	$\Rightarrow$	a	b	c
distance ②	$\Rightarrow$	a	c	b
distance ③	$\Rightarrow$	b	a	c
distance ④	$\Rightarrow$	b	c	a
distance ⑤	$\Rightarrow$	c	a	b
distance ⑥	$\Rightarrow$	c	b	a

Décodage d'une distance : $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3 \rightarrow d$

?

$$\mathcal{D}_1 < \mathcal{D}_2 < \mathcal{D}_3 \Rightarrow d = 1$$

$$\mathcal{D}_1 < \mathcal{D}_3 < \mathcal{D}_2 \Rightarrow d = 2$$

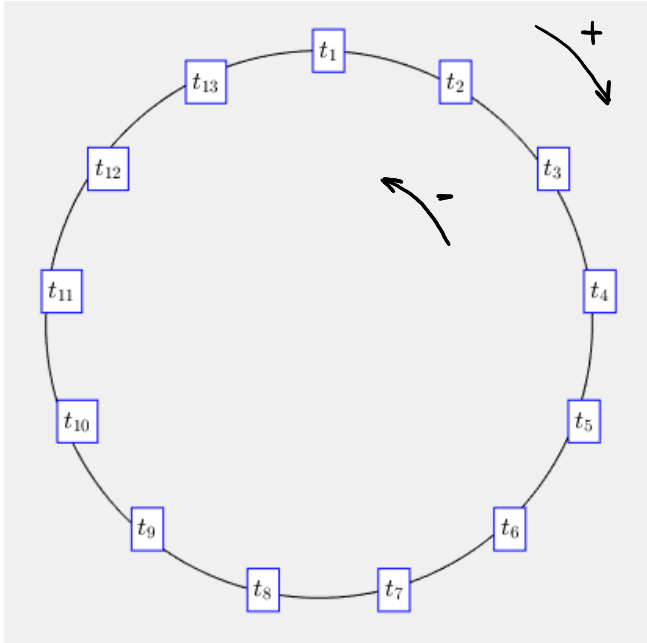
$$\mathcal{D}_2 < \mathcal{D}_1 < \mathcal{D}_3 \Rightarrow d = 3$$

$$\mathcal{D}_3 < \mathcal{D}_1 < \mathcal{D}_2 \Rightarrow d = 4$$

$$\mathcal{D}_2 < \mathcal{D}_3 < \mathcal{D}_1 \Rightarrow d = 5$$

$$\mathcal{D}_3 < \mathcal{D}_2 < \mathcal{D}_1 \Rightarrow d = 6$$

Distance circulaire



Il faut déterminer le nombre caché C à partir
de $P = \text{output}[0]$ et $d_+(P, C) = d \in \{1, \dots, 6\}$

On pose

$$G = P + d$$

si G et P ∈ au $\sim m$ sous ensemble alors
 $C = G$?

sinon

$$C = G - 13$$
$$= P - (13 - d)$$