

Théorème de Fine-Wilf

Travail
01

Ceci est une proposition de correction. Il existe d'autres chemins pour arriver au même résultat.

Partie 1 : Cas des mots infinis

Pour un alphabet $\mathcal{A}$, un mot infini est un élément de $\mathcal{A}^{\mathbb{N}}$. Un entier $p \in \mathbb{N}$ est une période d'un mot infini x si pour tout $j \in \mathbb{N}$, $x_j = x_{j+p}$.

Exercice 1

1. Montrer que pour tout mot infini, 0 est une période.
2. Montrer que l'ensemble des périodes d'un mot infini est de la forme $p\mathbb{N}$, où $p \in \mathbb{N}$.

Solution.

1. Soit $x \in \mathcal{A}^{\mathbb{N}}$. Alors pour tout $j \in \mathbb{N}$, $x_j = x_{j+0}$. Donc 0 est une période de x .

2. Soit $x \in \mathcal{A}^{\mathbb{N}}$, et soit $P \subseteq \mathbb{N}$ l'ensemble des périodes de x .

Traisons d'abord le cas où $P = \{0\}$: alors $P = 0\mathbb{N}$.

Maintenant, si $P \neq \{0\}$, P contient des éléments strictement positifs. Soit p le plus petit élément de P strictement positif. Soit p' une autre période de x . Procédons à la division euclidienne de p' par p : on dispose d'entiers $q \in \mathbb{N}$ et $0 \leq r < p$ tels que $p' = pq + r$.

Pour tout $j \in \mathbb{N}$, on a $x_j = x_{j+p'} = x_{j+pq+r} = x_{j+p+p+\dots+p+r} = x_{j+r}$ par p -périodicité de x . Donc r est aussi une période de x . Si $r \neq 0$, on aurait alors $r < p$ une autre période de x strictement positive et strictement plus petite que p : absurde ! Donc $r = 0$. Donc $p' = qp$, donc $p' \in p\mathbb{N}$. Donc $P \subseteq p\mathbb{N}$.

Pour montrer $p\mathbb{N} \subseteq P$, il suffit de procéder à une simple récurrence.

Partie 2 : Cas des mots finis

Pour un mot fini m , un entier $p \in \mathbb{N}$ est une période de m si pour tout $0 \leq j \leq |m| - p - 1$, $m_j = m_{j+p}$.

Exercice 2

1. Justifier que *abbabb* et *bamba* sont tous deux 3-périodiques.
2. Justifier que *oui* est 5-périodique.

Solution.

1.

<i>a</i>	<i>b</i>	<i>b</i>	<i>a</i>	<i>b</i>	<i>b</i>			
			<i>a</i>	<i>b</i>	<i>b</i>	<i>a</i>	<i>b</i>	<i>b</i>

<i>b</i>	<i>a</i>	<i>m</i>	<i>b</i>	<i>a</i>			
			<i>b</i>	<i>a</i>	<i>m</i>	<i>b</i>	<i>a</i>

2.

<i>o</i>	<i>u</i>	<i>i</i>					
					<i>o</i>	<i>u</i>	<i>i</i>

Dans le cas des mots finis, l'équivalent du résultat évoqué dans la partie précédente est le théorème de Fine-Wilf, dont la démonstration est l'objectif de ce DM :

Théorème 1 : théorème de Fine-Wilf

Soit $m \in \mathcal{A}^*$ un mot, et p et q deux périodes de m . On suppose que $|m| \geq p + q - \text{PGCD}(p, q)$. Alors m admet aussi $\text{PGCD}(p, q)$ comme période.

Exercice 3

Démontrer le théorème de Fine-Wilf dans le cas où l'un de p ou de q est nul.

Solution.

On étudie le cas $p = 0$, l'autre étant symétrique. Alors $\text{PGCD}(p, q) = q$: donc $\text{PGCD}(p, q)$ est bien une période de m .

Exercice 4

Soit m un mot fini et p et q deux de ses périodes non nulles. On fait deux hypothèses supplémentaires :

- p et q sont premiers entre eux;
- $|m| = p + q - \text{PGCD}(p, q)$.

1. On considère la fonction suivante :

$$f : \begin{pmatrix} \llbracket 0, p + q - 1 \rrbracket & \rightarrow & \llbracket 0, p + q - 1 \rrbracket \\ x & \mapsto & \begin{cases} x + p & \text{si } x < q \\ x - q & \text{sinon} \end{cases} \end{pmatrix}$$

- a) Montrer que $f(\llbracket 0, q - 1 \rrbracket) = \llbracket p, p + q - 1 \rrbracket$ et que $f(\llbracket q, p + q - 1 \rrbracket) = \llbracket 0, p - 1 \rrbracket$.
- b) En déduire que f est une permutation de $\llbracket 0, p + q - 1 \rrbracket$.

2. Soit j l'ordre de 0 pour cette permutation.

- a) Justifier que $j \leq p + q$.
- b) Montrer qu'il existe a et b deux entiers tels que $j = a + b$ et $ap - bq = 0$.
- c) En déduire que $j \geq p + q$.

3. Montrer que m est un mot constant.

Solution.

- 1. a) Pour tout x vérifiant $0 \leq x \leq q - 1$, on a $f(x) = x + p$, donc $p \leq x \leq p + q - 1$. Donc $f(\llbracket 0, q - 1 \rrbracket) \subseteq \llbracket p, p + q - 1 \rrbracket$. De plus, f est injective (c'est une fonction linéaire de pente non nulle), et les deux intervalles sont de même cardinal fini : donc f est aussi bijective.
Un raisonnement analogue s'applique pour montrer $f(\llbracket q, p + q - 1 \rrbracket) = \llbracket 0, p - 1 \rrbracket$.
- b) Montrons que f est injective : soient $x \neq y$ deux éléments de $\llbracket 0, p + q - 1 \rrbracket$.
Si x et y appartiennent tous deux à $\llbracket 0, q - 1 \rrbracket$, l'injectivité de f sur cet intervalle évoquée à la question précédente permet d'en déduire que $f(x) \neq f(y)$. Un raisonnement analogue s'applique au cas où x et y appartiennent tous deux à $\llbracket q, p + q - 1 \rrbracket$.
Si $x \in \llbracket 0, q - 1 \rrbracket$ et $y \in \llbracket q, p + q - 1 \rrbracket$, alors $f(x) \in \llbracket p, p + q - 1 \rrbracket$ et $f(y) \in \llbracket 0, p - 1 \rrbracket$; ces deux ensembles sont d'intersection vide; donc $f(x) \neq f(y)$.
Donc f injective d'un ensemble fini dans lui-même; donc f est bijective.
- 2. a) Pour tout élément d'une permutation, son ordre est plus petit que la taille de l'ensemble étudié. Donc $j \leq p + q$.
- b) On sait que $f^j(0) = 0$. Distinguons, dans ces itérations successives de f , celles où on a ajouté p et celles où on a retiré q : supposons avoir appliqué a fois la première règle, et b fois la seconde. On a donc $j = a + b$.

En partant de 0, appliquer a fois la première règle consiste à ajouter a fois p ; appliquer b fois la seconde consiste à retirer b fois q . Donc $f^j(0) = 0 + ap - bq$: donc $0 = ap - bq$.

c) On a $ap = bq$. Mais p et q sont supposés premiers entre eux : donc, d'après le lemme de Gauß, $p \mid b$ et $q \mid a$. Ni a ni b ne peut être nul; donc $p \leq b$ et $q \leq a$. Donc $p + q \leq a + b = j$: donc $j \geq p + q$.

3. On déduit des questions précédentes que $j = p + q$: donc, dans la permutation f , 0 se trouve dans un cycle de longueur $p + q$; donc f est en fait composée d'un seul cycle de longueur $p + q$. Donc, pour tout $j \in \llbracket 0, p + q - 1 \rrbracket$, il existe $k_j \in \mathbb{N}$ tel que $f^{k_j}(0) = j$.

On remarque par ailleurs que pour tout $i \in \llbracket 0, p + q - 1 \rrbracket$, $m_i = m_{f(i)}$ par p ou q -périodicité de m ; donc pour tout $j \in \llbracket 0, p + q - 1 \rrbracket$, $m_j = m_{f^{k_j}(0)} = m_0$. Donc m est constant.

Exercice 5

Soit m un mot et p et q deux de ses périodes non nulles. On ne suppose plus que p et q sont premiers entre eux, mais on suppose toujours que $|m| = p + q - \text{PGCD}(p, q)$. On note $d = \text{PGCD}(p, q)$.

On pose $m^{(i)} = m_i m_{i+d} m_{i+2d} m_{i+3d} \dots$ le sous-mot obtenu en sautant de d lettres en d lettres dans m à partir de la position i , pour $0 \leq i < d$.

1. Déterminer la longueur des $m^{(i)}$.
2. Montrer que p/d et q/d sont des périodes des $m^{(i)}$.
3. En déduire que m admet d comme période.

Solution.

1. On remarque que pour construire $m^{(i)}$, on prend une lettre sur d dans m . Donc comme m contient $p + q - d$ lettres, $m^{(i)}$ contient $\frac{p + q - d}{d} = p/d + q/d - 1$ lettres.

2. Pour tout $k \in \llbracket 0, q/d - 1 \rrbracket$, on a $m_k^{(i)} = m_{i+kd} = m_{i+kd+p} = m_{i+kd+p/d \times d} = m_{i+d \times (k+p/d)} = m_{k+p/d}^{(i)}$: donc p/d est bien une période de $m^{(i)}$. La condition $k \leq q/d - 1$ assure qu'on ne va pas trop loing dans le mot.

Un raisonnement analogue donne que q/d est aussi une période de $m^{(i)}$.

3. Pour tout i , on a donc $m^{(i)}$ admettant p/d et q/d comme périodes, et de longueur $p/d + q/d - 1$, avec p/d et q/d premiers entre eux : on peut appliquer l'exercice 4 et en déduire que $m^{(i)}$ est constant. Donc, pour tout $i \in \llbracket 0, p + q - 2d \rrbracket$, $m_i = m_{i+d}$: donc d est bien une période de m .

Exercice 6

Soit m un mot, et p et q deux de ses périodes non nulles, de PGCD d . On suppose finalement que $|m| \geq p + q - d$.

1. Montrer que $m_{\llbracket 0, p+q-d-1 \rrbracket}$ (le préfixe de m de longueur $p + q - d$) admet d comme période.
2. En déduire que m admet d comme période.

Solution.

1. C'est une application de l'exercice 5 à $m_{\llbracket 0, p+q-d-1 \rrbracket}$.

2. On montre par récurrence forte que pour tout $i \in \llbracket 0, |m| - d - 1 \rrbracket$, $m_i = m_{i+d}$.

Initialisation : pour $i \leq p + q - 2d - 1$, $m_i = m_{i+d}$ par d -périodicité du préfixe de m de longueur $p + q - d$.

Hérédité : pour $i \geq p + q - 2d$, on a $m_i = m_{i+d}$, alors $m_{i+1} = m_{i-p+1} \stackrel{\text{HR}}{=} m_{i-p+1+d} = m_{i+1+d}$.