

Option Informatique en Spé MP et MP*

DS du 5 mars 2002 : le corrigé

Question 1 • $|\Sigma| = 2$ donc $0 \leq a_n \leq |L \cap \Sigma^n| = 2^n$, si bien que le rayon de convergence est au moins égal à 2.

Question 2 • $L \cap M = \emptyset$ implique $(L \cap \Sigma^n) \cap (M \cap \Sigma^n) = \emptyset$ donc :

$$\begin{aligned} [z^n](f_{L \cup M})(z) &= \text{Card}((L \cup M) \cap \Sigma^n) = \text{Card}(L \cap \Sigma^n) + \text{Card}(M \cap \Sigma^n) \\ &= [z^n](f_L)(z) + [z^n](f_M)(z) = [z^n](f_L + f_M)(z) \end{aligned}$$

Nous en déduisons $f_{L \cup M} = f_L + f_M$.

Question 3 • Il est clair que $(L \cdot M) \cap \Sigma^n = \bigcup_{0 \leq k \leq n} (L \cap \Sigma^k) \cdot (M \cap \Sigma^{n-k})$. L'hypothèse de l'énoncé fait que les $n + 1$ ensembles qui interviennent dans cette réunion sont deux à deux disjoints ; d'où :

$$\begin{aligned} [z^n](f_{L \cdot M})(z) &= \text{Card}((L \cdot M) \cap \Sigma^n) = \sum_{0 \leq k \leq n} \text{Card}(L \cap \Sigma^k) \times \text{Card}(M \cap \Sigma^{n-k}) \\ &= \sum_{0 \leq k \leq n} [z^k]f_L(z) \times [z^{n-k}]f_M(z) = [z^n](f_L \times f_M)(z) \end{aligned}$$

Nous en déduisons $f_{L \cdot M} = f_L \times f_M$.

Question 4 • f_L est polynomiale ssi $a_n = 0$ APCR ce qui revient à dire que la longueur des éléments de L est bornée, ou encore que L est fini.

Question 5 • L_1 est l'ensemble des mots dont $\mathbf{0}$ n'est pas facteur, c'est donc $\mathbf{1}^*$; par suite, $[z^n]f_1(z) = 1$ puis $f_1(z) = \sum_{n \in \mathbb{N}} z^n = \frac{1}{1-z}$.

Question 6 • $L_2 \cap \Sigma^0 = \{\varepsilon\}$, donc $a_0 = 1$; $L_2 \cap \Sigma^1 = \{\mathbf{0}, \mathbf{1}\}$, donc $a_1 = 2$. $L_2 \cap \Sigma^{n+2}$ est l'union disjointe des deux ensembles suivants :

- $L_2 \cap (\Sigma^{n+1} \cdot \{\mathbf{1}\})$: c'est l'ensemble des mots de L_2 , de longueur $n + 2$, et dont la dernière lettre est $\mathbf{1}$;
- $L_2 \cap (\Sigma^n \cdot \{\mathbf{10}\})$: c'est l'ensemble des mots de L_2 , de longueur $n + 2$, et dont la dernière lettre est $\mathbf{0}$; cette condition implique que l'avant-dernière lettre est $\mathbf{1}$.

Nous en déduisons $a_{n+2} = a_{n+1} + a_n$. La suite $(a_n)_{n \in \mathbb{N}}$ vérifie la même relation de récurrence que la suite de FIBONACCI ; les premiers termes de celle-ci sont $F_0 = 0$, $F_1 = 1$, $F_2 = 1$ et $F_3 = 2$. Nous en déduisons $a_n = F_{n+2}$. Alors $f_2(z) = \sum_{n \in \mathbb{N}} a_n z^n$ vérifie :

$$\begin{aligned} f_2(z) &= a_0 + a_1 z + \sum_{n \geq 2} a_n z^n = 1 + 2z + \sum_{n \in \mathbb{N}} a_{n+2} z^{n+2} = 1 + 2z + \sum_{n \in \mathbb{N}} (a_{n+1} + a_n) z^{n+2} \\ &= 1 + 2z + z \sum_{n \in \mathbb{N}} a_{n+1} z^{n+1} + z^2 \sum_{n \in \mathbb{N}} a_n z^n = 1 + 2z + z(f_2(z) - 1) + z^2 f_2(z) \end{aligned}$$

Donc $(1 - z - z^2)f_2(z) = 1 + z$, d'où nous déduisons $f_2(z) = \frac{1+z}{1-z-z^2}$.

Question 7 • L_k est la réunion de deux ensembles :

- l'ensemble des mots de L_k ne contenant aucune occurrence de $\mathbf{1}$; ces mots sont de la forme $\mathbf{0}^j$ avec $0 \leq j < k$; leur ensemble est précisément M_k ;
- l'ensemble des mots de L_k contenant au moins une occurrence de $\mathbf{1}$; ces mots sont de la forme $\mathbf{0}^j \mathbf{1} w$ avec $0 \leq j < k$ et $w \in L_k$, donc leur ensemble est exactement $M_k \cdot \{\mathbf{1}\} \cdot L_k$.

L'égalité $L_k = M_k \cup (M_k \cdot \{\mathbf{1}\} \cdot L_k)$ en résulte immédiatement. Remarquons que cette union est disjointe.

Question 8 • Notons $a_n = [z^n]f_{L_k}(z)$ et exploitons le résultat précédent :

$$a_n = \text{Card}(L_k \cap \Sigma^n) = \text{Card}(M_k \cap \Sigma^n) + \text{Card}((M_k \cdot \{1\}) \cdot L_k \cap \Sigma^n)$$

Distinguons deux cas de figure selon que n est strictement inférieur à k , ou supérieur ou égal à k .

• Si $n < k$, alors $M_k \cap \Sigma^n = \{\mathbf{0}^n\}$. Si $n = 0$, alors $(M_k \cdot \{1\}) \cdot L_k \cap \Sigma^n = \emptyset$, ce qui nous donne $a_0 = 1$; sinon, pour chaque $j \in \llbracket 0, n-1 \rrbracket$, M_k contient un et un seul mot de longueur j (à savoir $\mathbf{0}^j$) si bien que

$$(M_k \cdot \{1\}) \cdot L_k \cap \Sigma^n = \bigcup_{0 \leq j < n} (\{\mathbf{0}^j\} \cdot \{1\} \cdot L_k) \cap \Sigma^n = \bigcup_{0 \leq j < n} \{\mathbf{0}^j \mathbf{1}\} \cdot (L_k \cap \Sigma^{n-j-1})$$

Cette union est clairement disjointe, si bien que :

$$a_n = 1 + \sum_{j=0}^{n-1} \text{Card}(L_k \cap \Sigma^{n-j-1}) = 1 + \sum_{j=0}^{n-1} a_{n-j-1} = 1 + \sum_{j=1}^n a_{n-j}$$

• Si $n \geq k$, alors $M_k \cap \Sigma^n = \emptyset$; le raisonnement qui vient d'être tenu pour $n < k$ s'applique encore, si bien que :

$$\begin{aligned} (M_k \cdot \{1\}) \cdot L_k \cap \Sigma^n &= \bigcup_{0 \leq j < k} (\{\mathbf{0}^j\} \cdot \{1\} \cdot L_k) \cap \Sigma^n = \bigcup_{0 \leq j < k} \{\mathbf{0}^j \mathbf{1}\} \cdot (L_k \cap \Sigma^{n-j-1}) \\ a_n &= \sum_{j=0}^{k-1} \text{Card}(L_k \cap \Sigma^{n-j-1}) = \sum_{j=0}^{k-1} a_{n-j-1} = \sum_{j=1}^k a_{n-j} \end{aligned}$$

Nous pouvons maintenant écrire :

$$\begin{aligned} f_{L_k}(z) &= \sum_{n \in \mathbb{N}} a_n z^n = a_0 + \sum_{n=1}^{k-1} a_n z^n + \sum_{n \geq k} a_n z^n = 1 + \sum_{n=1}^{k-1} \left(1 + \sum_{j=1}^n a_{n-j}\right) z^n + \sum_{n \geq k} \sum_{j=1}^k a_{n-j} z^n \\ &= \sum_{n=0}^{k-1} z^n + \sum_{n=1}^{k-1} \sum_{j=1}^n a_{n-j} z^n + \sum_{j=1}^k \sum_{n \geq k} a_{n-j} z^n = \frac{1-z^k}{1-z} + \sum_{j=1}^{k-1} \sum_{n=j}^{k-1} a_{n-j} z^n + \sum_{j=1}^k \sum_{n \geq k} a_{n-j} z^n \\ &= \frac{1-z^k}{1-z} + \sum_{j=1}^{k-1} z^j \sum_{n=j}^{k-1} a_{n-j} z^{n-j} + \sum_{j=1}^k z^j \sum_{n \geq k} a_{n-j} z^{n-j} \\ &= \frac{1-z^k}{1-z} + \sum_{j=1}^{k-1} z^j \sum_{n=0}^{k-1-j} a_n z^n + \sum_{j=1}^k z^j \sum_{n \geq k-j} a_n z^n \\ &= \frac{1-z^k}{1-z} + \sum_{j=1}^{k-1} z^j \sum_{n \geq 0} a_n z^n + z^k \sum_{n \geq 0} a_n z^n = \frac{1-z^k}{1-z} + \sum_{j=1}^{k-1} z^j f_{L_k}(z) + z^k f_{L_k}(z) \\ &= \frac{1-z^k}{1-z} + \sum_{j=1}^k z^j f_{L_k}(z) \end{aligned}$$

Nous en déduisons la relation $\left(1 - \sum_{j=1}^k z^j\right) f_{L_k}(z) = \frac{1-z^k}{1-z}$. Mais :

$$1 - \sum_{j=1}^k z^j = 1 - \sum_{j=0}^{k-1} z^{j+1} = 1 - z \sum_{j=0}^{k-1} z^j = 1 - z \frac{1-z^k}{1-z} = \frac{1-2z+z^{k+1}}{1-z}$$

Donc $\frac{1-2z+z^{k+1}}{1-z} f_{L_k}(z) = \frac{1-z^k}{1-z}$ et finalement $f_{L_k}(z) = \frac{1-z^k}{1-2z+z^{k+1}}$.

Question 9 • Pour $k = 1$, nous obtenons $f_1(z) = \frac{1-z}{1-2z+z^2} = \frac{1-z}{(1-z)^2} = \frac{1}{1-z}$; et pour $k = 2$, nous obtenons $f_2(z) = \frac{1-z^2}{1-2z+z^3} = \frac{(1-z)(1+z)}{(1-z)(1-z-z^2)} = \frac{1+z}{1-z-z^2}$.

Question 10 • Remarquons que $1 - z^k = (1 - z)P_k(z)$. Par ailleurs, $1 - 2z + z^{k+1} = (1 - z)\left(1 - \sum_{j=1}^k z^j\right)$.

Notant $Q_k = 1 - \sum_{j=1}^k X^j$, nous aurons $f_k(z) = \frac{P_k(z)}{Q_k(z)}$.

• Le calcul mené à la question 8 montre que $Q_k(z) = 1 - zP_k(z)$, donc $XP_k + Q_k = 1$; le théorème de BÉZOUT permet d'affirmer que P_k et Q_k n'ont pas de facteur commun.

Question 11 • Raisonnons par l'absurde. Soit α une racine multiple de Q_k : alors $Q'_k(\alpha) = 0$. Mais $Q'_k = (k+1)X_k - 2$, donc $\alpha^k = \frac{2}{k+1}$. Alors:

$$Q_k(\alpha) = \alpha^{k+2} - 2\alpha + 1 = \frac{2\alpha}{k+1} - 2\alpha + 1 = \frac{k+1-2k\alpha}{k+1}$$

$Q_k(\alpha) = 0$ implique $\alpha = \frac{k+1}{2k}$ donc $\frac{2}{k+1} = \left(\frac{k+1}{2k}\right)^k$ puis $2^{k+1}k^k = (k+1)^{k+1}$: nécessairement k est impair, $k = 2q + 1$. Nous en déduisons $2^{2q+2}(2q+1)^{2q+1} = (2q+2)^{2q+2}$ d'où (en simplifiant par 2^{2q+2}) l'égalité $(2q+1)^{2q+1} = (q+1)^{2q+2}$ puis $q+1 = \left(\frac{2q+1}{q+1}\right)^{2q+1}$. Comme $q+1 \in \mathbb{N}$, il faut $q = 0$ puis $k = 1$ ce qui est exclu par l'énoncé.

Question 12 • La restriction de $Q_k : x \mapsto 1 - \sum_{i=1}^k x^i$ à l'intervalle $\mathbb{R}_+ = [0, +\infty[$ est continue et strictement décroissante; elle réalise donc une bijection de \mathbb{R}_+ sur l'intervalle $] \lim_{x \rightarrow +\infty} Q_k(x), Q_k(0)] =]-\infty, 1]$. Par suite, elle s'annule une fois et une seule sur \mathbb{R}_+ ; comme $Q_k(0) = 1 > 0$, nous pouvons même affirmer qu'elle s'annule sur \mathbb{R}_+^* .

• Remarquons que $Q_k(1) = 1 - k < 0$ (puisque $k \geq 2$) tandis que $Q_k(1/2) = 1 - \sum_{i=1}^k 2^{-i} = 2^{-k} > 0$.

Conclusion: $1/2 < \alpha < 1$.

Question 13 • $T_k = X^k Q_k(1/X) = X^k \left(1 - \sum_{j=1}^k X^{-j}\right) = X^k - \sum_{j=1}^k X^{k-j} = X^k - \sum_{j=0}^{k-1} X^j = X^k - P_k$.

Question 14 • $T_k(x) = 0$ ssi $x^k Q_k(1/x) = 0$; $x = 0$ étant exclu, la seule possibilité est $Q_k(1/x) = 0$, soit $x = 1/\alpha$ puisque nous cherchons les solutions sur \mathbb{R}_+^* . Ainsi $\beta = 1/\alpha$; de l'encadrement $1/2 < \alpha < 1$, nous en déduisons $1 < \beta < 2$.

Question 15 • En développant et en identifiant, nous obtenons les égalités $\lambda_1 - \beta = -1$; $\lambda_i - \beta\lambda_{i-1} = -1$ pour $i \in \llbracket 2, k-2 \rrbracket$; et $-\beta\lambda_{k-1} = -1$. Il est commode de définir $\lambda_0 = 1$, ainsi $\lambda_j - \beta\lambda_{j-1} = -1$ pour $j \in \llbracket 1, k-2 \rrbracket$; cette dernière égalité peut s'écrire $\frac{\lambda_j}{\beta^j} - \frac{\lambda_{j-1}}{\beta^{j-1}} = -\frac{1}{\beta^j}$, ce qui se prête à un télescopage:

$$\frac{\lambda_i}{\beta^i} = \frac{\lambda_0}{\beta^0} - \sum_{1 \leq j \leq i} \frac{1}{\beta^j} \text{ d'où } \lambda_i = \beta^i - \sum_{1 \leq j \leq i} \beta^{i-j}, \text{ soit enfin, avec un changement d'indice: } \lambda_i = \beta^i - \sum_{0 \leq j < i} \beta^j.$$

Cette formule reste valable pour $i = k-1$; en effet:

$$\beta^{k-1} - \sum_{0 \leq j < k-1} \beta^j = \frac{1}{\beta} \left(\beta^k - \sum_{1 \leq j < k} \beta^j \right) = \frac{1}{\beta} (T_k(\beta) + 1) = \frac{1}{\beta} = \lambda_{k-1}$$

Question 16 • Raisonnons par récurrence sur $i \in \llbracket 1, k-1 \rrbracket$. $\lambda_{k-1} = \frac{1}{\beta} > 0$ car $\beta > 1$. Supposons acquise l'inégalité $\lambda_{k-i} > 0$ avec $0 \leq i < k-1$; alors $\lambda_{k-i-1} = \frac{1 + \lambda_{k-i}}{\beta} > 0$. Donc $\lambda_{k-i} > 0$ pour tout $i \in \llbracket 1, k-1 \rrbracket$, soit encore $\lambda_i > 0$ pour tout $i \in \llbracket 1, k-1 \rrbracket$.

• Raisonnons à nouveau par récurrence. $\lambda_1 = \beta - 1 < 1$ car $\beta < 2$. Supposons acquise l'inégalité $\lambda_i < 1$ avec $1 \leq i < k-1$; $\lambda_{i+1} = \beta\lambda_i - 1$; $1 < \beta < 2$ et $0 < \lambda_i < 1$ impliquent $\beta\lambda_i < 2$, donc $\lambda_{i+1} < 1$. Ainsi $\lambda_i < 1$ pour tout $i \in \llbracket 1, k-1 \rrbracket$.

Question 17 • La fraction rationnelle $\frac{P_k}{Q_k}$ est réduite et de degré négatif puisque $\deg P_k = k-1$ et $\deg Q_k = k$. Les racines de Q_k sont simples, puisque ce sont des racines de $1 - 2X + X^{k+1}$; notons-les

z_1, \dots, z_k . Alors la D.E.S. de notre fraction s'écrit $\frac{P_k}{Q_k} = \sum_{1 \leq i \leq k} \frac{\gamma_i}{X - z_i}$ avec $\gamma_i = \frac{P_k(z_i)}{Q'_k(z_i)}$. Nous pouvons écrire :

$$\begin{aligned} f_k(z) &= \frac{P_k(z)}{Q_k(z)} = \sum_{1 \leq i \leq k} \frac{\gamma_i}{z - z_i} = - \sum_{1 \leq i \leq k} \frac{\gamma_i}{z_i - z} = - \sum_{1 \leq i \leq k} \frac{\gamma_i}{z_i} \times \frac{1}{1 - \frac{z}{z_i}} \\ &= - \sum_{1 \leq i \leq k} \frac{\gamma_i}{z_i} \left(\sum_{n \in \mathbb{N}} \left(\frac{z}{z_i} \right)^n \right) = \sum_{n \in \mathbb{N}} \left(- \sum_{1 \leq i \leq k} \frac{\gamma_i}{(z_i)^{n+1}} \right) z^n \end{aligned}$$

Ainsi $a_n = - \sum_{1 \leq i \leq k} \frac{\gamma_i}{(z_i)^{n+1}}$. Or les racines z_i de Q_k sont les inverses des racines de T_k ; notons celles-ci u_1, \dots, u_k avec $u_1 = \beta$, ainsi $a_n = - \sum_{1 \leq i \leq k} \gamma_i (u_i)^{n+1}$. Comme $|u_i| < \beta$ pour $i \geq 2$, chacun des termes $\gamma_i (u_i)^{n+1}$ d'indice $i \geq 2$ est négligeable devant $\gamma_1 \beta^{n+1}$, si bien que a_n est équivalent à $-\gamma_1 \beta^{n+1}$ lorsque n tend vers l'infini. Ceci montre que la suite de terme général $\frac{a_n}{\beta^n}$ converge vers $\mu = -\gamma_1 \beta$.

• Il reste à exprimer γ_1 en fonction de β et k . $z_1 = 1/u_1 = 1/\beta = \alpha$, donc $\gamma_1 = \frac{P_k(z_1)}{Q'_k(z_1)} = \frac{P_k(\alpha)}{Q'_k(\alpha)}$. Mais :

$$P_k(\alpha) = \sum_{0 \leq i < k} \alpha^i = \frac{1 - \alpha^k}{1 - \alpha} = \frac{1 - \beta^{-k}}{1 - 1/\beta} = \beta^{1-k} \frac{\beta^k - 1}{\beta - 1}$$

D'autre part, $Q_k = 1 - \sum_{i=1}^k X^i$, donc $Q'_k = - \sum_{i=1}^k i X^{i-1}$ puis :

$$Q'_k(\alpha) = - \sum_{i=1}^k i \alpha^{i-1} = - \frac{k - (k+1)\alpha + \alpha^{k+1}}{(1 - \alpha)^2} = - \frac{k - (k+1)/\beta + \beta^{-k-1}}{(1 - 1/\beta)^2} = \beta^{1-k} \frac{k\beta^{k+1} - (k+1)\beta^k + 1}{(\beta - 1)^2}$$

Nous en déduisons $\mu = - \frac{\beta(\beta - 1)(k\beta^{k+1} - (k+1)\beta^k + 1)}{\beta^k - 1}$.

Question 18 • β_k est l'inverse du réel strictement positif α_k qui annule $Q_k : x \mapsto 1 - \sum_{j=1}^k x^j$. Mettons en évidence la monotonie de la suite $(\alpha_k)_{k \geq 2}$:

$$Q_{k+1}(\alpha_k) = 1 - \sum_{j=1}^{k+1} (\alpha_k)^j = 1 - \sum_{j=1}^k (\alpha_k)^j - (\alpha_k)^{k+1} = Q_k(\alpha_k) - (\alpha_k)^{k+1} = -(\alpha_k)^{k+1} < 0$$

Q_{k+1} est strictement décroissante sur \mathbb{R}_+ , et $Q_{k+1}(\alpha_{k+1}) = 0$. Donc $\alpha_k > \alpha_{k+1}$: la suite $(\alpha_k)_{k \geq 2}$ est strictement décroissante. Comme elle est minorée (par $1/2$), elle converge vers une limite au plus égale à $1/2$. En notant ℓ l'inverse de cette limite, nous pouvons affirmer que la suite $(\beta_k)_{k \geq 2}$ converge vers ℓ . Nous allons montrer que $\ell = 2$. Pour ce faire, observons le signe de $T_k(\ell)$:

$$T_k(\ell) = \ell^k - \sum_{j=0}^{k-1} \ell^j = \ell^k - \frac{1 - \ell^k}{1 - \ell} = \frac{\ell^k - \ell^{k+1} - 1 + \ell^k}{1 - \ell} = \frac{\ell^k(2 - \ell) - 1}{1 - \ell}$$

$1/\ell < \alpha_k$, donc $T_k(\ell) > 0$; Comme $1 - \ell < 0$, nous en déduisons $\ell^k(2 - \ell) - 1 < 0$. Ceci n'est possible que si $\ell = 2$; en effet, si $\ell < 2$, la suite de terme général $\ell^k(2 - \ell) - 1$ diverge vers $+\infty$.

Question 19 • $c_0 = 1$; $c_1 = 0$ car **010010** \neq **100101** ; de même, nous trouvons $c_2 = 0$, $c_3 = 0$, $c_4 = 0$, $c_5 = 1$ et $c_6 = 0$. Finalement $P_m = 1 + X^5$.

Question 20 • Soit $m = abcde \in \Sigma^5$, de PACO $1 + X^3 + X^4$. $c_4 = 1$, donc $e = a$; $c_3 = 1$, donc $de = ab$, soit $d = a$ et $e = b$; ainsi $a = b = d = e$. $c_2 = 0$, donc $abc \neq cde$; comme $b = d$, ceci implique $a \neq c$ ou $c \neq e$; come $a = e$, ceci équivaut à $a \neq c$. Donc $m = \mathbf{00100}$ ou $m = \mathbf{11011}$. Vérifions que ces deux mots conviennent.

Question 21 • Soit $m = abcdef \in \Sigma^6$, de PACO $1 + X^3 + X^4$. $c_5 = 0$ implique $f \neq a$. $c_4 = 1$ implique $ab = ef$, donc $a = e$ et $b = f$. $c_3 = 1$ implique $abc = def$, donc $a = d$, $b = e$ et $c = f$. Mais alors $a = b = c = d = e = f$, ce qui est contradictoire. Il n'existe donc aucun mot de longueur 6 dont le PACO est $1 + X^3 + X^4$.

Question 22 • Preuve de $G_m \cup W_m \subset \{\varepsilon\} \cup (G_m \cdot \Sigma)$.

Soit $u \in G_m \cup W_m$; si $|u| = 0$, alors $u \in \{\varepsilon\}$. Sinon, $u = vx$ avec $x \in \Sigma$ et $|v| = |u| - 1$; si $u \in G_m$, alors m n'est pas facteur de u , donc n'est pas facteur de v ; si $u \in W_m$, alors u admet m comme suffixe, mais aucun autre facteur de u n'est égal à m , donc m ne peut être facteur de v ; dans tous les cas, m n'est pas facteur de v , donc $v \in G_m$ et $u \in G_m \cdot \Sigma$.

• Preuve de $\{\varepsilon\} \cup (G_m \cdot \Sigma) \subset G_m \cup W_m$.

m ne peut être facteur de ε , donc $\varepsilon \in G_m$. Soit $u \in G_m \cdot \Sigma$: si m n'est pas facteur de u , alors $u \in G_m$; sinon, $u = vx$ avec $v \in G_m$ et $x \in \Sigma$; m est facteur de u mais pas de v , donc m est suffixe de u , ce qui prouve $u \in W_m$. Dans tous les cas, $m \in G_m \cup W_m$.

Question 23 • Preuve de $G_m \cdot \{m\} \subset W_m \cdot D_m$.

Soit $u \in G_m \cdot \{m\}$; notons x l'élément de G_m tel que $u = xm$. Parmi les décompositions de u de la forme vmw , observons celle pour laquelle $|v|$ est minimale. $|vm| > |x|$, sinon m serait facteur de x , alors que $x \in G_m$. m est suffixe de vm , mais aucun autre facteur de vm n'est égal à m , de par l'hypothèse de minimalité faite sur $|v|$; donc $vm \in W_m$. w est suffixe propre de m car $|w| = |u| - |vm| = |x| + |m| - |v| - |m| = |x| - |v| < |m|$. Notons alors y le mot tel que $m = yw$: nous aurons $u = xm = xyw$ mais aussi $u = vmw$ donc $vm = xy$: y est à la fois préfixe et suffixe de m ; notant $j = |w|$, nous aurons $c_j = 1$, donc $w = d_j \in D_m$ et finalement $u \in W_m \cdot D_m$.

• Preuve de $W_m \cdot D_m \subset G_m \cdot \{m\}$.

Soit $u \in W_m \cdot D_m$: il existe $i \in \llbracket 0, k-1 \rrbracket$ et $v \in \Sigma^*$ tels que $u = vmd_j$ et $c_j = 1$. Si $j = 0$, alors $d_j = \varepsilon$, donc $u = vm$; $vm \in G_m$, donc m ne peut être facteur de v : $v \in G_m$. Finalement, $u \in G_m \cdot \{m\}$. Examinons maintenant le cas $j \geq 1$: d_j est le mot $m[k-j..k-1]$, et l'on a $m[0..k-j-1] = m[j..k-1]$ puisque $c_j = 1$. Alors $u = vmd_j = vm[0..j-1]m[j..k-1]d_j = vm[0..j-1]m[0..k-j-1]m[k-j..k-1] = vm[0..j-1]m$ donc m est suffixe de u . D'autre part, $j \geq 1$ implique $d_j \neq \varepsilon$, donc $vm[0..j-1]$ est préfixe propre de vm ; comme ce dernier mot appartient à G_m , m ne peut être facteur de $vm[0..j-1]$, donc $vm[0..j-1] \in G_m$; ainsi $u \in G_m \cdot \{m\}$ est facteur de vm dans ce cas également.

Question 24 • G_m et W_m sont disjoints, donc $f_{G_m \cup W_m}(z) = g_m(z) + w_m(z)$. La décomposition $u = vx$ d'un élément de $G_m \cdot \Sigma$, avec $v \in G_m$ et $x \in \Sigma$, est clairement unique; de plus, $\{\varepsilon\} \cap (G_m \cup W_m) = \emptyset$ donc $f_{\{\varepsilon\} \cap (G_m \cup W_m)}(z) = f_{\{\varepsilon\}}(z) + f_{G_m}(z) \cdot f_{\Sigma}(z)$; mais $f_{G_m}(z) = g_m(z)$, $f_{\{\varepsilon\}}(z) = 1$ et $f_{\Sigma}(z) = 2z$, donc $f_{\{\varepsilon\} \cap (G_m \cup W_m)}(z) = 1 + 2zg_m(z)$. L'égalité établie à la question 22 implique $g_m(z) + w_m(z) = 1 + 2zg_m(z)$.

• La décomposition $u = vm$ d'un élément de $G_m \cdot \{m\}$, avec $v \in G_m$ est clairement unique; donc $f_{G_m \cdot \{m\}}(z) = f_{G_m}(z) \cdot f_{\{m\}}(z) = z^k g_m(z)$ puisque $\{m\}$ contient un seul mot, de longueur k .

• De même, la décomposition $u = vmw$ d'un élément de $W_m \cdot D_m$ est unique: si l'on avait $u = vmw = v'mw'$ avec (pour fixer les idées) $|v| < |v'|$, alors vm serait préfixe propre de $v'm$; m apparaîtrait donc dans $v'm$, ailleurs que comme suffixe, contredisant l'appartenance de $v'm$ à G_m . Donc $f_{W_m \cdot D_m}(z) = f_{W_m}(z) \cdot f_{D_m}(z) = w_m(z)P_m(z)$. L'égalité établie à la question 23 implique $z^k g(z) = w_m(z)P_m(z)$.

Question 25 • La première relation donne $w_m(z) = 1 + (2z - 1)g_m(z)$; en reportant dans la deuxième, il vient $z^k g(z) = (1 + (1 - 2z)g_m(z))P_m(z)$, soit $(z^k + (1 - 2z)P_m(z))g_m(z) = P_m(z)$. Ainsi $g_m(z) = \frac{P_m(z)}{z^k + (1 - 2z)P_m(z)}$.

• Appliquons ceci au mot $m = \mathbf{0}^k$: G_m sera l'ensemble des mots n'ayant pas $\mathbf{0}^k$ pour facteur, c'est-à-dire le langage L_k de la question 8. Pour tout $i \in \llbracket 0, k-1 \rrbracket$, nous avons $c_i = 1$ puisque les facteurs gauche et droit de longueur $k - i$ de ce mot sont égaux (à $\mathbf{0}^{k-i}$). Ainsi $P_m = \sum_{0 \leq i < k} X^i$, puis $P_m(z) = \frac{1 - z^k}{1 - z}$; nous

obtenons alors $g_m(z) = \frac{1 - z^k}{(1 - z)z^k + (1 - 2z)(1 - z^k)} = \frac{1 - z^k}{1 - 2z + z^{k+1}}$. Nous retrouvons ainsi le résultat de la question 8.

Références bibliographiques

► Les idées des trois dernières parties de ce texte proviennent du livre *An introduction to the analysis of algorithms*, de Philippe FLAJOLET et Robert SEDGEWICK.

FIN