*Journal de Théorie des Nombres*
*de Bordeaux* **11** (1999), 111–132

# Opérations sur les mots de Christoffel

par Éric LAURIER

RÉSUMÉ. On peut définir la pente d'un mot écrit avec des 0 et des 1 comme le nombre de 1 divisé par le nombre de 0, et généraliser cette définition aux mots de longueur infinie. Considérant le lien entre les mots de Christoffel et les fractions continues, on se propose d'étudier le comportement de tels mots lorsqu'on additionne leurs pentes, ou qu'on les multiplie par un entier positif.

Après un bref exposé des différentes notions liées aux mots de Christoffel, l'étude de la somme et de la multiplication sont présentées sous forme d'algorithmes permettant de connaître au mieux le mécanisme de ces opérations.

ABSTRACT. The slope of a finite sequence of 0 and 1 can be defined as the number of 1 divided by the number of 0 and it is possible to generalize this definition to infinite sequences. Considering the link between Christoffel words (or characteristic sequences) and continued fractions, we study the behaviour of such words when adding their slopes, or multiplying them by a positive integer.

After an outline of the different notions around Christoffel words, the sum and product are introduced as algorithms permitting to understand the mechanism of these operations as well as possible.

On se propose de construire des algorithmes donnant le mot de Christoffel primitif dont la pente est la somme de celles de deux autres mots de Christoffel donnés, ou bien le produit de celle d'un mot par un entier. Les algorithmes présentés ici concernent surtout l'aspect théorique des mots de Christoffel, sans aucune recherche de performance. Concernant l'addition, on construit d'abord, par une procédure d'addition naïve des mots de Christoffel, un premier mot de Lyndon dont la pente est effectivement la somme des pentes données, puis une suite strictement croissante de mots de Lyndon dont le dernier terme (ou la limite) est le mot de Christoffel recherché. La multiplication par un entier consiste à construire pas à pas le résultat en faisant intervenir des intervalles non standard et des matrices de transformations planes.

Ces algorithmes sont fondés sur certaines propriétés et observations qui sont résumées ci-après et développées dans cet article sans les preuves : nous renvoyons le lecteur à [10] pour l'exposé complet de ces notions.

Les mots de Lyndon peuvent être construits sur des alphabets de plus de deux lettres, ce sont les mots qui pour l'ordre lexicographique sont supérieurs à leurs suffixes. Pour une pente donnée, il existe un unique mot de Lyndon maximal pour l'ordre lexicographique, c'est le mot de Christoffel de ladite pente. Depuis Bernoulli (1772) et Christoffel (1875), les mots de Christoffel ont été étudiés récemment (voir [1], [2], [3], [5], [8]), ceux de pente quadratique ayant fait l'objet d'une attention particulière. On peut facilement passer d'un mot de Christoffel à la fraction continue de sa pente : l'idée est donc d'utiliser les mots de Christoffel pour permettre un nouvel éclairage de l'addition des fractions continues.

Les mots de Christoffel qu'on définit ci-dessous par récurrence sont des éléments de $\{0,1\}^*$, où $\{0,1\}^*$ désigne l'ensemble des mots sur l'alphabet $\{0,1\}$. On trouvera une description complète de ces mots, introduits différement, dans [1], [2], [8] et d'autres résultats dans [3]. Si $f$ est un mot de $\{0,1\}^*$, on note $f_0$ le nombre de 0 de $f$ et $f_1$ le nombre de 1 ; $\rho(f) = f_1/f_0$ est la pente de $f$ ; On peut représenter un mot sur le réseau des points à coordonnées entières du plan, en partant de l'origine : 0 correspond à un pas horizontal vers la droite, 1 un pas vers le haut, et ainsi la pente du mot prend tout son sens. On entend par déterminant d'un couple de mots $(f,g)$ l'entier $\det(f,g) = f_0g_1 - f_1g_0$. On dispose des propriétés habituelles du déterminant, en remplaçant l'addition par la concaténation. Enfin $fg$ représente la concaténation de $f$ et $g$ ; $f^n = ff...f$, $n$ fois ; si $f = uv$, $u$ est un préfixe de $f$ et $v$ en est un suffixe.

Les mots de Christoffel sont définis comme suit : les mots 0 et 1 sont des mots de Christoffel, puis si $f$ et $g$ sont deux mots de Christoffel tels que $\det(f,g) = 1$ alors $fg$ est un mot de Christoffel et tous sont obtenus de cette manière. Réciproquement, il existe une unique façon d'écrire un mot de Christoffel $f$ différent de 0 et 1 sous la forme $f = f_\gamma f_\delta$ où $(f_\gamma, f_\delta)$ est un couple de mots de Christoffel de déterminant 1 : cette écriture s'appelle la factorisation standard. La notion de factorisation standard existe aussi pour les mots de Lyndon, en prenant $f_\gamma$ de longueur minimale ; si de plus cette factorisation minimise le déterminant, on parlera de factorisation de Christoffel.

L'ordre de $\mathbb{R}$ induit via les pentes un ordre sur l'ensemble des mots de Christoffel, ordre qui coïncide avec l'ordre lexicographique : si on considère deux mots de Christoffel $f < g$, $(f,g)$ détermine un intervalle de $\mathbb{R}$, et lorsque $\det(f,g) = 1$ on parlera d'intervalle standard. Lorsque $(f,g)$ est standard, $[\rho(f), \rho(g)]$ est un intervalle de Farey. Si $h$ est un mot de Christoffel appartenant à l'intervalle standard $(f,g)$ alors $h$ s'écrit de manière unique avec $f$ et $g$ où $f$ et $g$ peuvent être considérés comme des lettres. Réciproquement si $k$ est un mot de Christoffel et si dans $k$ on remplace 0 par $f$ et 1 par $g$ on obtient un nouveau mot de Christoffel appartenant à $(f, g)$. De manière générale on peut définir la notion de substitution standard de l'intervalle standard $(f, g)$ vers l'intervalle standard $(h, k)$ : l'image d'un mot est obtenue en substituant $h$ à $f$ et $k$ à $g$ ; il est clair qu'on obtient un mot de Christoffel. Si $k$ est l'image de $h$ appartenant à l'intervalle standard $(f, g)$ par la substitution standard envoyant $(f, g)$ sur $(u, v)$ on dira que $\rho(k)$ est l'image de la pente de $h$ et que la fraction continue de $\rho(k)$ est l'image de celle de $\rho(h)$ par $(f \mapsto u, g \mapsto v)$.

Ces différentes notions sont reprises dans [10] en construisant les mots de Christoffel de manière indépendante géométriquement puis en utilisant la récurrence.

## 1. Mots réductibles

On considère (figure 1) le chemin du mot 011 et on divise le pas de la grille par 4. Ensuite on dessine le chemin joignant les extrémités de 011 en passant au plus près de sa pente sans la rencontrer : on obtient alors le mot 010110110111. Le théorème suivant donne des conditions pour qu'un mot quelconque soit le résultat d'une telle opération.

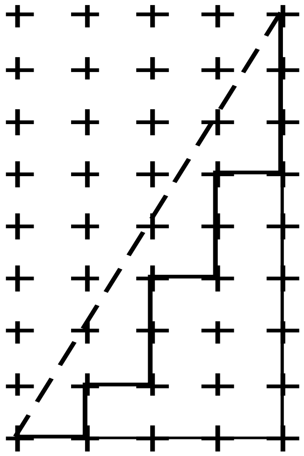


Figure 1 : division du pas de la grille par 4.

**Théorème 1.** *Soient $s$, $t$, $u$ et $v$ quatre mots de Christoffel primitifs non vides tels que $st = uv$. On pose $n = det(s, t)$. Alors :*

*(1) $det(u, v) = det(s, t) = n$.*

*(2) Il existe un mot de Christoffel primitif non vide $m$ tel que :*

$$uv = st = m_\gamma m^{n-1} m_\delta.$$

**Notation et terminologie.** Si $f = uv = st$ on dit que $f$ est "réductible" et on pose $f_{:n} = m$.

*Preuve.* On pose $f = st = uv = uwt$ en supposant que $u$ est plus court que $s$ et qu'ainsi $v$ est plus long que $t$. D'après la méthode permettant de retrouver une fraction continue à partir de son mot de Christoffel, $uw$ appartient à l'intervalle standard $(u, u_\delta)$ et $wt$ à $(t_\gamma, t)$. Ainsi il existe deux mots de Christoffel primitifs $u'$ et $t'$, respectivement suffixe et préfixe de $w$, maximaux pour la longueur, tels que $uw$ soit dans $(u, u')$ et $wt$ dans $(t', t)$.

**Démonstration de (1).** Le mot $w$ ne peut finir par $uu'$ car $(u, uu')$ est standard et contiendrait $uw$, et cela contredirait le caractère maximal de $u'$. Ainsi $w$ finit par $u'u'$ donc commence par $u'$ car $uw$ est de Christoffel. Pour les mêmes raisons, $w$ finit par $t'$.

Donc, $t'$, préfixe maximal de $w$, commence par $u'$ et $u'$ finit par $t'$, d'où $u' = t'$, et on pose alors $m = u' = t'$. Ainsi, $uw$ appartient à l'intervalle standard $(u, m)$ et $wt$ à $(m, t)$, ce qui signifie que $w$ est de la forme $m^i$ et alors :

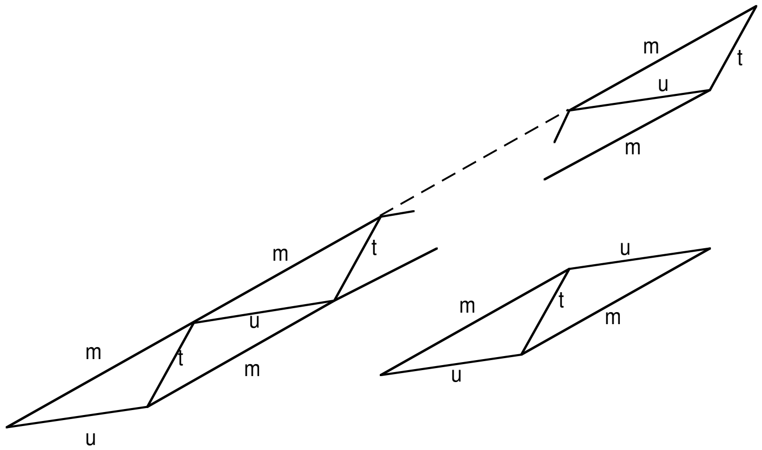
$$\begin{aligned} \det(u, v) &= \det(u, m^i t) &= i + \det(u, t) \\ \det(s, t) &= \det(um^i, t) &= \det(u, t) + i \end{aligned}$$

Finalement, $\det(u, v) = \det(s, t) = n$.

**Démonstration de (2).** Quitte à changer les notations, on peut maintenant supposer que $m$ n'est ni un suffixe de $u$ ni un préfixe de $t$. Montrons alors que $u = m_\gamma$ et $v = m_\delta$.

Tout d'abord, on constate que la pente de $m$ est la même que celle de $f$ :

$$\det(f, m) = \det(uwt, m) = \det(u, m) + \det(t, m) = 1 - 1 = 0.$$




Démonstration de (2).

Nous sommes alors dans la situation de la figure. Il est donc clair que l'aire du parallélogramme induit par $u$ et $t$ est la même que celle du parallélogramme correspondant à $u$ et $m$, et de ce fait, $(u, t)$ est un intervalle standard. On constate d'autre part que $m = ut$ et l'unicité de la factorisation standard permet d'obtenir $u = m_\gamma$ et $t = m_\delta$. Ainsi, $f$ est de la forme $m_\gamma m^\nu m_\delta$, et :

$$n = \det(u, v) = det(m_\gamma, m^\nu m_\delta) = \nu + 1.$$

d'où $\nu = n - 1$ ce qui termine la démonstration.

**Corollaire 1.** *Soit $u$ un mot de Lyndon dont la factorisation de Christoffel est $u = fg$ où $f$ et $g$ sont des mots de Christoffel primitifs tels que* $\det(f, g) = n > 1$. *Alors $u$ est un mot réductible.*

*Preuve.* Le mot $u$ ne peut être un mot de Christoffel car $\det(f, g) = n > 1$. On ne peut avoir simultanément $f = 0$ et $g = 1$, supposons donc que $f$ soit différent de 0 alors, comme $f$ est le plus petit mot de Lyndon minimisant le déterminant, $\det(f, g) < \det(f_\gamma, f_\delta g) = 1 + \det(f_\gamma, g)$ ; or $\det(f, g) = \det(f_\gamma, g) + \det(f_\delta, g)$ donc $\det(f_\delta, g) < 1$ d'où $g \in (f, f_\delta)$. Finalement, $g \neq 1$ et par un raisonnement analogue, $\det(f, g_\gamma) \leq 1$ : si $\det(f, g_\gamma) < 1$ alors $f \in (g_\gamma, g)$ donc $f = g$ ce qui est absurde ; donc $\det(f, g_\gamma) = 1$ et ainsi $(f, g_\gamma)$ est standard donc $h = fg_\gamma$ est un mot de Christoffel et ainsi $u = fg = hg_\delta$ d'où $u$ est réductible par le précédent théorème.

**Mots réductibles généralisés.** On souhaite trouver le mot de Christoffel primitif $m$ de même pente que le mot $f = a^i b^j c^k$ où $(a, c)$ est un intervalle standard et $b = ac$. La pente de $m$ est liée à la fraction continue de $\frac{j+k}{i+j}$ : on peut utiliser l'algorithme d'Euclide.

Mais si $i$ et $k$ sont strictement supérieurs à 1, on reconnait dans $f$ le mot réductible $ab^j c$ que l'on peut remplacer par $b^{j+1}$, et on recommence l'opération autant de fois qu'il le faut jusqu'à obtenir $b^{i+j}c^{k-i}$ si $k \geq i$ et $a^{i-k}b^{j+k}$ sinon. Si $k = i$ alors $m = b$, sinon dans le cas où $k > i$ on pose $a' = b$, $c' = c$, $b' = bc$, $i' = i + j - 1$, $j' = 1$, $k' = k - i - 1$ et dans le cas contraire, $a' = a$, $c' = b$, $b' = ab$, $i' = i - k - 1$, $j' = 1$, $k' = j + k - 1$ puis on recommence avec le nouveau mot $a'^{i'} b'^{j'} c'^{k'}$. Le mot $f$ est de Lyndon, à chaque étape on obtient un mot de Lyndon strictement supérieur à celui de l'étape précédente, Chaque mot de Lyndon est majoré par $m$ qui est le mot de Lyndon maximal de la bonne pente. On a construit une suite strictement croissante et majorée de mots de Lyndon, et on obtient alors le mot $m$ recherché au bout d'un nombre fini d'étapes.

Considérons l'exemple de $f = 0001111 = 0^2(01)^1 1^3$ : 0011 est réductible, on le remplace par 0101,on obtient 0010111 où $0(01)^2 1$, réductible, est remplacé par 010101 et alors 0101011 est le mot de Christoffel primitif de même pente que $f$. Cet algorithme est plus rapide que l'algorithme d'Euclide, car pour ce dernier tout se passe comme si on partait systématiquement de $a^{i+j}c^{j+k}$.

Nous appellerons les mots de la forme $a^i b^j c^k$ "mots réductibles généralisés".

## 2. Formules de récurrence pour les mots de Lyndon

Soit $f$ un mot de Lyndon de pente $r$ rationnelle. On propose ici un algorithme permettant, à partir de $f$, de construire le mot de Christoffel primitif $\varphi$ de pente $r$. Tout d'abord, soit $(a,c)$ un intervalle standard, on pose $b = ac$. Soit $\mathcal{L}(a,c)$ l'ensemble des mots de Lyndon s'écrivant à l'aide de $a$ et $c$, c'est-à-dire l'image de l'ensemble des mots de Lyndon sur $\{0,1\}$ par la substitution $0 \mapsto a$, $1 \mapsto c$, et où l'on remplace l'occurrence $ac$ par $b$. Enfin si $f$ est un mot de Lyndon de $\{0,1\}^*$ on désignera par $f = f_\gamma f_\delta$ la factorisation de Christoffel. On considère donc l'application $\Phi$ de $\mathcal{L}(a,c)$ dans $\mathcal{L}(a,c)$ telle que :

- L'image par $\Phi$ d'un mot de Christoffel est le mot de Christoffel primitif de même pente.
- L'image par $\Phi$ du mot réductible généralisé $a^i b^j c^k$ est le mot de Christoffel obtenu en remplaçant 0 par $a$ et 1 par $c$ dans le mot de Christoffel primitif de pente $\frac{j+k}{i+j}$.
- Puis par récurrence, l'image par $\Phi$ du mot de Lyndon $f$ en fonction de $f_\gamma$ et $f_\delta$ est :

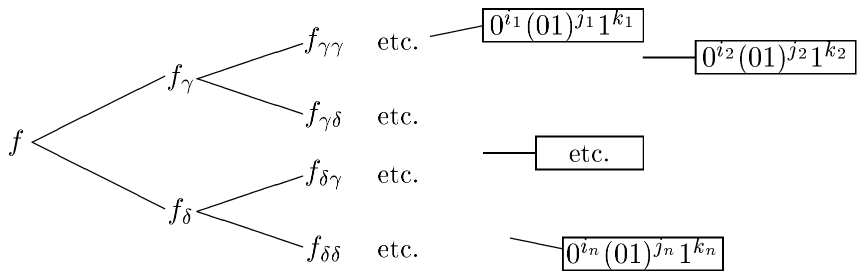
$$\begin{array}{lll}
\text{Si } \rho(f_\gamma) < \rho(f_\delta) & \Phi(f) = \Phi\left[(\Phi(f_\gamma))^{\mathrm{pgcd}((f_\gamma)_0,(f_\gamma)_1)} \quad (\Phi(f_\delta))^{\mathrm{pgcd}((f_\delta)_0,(f_\delta)_1)}\right] \\
\text{Si } \rho(f_\gamma) > \rho(f_\delta) & \Phi(f) = \Phi\left[(\Phi(f_\delta))^{\mathrm{pgcd}((f_\delta)_0,(f_\delta)_1)} \quad (\Phi(f_\gamma))^{\mathrm{pgcd}((f_\gamma)_0,(f_\gamma)_1)}\right] \\
\text{Si } \rho(f_\gamma) = \rho(f_\delta) & \Phi(f) = \Phi(f_\gamma)
\end{array}$$

**Théorème 2.** *Soit $f$ un mot de Lyndon. Alors $\Phi(f)$ est le mot de Christoffel primitif de même pente que $f$.*

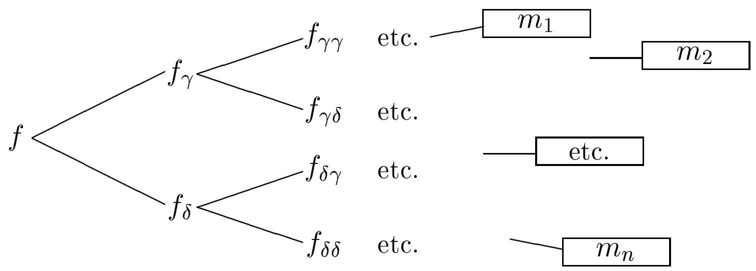
*Preuve.* En premier lieu puisque $\Phi$ n'agit sur les mots que par permutation de paquets de 1 et de 0, il est aisé de voir que $\Phi$ conserve les pentes. Avant de poursuivre la démonstration, faisons une remarque sur l'utilisation des arbres pour représenter les mots de Christoffel ou de Lyndon. On écrit le mot de Lyndon $f$ de la manière suivante :

$$f = 0^{i_1}(01)^{j_1}1^{k_1}0^{i_2}(01)^{j_2}1^{k_2}...0^{i_n}(01)^{j_n}1^{k_n}$$

avec éventuellement des $i_p$, $j_p$ ou $k_p$ nuls. On factorise $f$ puis $f_\gamma$, $f_\delta$, $f_{\gamma\gamma}$, etc, autant de fois que possible et il est clair qu'à chaque factorisation on ne coupe de paquet $0^{i_p}(01)^{j_p}1^{k_p}$ que lorsqu'il constitue le mot à factoriser. En effet, ce sont les extrémités du chemin géométrique de tels paquets qui minimisent la distance du chemin du mot à factoriser à sa pente. On obtient l'arbre suivant :




Ainsi chaque extrémité de l'arbre est soit un mot de Christoffel, soit un mot réductible généralisé, donc on obtient en factorisant le moins loin possible :




où $m_1$, $m_2$ et $m_n$ sont des mots de Christoffel primitifs ou réductibles généralisés. On appellera cet arbre $\mathcal{A}(f)$.

Il est clair qu'appliquer $\Phi$ à $f$ induit dans un premier temps la construction de $\mathcal{A}(f)$. D'autre part, soit $u$ un mot de $\{\gamma, \delta\}^*$ tel que $f_u$ soit un nœud de $\mathcal{A}(f)$ : si $\rho(f_{u\gamma}) > \rho(f_{u\delta})$, alors les deux sous-arbres correspondants à $f_{u\gamma}$ et $f_{u\delta}$ sont échangés, car c'est le deuxième point de la récurrence dans la définition de $\Phi$ qui intervient. Cela a pour conséquence de réordonner $\mathcal{A}(f)$. Supposons donc que $\mathcal{A}(f)$ soit ordonné.

On prouve le théorème par récurrence sur la longueur de $f$. Si $f$ est le mot 0, 1 ou même 01, il n'y a rien à prouver. On suppose donc que si $f$ est un mot de Lyndon de longueur au moins égale à 3, alors $g$ est un mot de Lyndon de longueur strictement inférieure à celle de $f$ implique que $\Phi(g)$ est le mot de Christoffel de même pente que $g$. Donc en particulier $\Phi(f_\gamma)$ et $\Phi(f_\delta)$ sont des mots de Christoffel de même pente que respectivement $f_\gamma$ et $f_\delta$, puis par suite $\Psi_0 = \Phi(f_\gamma)\Phi(f_\delta)$ est un mot de Lyndon de même pente que $f$ tel que $\Psi_0 > f$.

Si la factorisation de Christoffel de $\Psi_0$ donne deux mots de Christoffel, alors on applique le corollaire 1, donc $\Phi(\Psi_0)$ est le mot de Christoffel de même pente que $f$. Sinon l'un des deux n'étant pas de Christoffel, il sera strictement inférieur à son image par $\Phi$, donc $\Phi(\Psi_0) > \Psi_0$. On recommence le raisonnement avec $\Psi_1 = \Phi((\Psi_0)_\gamma)\Phi((\Psi_0)_\delta)$. On obtient ainsi de proche en proche une suite strictement croissante de mots de Lyndon $f < \Psi_0 < \Psi_1 < \Psi_2 < ...$ où $\Psi_k = \Phi((\Psi_{k-1})_\gamma)\Phi((\Psi_{k-1})_\delta)$. Cette suite est majorée par le mot de Christoffel de même pente que $f$ : donc il existe un entier $k$ tel que $\Psi_k$ est ce mot de Christoffel, et ainsi $\Psi_k = \Phi(f)$. La preuve est alors complète.

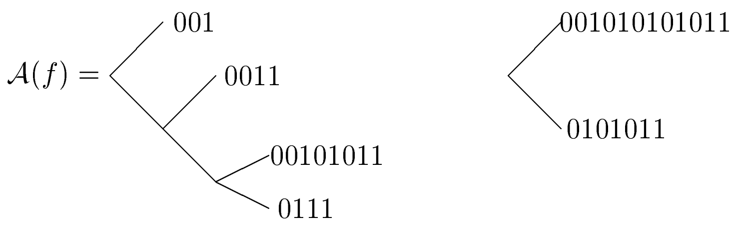
**Algorithme non récursif.** La démonstration précédente permet d'expliciter un algorithme itératif calculant $\Phi(f)$ : il suffit de construire $\mathcal{A}(f)$, de permuter les sous-arbres là où c'est nécessaire, puis de proche en proche de remplacer les mots réductibles généralisés par leur mot de Christoffel. Considérons pour cela l'exemple suivant.

$$\Phi(0010011001010110111) = \Phi(001\Phi(\Phi(0011)\Phi(\Phi(00101011)0111)))$$

Ce qui donne le premier arbre de factorisation ci-après. Puis on substitue les mots de Christoffel aux mots réductibles :

$$\begin{aligned}\Phi(0010011001010110111) &= \Phi(001\Phi(0101\Phi(010101010111))) \\ &= \Phi(001\Phi(0101010101101011)) \\ &= \Phi(0010101010110101011) \\ &= \Phi(\Phi(001010101011)0101011)\end{aligned}$$

On obtient le second arbre suivant.




Voici maintenant le dessin correspondant à cet exemple. Le remplacement des différents mots réductibles généralisés se traduit par une rectification du chemin correspondant au mot de Lyndon de départ : le mot se “déplace" ainsi vers sa pente d'une ou plusieurs cases, marquées de différentes couleurs suivant les étapes. La couleur numéro 1 correspond au remplacement de 0011 par 0101 puis on a substitué 01010101 à 00101011 (couleur numéro 2) ; ensuite 0101010101101011 à 0101010101010111 (couleur numéro 3) ; enfin les couleurs 4 et 5 correspondent aux deux dernières substitutions effectuées.

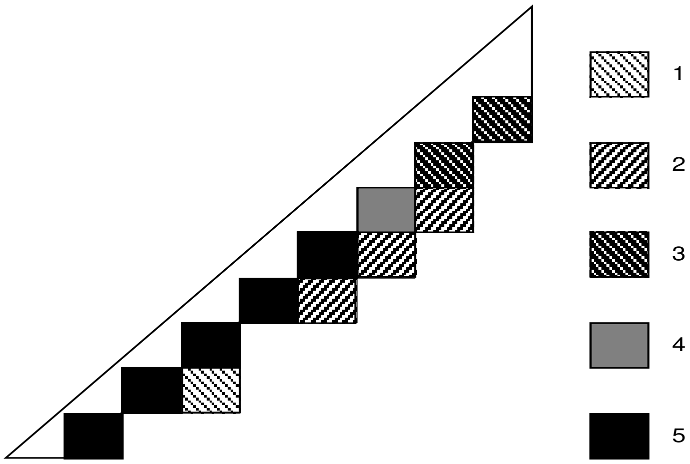



Figure 2 : calcul du mot de Christoffel

Le résultat est le mot 0101010101010101011.

## 3. Addition des mots de Christoffel

Le but qu'on se fixe est de comprendre comment se traduit l'addition des nombres en termes de mots de Christoffel. On se fonde sur une interprétation naturelle de cette addition pour construire l'algorithme.

3.1. **Etude préliminaire.** L'idée de base visualisée sur la figure 3 est que, si les deux pentes correspondant aux deux nombres à additionner sont données par l'hypothénuse de deux triangles rectangles de même base $d$, alors la somme de ces pentes est donnée par le triangle rectangle de base $d$ dont la hauteur est la somme des hauteurs des triangles précédents. Ainsi :

$$p_1 = \frac{h_1}{d},\ p_2 = \frac{h_2}{d} \text{ donc évidemment } p_1 + p_2 = \frac{h_1 + h_2}{d}.$$

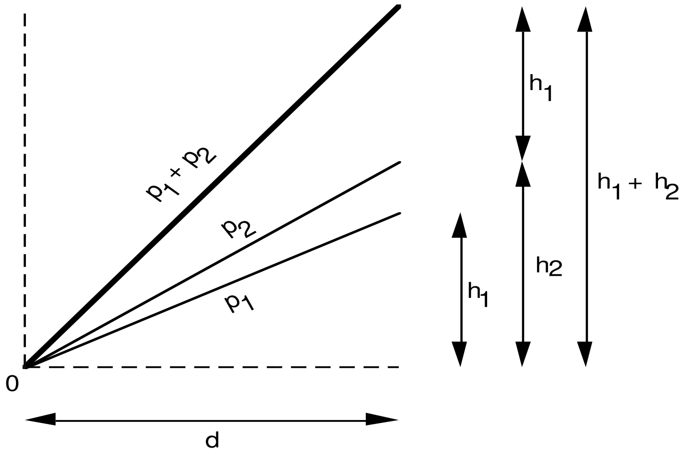



Figure 3 : addition des pentes.

Il est donc permis de penser qu'on peut, à partir de deux mots de Christoffel, construire facilement un mot dont la pente est la somme de leur pente, et ayant de bonnes propriétés.

On veut donc additionner deux mots de Christoffel : choisissons-les finis, en considérant des pentes rationnelles positives. Quitte à réduire les nombres concernés au même dénominateur, on peut supposer qu'il est identique pour les deux. On considère l'application :

$$\begin{array}{rcl} \oplus : \mathbf{L}_0^+ \times \mathbf{L}_0^+ & \longrightarrow & \{0,1\}^* \\ (f,g) & \longmapsto & f \oplus g \end{array}$$

où $f \oplus g$ est construit par récurrence comme suit :

$$\begin{array}{rcl} 01^i \oplus 01^j & = & 01^{i+j} \\ 01^i f' \oplus 01^j g' & = & 01^{i+j}(f' \oplus g') \end{array}$$

dès lors que $f'$ et $g'$ sont des suffixes de $f$ et $g$ commençant par 0.

On construit alors les mots de Christoffel $\varphi_1$ et $\varphi_2$ correspondant aux deux pentes ; $\varphi_1$ et $\varphi_2$ sont finis mais non nécessairement primitifs. Ils ont bien entendu le même nombre de 0. On pose $\sigma = \varphi_1 \oplus \varphi_2$ et on désigne par $\varphi$ le mot de Christoffel de même pente et de même longueur que $\sigma$. Le but que l'on se fixe est de construire à partir de $\sigma$ un mot plus proche de $\varphi$. Le mot $\sigma$ est bien celui recherché : pour chaque 0 de $\varphi_1$ et $\varphi_2$ on additionne les 1 qui suivent (figure 4) et ainsi on retrouve la bonne pente, car les aires hachurées s'additionnent colonne par colonne. On remarque qu'alors $\sigma$ est proche de $\varphi$.

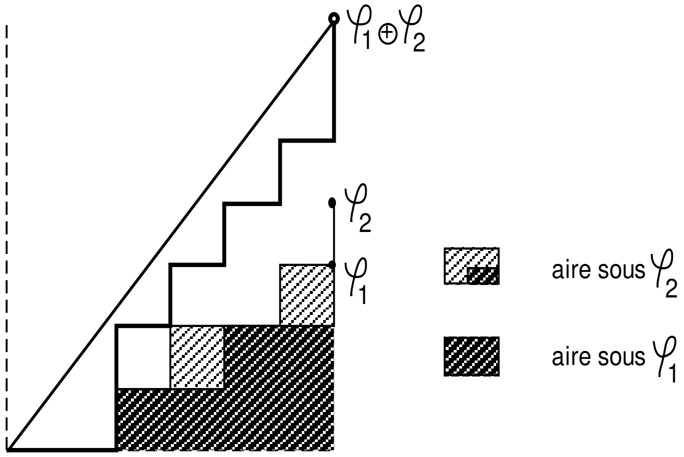



Figure 4 : addition. $001001001 \oplus 0010100101 = 0011010101011$.

Le but est donc d'étudier les propriétés de $\sigma$ afin de construire un algorithme corrigeant $\sigma$ en respectant ces propriétés, et ce de la façon la plus naturelle possible. Montrons d'abord que, géométriquement, pour chaque colonne d'une unité de la grille, il y a au plus une case de différence en hauteur entre le chemin correspondant à $\sigma$ et celui lié à $\varphi$.

**Lemme 1.** *Soient $\sigma'$, $\varphi'$ des préfixes de $\sigma$, $\varphi$ tels que les suffixes correspondants commencent par 0, et tels que $\sigma'_0 = \varphi'_0$. Alors $0 \leq \rho(\varphi') - \rho(\sigma') < 2/D$, $D$ étant le nombre de 0 de $\sigma'$ et $\varphi'$.*

*Preuve.* Soient $\varphi'_1$ et $\varphi'_2$ les préfixes de $\varphi_1$ et $\varphi_2$ ayant le même nombre de 0 que $\sigma'$ ou $\varphi'$, dont les suffixes correspondants commencent aussi par 0 : alors il est clair que $\sigma' = \varphi'_1 \oplus \varphi'_2$. Comme $\varphi_1$ et $\varphi_2$ sont des mots de Christoffel, les pentes de $\varphi'_1$ et $\varphi'_2$ sont respectivement inférieures à celles de $\varphi_1$ et $\varphi_2$ : ainsi, par définition de $\oplus$, la pente de $\sigma'$ est inférieure à celle de $\varphi'$ ce qui prouve la première
inégalité.

S'agissant de la seconde inégalité, si on utilise le fait que, géométriquement, entre une pente donnée et le chemin représentant son mot de Christoffel primitif, ne peut tenir une case entière de la grille :

$$1/D + \rho(\varphi'_1) > \rho(\varphi_1)$$
$$1/D + \rho(\varphi'_2) > \rho(\varphi_2)$$

donc, en additionnant :

$$2/D + \rho(\varphi'_1) + \rho(\varphi'_2) > \rho(\varphi_1) + \rho(\varphi_2)$$

finalement :

$$\rho(\varphi') - \rho(\sigma') < 2/D.$$

La seconde inégalité est alors prouvée.

3.2. **Correction des erreurs.** Le mot $\sigma$ peut être interprété comme étant le mot $\varphi$ entaché d'erreurs et nous allons utiliser les algorithmes exposés dans les paragraphes précédents pour les corriger.

**Lemme 2.** *Soient $f$ et $g$ deux mots de Lyndon, alors $f \oplus g$ est un mot de Lyndon.*

*Preuve.* On remarquera d'abord que, si $u$ est l'itéré d'un mot de Lyndon $v$ et si $u'$ est un suffixe de $u$ alors soit $u'$ est itéré de $v$ et $u' \leq u$, soit ce n'est pas le cas et $u < u'$.

On pose $s = f \oplus g$, $s = s_1 s_2$ et on suppose que $f \oplus g = f^a \oplus g^b$ où $\mathrm{pgcd}(a,b) = 1$. Si $s_2$ commence par 1 alors $s_2 > s$ car $s$ commence par 0. On peut donc supposer que $s_2$ commence par 0. En conséquence, $s_1 = f_1 \oplus g_1$ et $s_2 = f_2 \oplus g_2$, où $f^a = f_1 f_2$ et $g^b = g_1 g_2$, $f_2$ et $g_2$ commencent par 0, $(f_1)_0 = (g_1)_0$.

**Premier cas.** Soit $f_2$, soit $g_2$ est un itéré respectivement de $f$ ou $g$. Comme $\oplus$ est commutative, supposons que $f_2 = f^{a'}$. Ainsi puisque $a$ et $b$ sont premiers entre eux, $g_2$ n'est pas un itéré de $g$ et on peut alors poser :

$$\begin{array}{rcl} g & = & k0(1)^j 0 g_3 \\ g_2 & = & k0(1)^{j+1} g_4 \end{array}$$

où $k$ est éventuellement vide (on sait par ailleurs que $g_2$ commence par 0). Soit enfin $F$ le préfixe de $f^{a'}$ tel que $F_0 = k_0$. Ainsi :

$$\begin{array}{rcl} f \oplus g & = & (F \oplus k)0(1)^{i+j} 0m \\ f_2 \oplus g_2 & = & (F \oplus k)0(1)^{i+1+j} m' \end{array}$$

Il apparaît alors que $f \oplus g < f_2 \oplus g_2$, soit $s < s_2$.

**Second cas.** Ni $f_2$, ni $g_2$ ne sont des itérés respectivement de $f$ et $g$. On suppose que le préfixe maximal pour le nombre de 0 commun à $f$ et $f_2$ contient moins de 0 que celui commun à $g$ et $g_2$. De manière analogue au premier cas, on peut poser :

$$\begin{array}{rclcrcl} f & = & h0(1)^i 0 f_3 & \text{et} & g & = & k0(1)^j 0 g_3 \\ f_2 & = & h0(1)^{i+1} f_4 & \text{et} & g_2 & = & k0(1)^{j+r} g_4 \end{array}$$

où $h$ et $k$ sont éventuellement vides ;

$$\begin{array}{rcl} f \oplus g & = & (h \oplus k)0(1)^{i+j} 0m \\ f_2 \oplus g_2 & = & (h \oplus k)0(1)^{i+1+j+r} m' \end{array}$$

Il apparaît encore que $f \oplus g < f_2 \oplus g_2$, soit $s < s_2$. Dans tous les cas, $f \oplus g$ est donc un mot de Lyndon.

Ainsi $\sigma$ est un mot de Lyndon, et on utilise les algorithmes précédents pour le corriger.

3.3. **Lien entre la multiplication par 2 et l'algorithme d'addition.** On note $2f$ le mot de Christoffel dont la pente est le double de celle de $f$. Lorsqu'on calcule $fg \oplus fg$, la factorisation standard en $f$ et $g$ conserve un sens de façon évidente : en effet, $fg \oplus fg = (f \oplus f)(g \oplus g)$. On corrige $f \oplus f$ et $g \oplus g$, ce qui donne $2f$ et $2g$ : si $(2f, 2g)$ est standard alors $2(fg) \in (2f, 2g)$ donc $2f$ et $2g$ apparaissent dans l'algorithme de correction des erreurs : cela signifie que $f \oplus f$ et $g \oplus g$ ont été corrigés sans interférence entre les deux mots.

De même, dans le cas où $(2f, 2g)$ n'est pas standard, $((2f2g)_{:2})_\gamma$ et $((2f2g)_{:2})_\delta$ doivent apparaître dans l'algorithme, donc $2f$ et $2g$ aussi. La seule interférence entre $2f$ et $2g$ est alors le calcul de $(2f2g)_{:2}$. On cherche des formules de récurrence à l'aide de $\Phi$.

- si $f$ ou $g$ a un nombre pair de 0 alors $(2f, 2g)$ est standard :

$$\begin{aligned}\Phi(fg \oplus fg) &= \Phi((f \oplus f)(g \oplus g)) \\ &= \Phi(\Phi(f \oplus f)\Phi(g \oplus g)) \\ &= \Phi((2f)^2(2g)) \text{ ou } \Phi((2f)(2g)^2) \\ &= (2f)^2(2g) \text{ ou } (2f)(2g)^2\end{aligned}$$

- sinon $(2f, 2g)$ est réductible :

$$\begin{aligned}\Phi(fg \oplus fg) &= \Phi((f \oplus f)(g \oplus g)) \\ &= \Phi(\Phi(f \oplus f)\Phi(g \oplus g)) \\ &= \Phi((2f)(2g)) \\ &= ((2f)(2g))_{:2}\end{aligned}$$

Ainsi on retrouve les formules du lemme.

3.4. **Conclusion : cas des réels.** Les mots de Christoffel correspondant aux pentes irrationnelles sont infinis. Malgré tout, la formule de récurrence permettant de définir $f \oplus g$, où $f$ et $g$ sont deux mots de Christoffel de pente irrationnelle, reste valable mais il n'est évidement pas possible d'obtenir le mot corrigé en un temps fini. Il faut donc tronquer $f \oplus g$ de sorte que le préfixe restant soit un mot de Lyndon, et on obtiendra une valeur par défaut, puis, pour obtenir une valeur par excès, sachant que là où on coupe il peut y avoir une erreur, on ajoute $01^{\lfloor r_1 + r_2 + 2 \rfloor}$ où $r_1$ et $r_2$ désignent les pentes de $f$ et $g$.

Si $n/d$ est le rationnel obtenu par défaut, la différence entre les deux valeurs obtenues est de l'ordre de $1/d$ donc tend vers 0 lorsque la longueur du mot tronqué grandit.

## 4. Multiplication d'un mot de Christoffel par un entier

A partir d'un intervalle standard auquel appartient un mot de Christoffel, on cherche un autre intervalle standard le plus petit possible contenant le mot de Christoffel dont la pente est un multiple entier de celle du mot donné. Plus généralement, on établit un algorithme permettant de calculer ce multiple, en utilisant à la fois les mots de Christoffel et les fractions continues.

Il existe déjà des algorithmes permettant de tels calculs : voir notamment [4], [6], [9] et [14]. Nous proposons un nouvel algorithme qui peut être considéré comme un algorithme de multiplication tant des fractions continues que des mots de Christoffel.

4.1. **Etude de quelques cas particuliers.** Lorsqu'un mot de Christoffel $g$ a pour pente $n$ fois celle d'un autre mot de Christoffel $f$ on dit qu'on a multiplié $f$ par $n$ et on note $g = nf$. On connaît des formules simples permettant de calculer $2f$ et $3f$ par récurrence à partir de $f$. Nous avons vu dans le paragraphe précédent les formules de multiplication par 2 :

$$\left\{\begin{array}{llcl} \text{si } f_0 \text{ est pair,} & 2(fg) & = & (2f)(2f)(2g) \\ \text{si } g_0 \text{ est pair,} & 2(fg) & = & (2f)(2g)(2g) \\ \text{sinon} & 2(fg) & = & ((2f)(2g))_{:2} \end{array}\right.$$

où $(f, g)$ est un intervalle standard.

Dans le cas de la multiplication par 3 on obtient des formules similaires : pour plus de détails voir [9] ; multiplier par 4 revient à multiplier deux fois par 2 ; pour la multiplication par un nombre premier $p$ supérieur ou égal à 5, on ne dispose pas de formule de récurrence générale car on ne parvient pas à trouver d'intervalle standard dépendant explicitement de $pf$ et $pg$ : considérer par exemple $5 \times [1; 3, 1, ..., 1, ...]$ (voir [9]).

4.2. **Fractions continues à grands quotients partiels.** Dans le cas des fractions continues dont les quotients partiels sont suffisamment grands, on peut obtenir un algorithme s'apparentant aux formules de récurrence ci-dessus. Soit $(f, g)$ un intervalle standard et soit $u \in (f, g)$ dont l'image de la fraction continue par $(f \mapsto 0, g \mapsto 1)$ est $[a; b, ...]$. Supposons que $a$ et $b$ soient supérieurs strictement à un nombre premier $p$ impair, par lequel on veut multiplier $u$. Posons $h = fg^a$ et $k = (fg^a)^b g$ : alors l'image de la fraction continue de $h$ par $(f \mapsto 0, g \mapsto 1)$ est $[a]$ et celle de $k$ est $[a; b]$. On cherche deux entiers $c$ et $d$ tels que $(fg^c)_0$ et $((fg^a)^d g)_0$ soient divisibles par $p$ : $(p(fg^c), pg)$ et $(p(fg^a), p((fg^a)^d g)$ sont alors deux intervalles standard qui contiennent $ph$, $pk$, et surtout $pu$. Les entiers $c$ et $d$ correspondent à une suite que nous allons maintenant définir.

On multiplie $x = [a_0; a_1, a_2, ...]$ par $p$. Soit $(u_n)$ la suite définie par $u_0 = 0$, puis si $a_n \not\equiv u_{n-1} \pmod p$ alors $u_n$ est le plus petit entier positif congru à $-(a_n - u_{n-1})^{-1}$ modulo $p$ (ainsi $u_1 \equiv -a_1^{-1} \pmod p$, etc.), sinon $u_n = \infty$, $u_{n+1} = 0$ et ainsi de suite. On constate immédiatement que $(u_n)$ est majorée par $p$ qui est inférieur aux quotients partiels de $x$.

**Théorème 3.** *Soient $f_0 = 0$, $g_0 = 1$, et $f_n$, $g_n$ les mots de Christoffel correspondant respectivement à $[a_0; ..., a_{2n-2}]$ et $[a_0; ..., a_{2n-1}]$. Alors :*

- *Si $u_{2n-1} = \infty$, alors $p$ divise $(g_n)_0$, ainsi $(pf_n, pg_n)$ est standard, $pf_{n+1} = (pf_n)(pg_n)^{a_{2n}p}$, et l'image de la fraction continue de $pg_{n+1}$ par $(pf_n \mapsto 0, pg_n \mapsto 1)$ est la fraction continue de $\frac{p(a_{2n}a_{2n+1}+1)}{a_{2n+1}}$.*
- *Sinon, $(p(f_n g_n^{u_{2n-1}}), pg_n)$ est standard et l'image de la fraction continue de $pf_{n+1}$ par la substitution envoyant cet intervalle sur $(0,1)$ est la fraction continue de $\frac{a_{2n}-u_{2n-1}}{p}$.*
  *Si $u_{2n} = \infty$, $p$ divise $f_{n+1}$, $(pf_{n+1}, pg_n)$ est standard*
  *et $pg_{n+1} = (pf_{n+1})^{pa_{2n+1}}(pg_n)$ ; sinon, $(pf_{n+1}, p(f_{n+1}^{u_{2n}} g_n))$ est standard, et ainsi l'image de la fraction continue de $pg_{n+1}$ par la substitution envoyant cet intervalle sur $(0,1)$ est la fraction continue de $\frac{p}{a_{2n+1}-u_{2n}}$.*

On multiplie $x = [a_0; a_1, a_2, ...]$ par $p$, on obtient l'algorithme qui suit.

- **Initialisation.**

$$\begin{array}{rcll} u_0 & = & 0 & \\ u_1 & \equiv & -a_1^{-1} \pmod p & \text{si } p \text{ ne divise pas } a_1 \\ u_1 & = & \infty & \text{sinon} \\ p(01^{a_0}) & = & 01^{pa_0} & ((01^{pa_0}, 1) \text{ est standard}) \\ p((01^{a_0})^{a_1}1) & = & s(m) & \text{si } p \text{ ne divise pas } a_1 \\ p((01^{a_0})^{a_1}1) & = & (01^{pa_0})^{a_1/p}1 & \text{sinon.} \end{array}$$

  $m$ étant le mot de Christoffel de $p/a_1$, et $s$ la substitution

$$(0 \mapsto 01^{pa_0}, 1 \mapsto 1).$$

- **Boucle.** Tant que les quotients partiels de la fraction continue de $x$ ne sont pas épuisés, connaissant $pf_n$, $pg_n$, où $f_n$ correspond à $[a_0; a_1, ..., a_{2n-2}]$ et $g_n$ à $[a_0; a_1, ..., a_{2n-1}]$, on calcule les termes de $(u_n)$ et on effectue en même temps les opérations suivantes.
  - Si $u_{2n-1} = \infty$ alors $p$ divise $(g_n)_0$ et :

$$\begin{array}{rcccl} pf_{n+1} & = & p(f_n g_n^{a_{2n}}) & = & (pf_n)(pg_n)^{pa_{2n}} \\ pg_{n+1} & = & p((f_n g_n^{a_{2n}})^{a_{2n+1}} g_n) & = & s(m) \end{array}$$

    où $m$ est le mot de Christoffel associé à $p\frac{a_{2n}a_{2n+1}+1}{a_{2n+1}}$ et $s$ la substitution $(0 \mapsto pf_n, 1 \mapsto pg_n)$.
  - Sinon, on calcule $p(f_n g_n^{u_{2n-1}})$, et $pf_{n+1} = p(f_n g_n^{a_{2n}})$ est l'image du mot de Christoffel associé à $\frac{a_{2n}-u_{2n-1}}{p}$ par $(0 \mapsto p(f_n g_n^{u_{2n-1}}), 1 \mapsto$

$pg_n)$.
Si $u_{2n} = \infty$ alors $p$ divise $(f_n g_n^{a_{2n}})_0$. Ainsi

$$pg_{n+1} = (p(f_n g_n^{a_{2n}}))^{pa_{2n+1}}(pg_n).$$

Sinon on calcule $p((f_n g_n^{a_{2n}})^{u_{2n}} g_n)$, et $pg_{n+1}$ est l'image du mot de Christoffel associé à $\frac{p}{a_{2n+1}-u_{2n}}$ par

$$(0 \mapsto p(f_n g_n^{a_{2n}}), 1 \mapsto p((f_n g_n^{a_{2n}})^{u_{2n}} g_n)).$$

Le résultat est le dernier mot de Christoffel obtenu, et on sait retrouver la fraction continue correspondante en cas de besoin. Il reste à trouver une méthode permettant de calculer $p(f_n g_n^{u_{2n-1}})$ et $p((f_n g_n^{a_{2n}})^{u_{2n}} g_n)$ : c'est l'objet du paragraphe suivant.

4.3. **Fractions continues à petits quotients partiels.** L'algorithme précédent est inopérant lorsque les quotients partiels sont inférieurs aux termes correspondants de la suite $(u_n)$. On va donc maintenant exposer une méthode permettant de prendre le relais quand un tel cas se produit, et surtout de calculer, avec les notations du paragraphe précédent, $p(fg^c)$ et $p((fg^a)^d g)$.

*Base théorique : intervalles non standard.* Lorsque $(pf, pg)$ n'est pas standard, $p(fg)$ ne peut s'exprimer à l'aide de $pf$ et $pg$. Néanmoins $p(fg)$ appartient à un intervalle standard contenu dans $(pf, pg)$.

Soient $f$, $g$ deux mots de Christoffel : on peut construire une suite de mots de Christoffel dont $f$ est le premier terme, $g$ le dernier, et dont deux termes consécutifs forment un intervalle standard.

**Proposition 1.** *Soient $f < g$ deux mots de Christoffel non vides et non simultanément égaux respectivement à 0 et 1. Alors il existe un mot de Christoffel noté $\mu(f,g)$ et deux entiers naturels $d_1(f,g)$, $d_2(f,g)$ tels que :*

$$\mu(f,g)_\gamma < f < f_\delta < \ldots < f_{\delta^{d_1(f,g)}}$$
$$= \mu(f,g) = g_{\gamma^{d_2(f,g)}} < \ldots < g_\gamma < g < \mu(f,g)_\delta$$

*La suite ainsi définie est notée $S(f,g)$ ; celle des intervalles standard sous-jacents est désignée par $I(f,g)$, et $(\mu(f,g)_\gamma, \mu(f,g)_\delta)$ s'écrit $(\gamma(f,g), \delta(f,g))$. La substitution standard qui envoie*
*$(\gamma(f,g), \delta(f,g))$ sur $(0,1)$ est notée $\Sigma_{(f,g)}$.*

*Preuve.* Si $h$ est un mot de Christoffel non vide, différent de 0 ou 1, $(h_\gamma, h)$ et $(h, h_\delta)$ sont deux intervalles standard contigus ; la suite $(f_{\delta^i})$ est une suite croissante dont le dernier terme
vaut 1 et $(g_{\gamma^j})$ est décroissante de dernier terme 0 : comme $0 \le f < g \le 1$ il existe alors deux entiers naturels $i_0$ et $j_0$ tels que

$$g_{\gamma^{j_0+1}} < f_{\delta^{i_0}} \le g_{\gamma^{j_0}} < f_{\delta^{i_0+1}},$$

d'où $f_{\delta^{i_0}} \in (g_{\gamma^{j_0+1}}, g_{\gamma^{j_0}})$ et $g_{\gamma^{j_0}} \in (f_{\delta^{i_0}}, f_{\delta^{i_0+1}})$, ce qui signifie en particulier que l'occurrence $g_{\gamma^{j_0}}$ apparaît dans $f_{\delta^{i_0}}$ et qu'inversement, $f_{\delta^{i_0}}$ apparaît dans $g_{\gamma^{j_0}}$. Ceci n'est possible que si $f_{\delta^{i_0}} = g_{\gamma^{j_0}}$ : ainsi,

$$f < f_\delta < ... < f_{\delta^{i_0}} = g_{\gamma^{j_0}} < ... < g_\gamma < g.$$

On en déduit l'existence et l'unicité de $\mu$, $d_1$ et $d_2$ ; Supposons maintenant que $\mu(f,g)_\gamma \geq f$ : alors il existe $i$ tel que $\mu(f,g)_\gamma \in (f_{\delta^i}, f_{\delta^{i+1}})$, ce qui est impossible car $\mu(f,g)_\gamma$ est un préfixe d'un suffixe de $f_{\delta^i}$ et $f_{\delta^{i+1}}$. Il en va de même si on suppose que $g \geq \mu(f,g)_\delta$, donc $\mu(f,g)_\gamma < f$ et $g < \mu(f,g)_\delta$ ce qui achève la démonstration.

**Exemples.**

- Si $(f,g)$ est standard mais différent de $(0,1)$, $f_\delta = g$ ou $g_\gamma = f$ et donc $\mu(f,g) = g$ ou $f$, $S(f,g) = (f;g)$, $I(f,g) = ((f,g))$ et $(\gamma(f,g), \delta(f,g)) = (g_\gamma, g_\delta)$ ou $(f_\gamma, f_\delta)$.
- Soient $f = 010101011$ et $g = 01011011$. Alors $\mu(f,g) = 01011$, $S(f,g) = (010101011; 0101011; 01011; 01011011)$ et $(\gamma(f,g), \delta(f,g)) = (01, 011)$

On utilise maintenant ces résultats lorsque $f$ et $g$ sont les multiples des bornes d'un intervalle standard.

4.4. **Algorithme de multiplication.** Soit $m$ un mot de Christoffel appartenant à un intervalle standard $(f,g)$ et $q$ un entier plus grand que 3. On veut savoir quel intervalle standard de $I(qf,qg)$ contient $qm$ et quelle est l'image de la fraction continue de $qm$ par la substitution qui envoie cet intervalle sur $(0,1)$.

On considère la multiplication par un nombre premier $p$. Supposons que $p$ ne divise ni $f_0$ ni $g_0$ : donc $(pf)_0 = f_0$, $(pg)_0 = g_0$, $(pf)_1 = pf_1$ et $(pg)_1 = pg_1$. Soit $u$ l'image de $m$ par $(f \mapsto 0, g \mapsto 1)$ et $v$ l'image de $pm$ par la substitution envoyant l'intervalle standard $(z,z')$ de $I(pf,pg)$ auquel appartient $pm$ sur $(0,1)$. Multiplier $m$ par $p$ revient à substituer $pf$ à 0 et $pg$ à 1 dans $u$ : on obtient ainsi un mot de même pente que $pm$, mais qui n'est pas de Christoffel puisque $(pf,pg)$ n'est pas standard. Cela revient à effectuer le calcul suivant (voir [2] et [8]) :

$$\begin{pmatrix} (pg)_1 & (pf)_1 \\ (pg)_0 & (pf)_0 \end{pmatrix} \begin{pmatrix} u_1 \\ u_0 \end{pmatrix} = \begin{pmatrix} (pm)_1 \\ (pm)_0 \end{pmatrix}.$$

Comme $pm \in (z,z')$, il existe une permutation de 0 et de 1 permettant de faire apparaître le mot de Christoffel $pm$ écrit avec $z$ et $z'$ : on remplace alors $z$ par 0 et $z'$ par 1. On obtient $v$ et le calcul est le suivant (pour les matrices de substitutions standard voir [2] ou [8]) :

$$\begin{pmatrix} v_1 \\ v_0 \end{pmatrix} = \begin{pmatrix} z'_1 & z_1 \\ z'_0 & z_0 \end{pmatrix}^{-1} \begin{pmatrix} (pm)_1 \\ (pm)_0 \end{pmatrix} = \begin{pmatrix} z_0 & -z_1 \\ -z'_0 & z'_1 \end{pmatrix} \begin{pmatrix} (pm)_1 \\ (pm)_0 \end{pmatrix}$$

$$= \begin{pmatrix} z_0 & -z_1 \\ -z'_0 & z'_1 \end{pmatrix} \begin{pmatrix} (pg)_1 & (pf)_1 \\ (pg)_0 & (pf)_0 \end{pmatrix} \begin{pmatrix} u_1 \\ u_0 \end{pmatrix}$$
$$= \begin{pmatrix} \det(z, pg) & -\det(pf, z) \\ -\det(z', pg) & \det(pf, z') \end{pmatrix} \begin{pmatrix} u_1 \\ u_0 \end{pmatrix}.$$

La fraction continue de $u$ est connue et est courte : il suffit donc de trouver $(z, z')$ pour obtenir $v$ en multipliant par la matrice des déterminants ci-dessus, qu'on note $M(z, z')$ ; d'autre part :

$$\begin{pmatrix} v_1 \\ v_0 \end{pmatrix} = \begin{pmatrix} \det(z, pm) \\ \det(pm, z') \end{pmatrix}.$$

Le bon intervalle est donc celui pour lequel les $v_1$ et $v_0$ obtenus sont simultanément positifs. Il faut donc tester tous les intervalles de $I(pf, pg)$.

Si maintenant $p$ divise $m_0$ on peut suivre l'évolution du calcul précédent pour s'apercevoir que $p = \mathrm{pgcd}(v_0, v_1)$ dans le cas où $v_0$ et $v_1$ sont non nuls, et que $p$ est égal à l'un si l'autre est nul. L'explication en est que si on substitue dans $m$ le mot $pf$ à $f$, $pg$ à $g$ et qu'on réordonne de manière à obtenir un mot de Christoffel, puisque $p$ divise $m_0$, $(pf)_1$ et $(pg)_1$, le résultat sera l'itéré $p$ fois de $pm$ ; $v_0 = 0$ ou $v_1 = 0$ implique $\det(pm, z') = 0$ ou $\det(z, pm) = 0$ donc $pm = z'$ ou $pm = z$. On voit alors qu'il est possible de généraliser l'algorithme à la multiplication par des nombres non premiers.

L'algorithme est pour l'essentiel celui adapté aux grands quotients partiels : ce qui change, c'est qu'on peut calculer $p(f_n g_n^{u_{2n-1}})$ et $p((f_n g_n^{a_{2n}})^{u_{2n}} g_n)$. Ainsi la phase d'initialisation est la même ; puis si on suppose qu'on connaît $pf_n$ et $pg_n$ on calcule $pf_{n+1}$ et $pg_{n+1}$ de la même manière. On cherche alors quand c'est nécessaire $p(f_n g_n^{u_{2n-1}})$ et $p((f_n g_n^{a_{2n}})^{u_{2n}} g_n)$ : si $u_{2n-1} = 0$ ou $u_{2n} = 0$ c'est évident : supposons alors que tel n'est pas le cas.

- Si $u_{2n-1}$ est non nul et différent de l'infini : on calcule $I(pf_n, pg_n)$ et pour chaque intervalle $(z, z')$ de $I(pf_n, pg_n)$ on calcule :
$$\begin{pmatrix} v_1 \\ v_0 \end{pmatrix} = \begin{pmatrix} \det(z, pg_n) & -\det(pf_n, z) \\ -\det(z', pg_n) & \det(pf_n, z') \end{pmatrix} \begin{pmatrix} u_{2n-1} \\ 1 \end{pmatrix}$$
ainsi $p(f_n g_n^{u_{2n-1}})$ est l'image du mot de Christoffel de pente $v_1/v_0$ par $(0 \mapsto z, 1 \mapsto z')$.
- De même, si $u_{2n}$ est non nul et différent de l'infini : on calcule $I(pf_{n+1}, pg_n)$ et pour chaque intervalle $(z, z')$ de $I(pf_{n+1}, pg_n)$ :
$$\begin{pmatrix} v_1 \\ v_0 \end{pmatrix} = \begin{pmatrix} \det(z, pg_n) & -\det(pf_{n+1}, z) \\ -\det(z', pg_n) & \det(pf_{n+1}, z') \end{pmatrix} \begin{pmatrix} 1 \\ u_{2n} \end{pmatrix}$$
ainsi $p((f_n g_n^{a_{2n}})^{u_{2n}} g_n)$ est l'image du mot de Christoffel de pente $v_1/v_0$ par $(0 \mapsto z, 1 \mapsto z')$.

Bien entendu à chaque fois $v_1/v_0$ est comme prévu l'unique couple d'entiers obtenus qui soient simultanément positifs.

Puis si $a_{2n} < u_{2n-1}$ ou $a_{2n+1} < u_{2n}$ on remplace dans les expressions ci-dessus $u_{2n-1}$ par $a_{2n}$ ou $u_{2n}$ par $a_{2n+1}$.

On entre maintenant dans le détail de l'algorithme. Posent problème le passage d'une fraction continue à son mot de Christoffel puis les calculs successifs des coefficients des matrices $M(z,z')$.

*Calcul des déterminants.* Le calcul du déterminant d'un couple de mots de Christoffel fait intervenir les réduites des fractions continues correspondantes donc ne doit pas être calculé de façon intrinsèque. Le calcul se fait par récurrence et n'utilise que des additions et des multiplications : on évite ainsi de manipuler des nombres trop grands puisqu'ils sont majorés par le résultat.

Soit $(f,g)$ un couple de mots de Christoffel dont on veut calculer le déterminant : $f \in (\gamma(f,g), \mu(f,g))$ et $g \in (\mu(f,g), \delta(f,g))$ : alors l'image de $f$ par $(\gamma(f,g) \mapsto 0, \mu(f,g) \mapsto 1)$ et l'image de $g$ par $(\mu(f,g) \mapsto 0, \delta(f,g) \mapsto 1)$ existent, et d'autre part :

$$\det(f,g) = \det(f_\gamma, g_\gamma) + \det(f_\gamma, g_\delta) + \det(f_\delta, g_\gamma) + \det(f_\delta, g_\delta).$$

Ces quatre déterminants peuvent à leur tour se décomposer de la même manière et on finit par obtenir :

$$\begin{array}{rclcl} \det(f,g) & = & \alpha\det(\gamma(f,g),\mu(f,g)) & + & \beta\det(\gamma(f,g),\delta(f,g)) \\ & + & \varepsilon\det(\mu(f,g),\mu(f,g)) & + & \varphi\det(\mu(f,g),\delta(f,g)) \\ & = & \alpha+\beta+\varphi. & & \end{array}$$

Pour ce qui concerne le calcul des coefficients de la matrice $M(z,z')$ il est possible de simplifier l'algorithme : en effet il existe $i$ tel que $z = (pf)_{\delta^i}$ ou $(pg)_{\gamma^{i+1}}$ et $z' = (pf)_{\delta^{i+1}}$ ou $z' = (pg)_{\gamma^i}$. Or, $\mu(pf,(pf)_{\delta^i}) = (pf)_{\delta^i}$, $\mu((pg)_{\gamma^i},pg) = (pg)_{\gamma^i}$ et $\mu(pf,(pg)_{\gamma^i}) = \mu((pf)_{\delta^i},pg) = \mu(pf,pg)$ d'où finalement :

$$\left\{\begin{array}{rclcl} \det(pf,(pg)_{\gamma^{j-1}}) & = & \det(pf,(pg)_{\gamma^j}) & + & \det(pf,(pg)_{\gamma^{j-1}\delta}) \\ \det((pf)_{\delta^{j-1}},pg) & = & \det((pf)_{\delta^{j-1}\gamma},pg) & + & \det((pf)_{\delta^j},pg) \end{array}\right.$$

D'autre part :

$$\left\{\begin{array}{rclcl} \det(pf,(pf)_{\delta^{i-1}}) & = & \det(pf,(pf)_{\delta^{i-1}\gamma}) & + & \det(pf,(pf)_{\delta^i}) \\ \det((pg)_{\gamma^{j-1}},pg) & = & \det((pg)_{\gamma^j},pg) & + & \det((pg)_{\gamma^{j-1}\delta},pg) \end{array}\right.$$

On considère les mots de Christoffel les images $\varphi_i$ et $\psi_j$ de $f$ et $g$, respectivement par les substitutions standard $(\gamma(pf,(pf)_{\delta^i}) \mapsto 0, \mu(pf,(pf)_{\delta^i}) \mapsto 1)$ et $(\mu((pg)_{\gamma^j},pg) \mapsto 0, \delta((pg)_{\gamma^j},pg) \mapsto 1)$. Les deux égalités ci-dessus permettent d'écrire :

$$\left\{\begin{array}{rclcl} (\varphi_{i-1})_0 & = & -(\varphi_{i-1})_1 & + & (\varphi_i)_0 \\ (\psi_{j-1})_1 & = & (\psi_j)_1 & - & (\psi_{j-1})_0 \end{array}\right.$$

puis on utilisera :

$$\begin{cases} \det(pf,(pf)_{\delta^i}) & = & (\varphi_i)_0 \\ \det((pg)_{\gamma^j},pg) & = & (\psi_j)_1 \end{cases}$$

Il est donc nécessaire de calculer $(\varphi_i)_0$, $(\varphi_i)_1$, $(\psi_j)_0$ et $(\psi_j)_1$ par récurrence. On a déjà obtenu :

$$\begin{cases} (\varphi_i)_0 & = & (\varphi_{i-1})_0 & + & (\varphi_{i-1})_1 \\ (\psi_j)_1 & = & (\psi_{j-1})_0 & + & (\psi_{j-1})_1 \end{cases}$$

Puis on doit considérer les deux cas suivants.

- Si les fractions continues de $(pf)_{\delta^{i-1}}$ et $(pg)_{\gamma^{j-1}}$ ont un nombre de quotients partiels respectivement pair et impair alors écrivons $(pf)_{\delta^{i-1}} = u^a v$ et $(pg)_{\gamma^{j-1}} = u'v'^b$, ainsi :

$$\begin{array}{rclcrcl} (pf)_{\delta^i} & = & u^{a-1}v & \text{et} & (pg)_{\gamma^j} & = & u'v'^{b-1} \\ (pf)_{\delta^{i-1}\gamma} & = & u & \text{et} & (pg)_{\gamma^{j-1}\delta} & = & v' \\ (pf)_{\delta^i\gamma} & = & u & \text{et} & (pg)_{\gamma^j\delta} & = & v' \end{array}$$

donc $(pf)_{\delta^{i-1}\gamma} = (pf)_{\delta^i\gamma}$ et $(pg)_{\gamma^{j-1}\delta} = (pg)_{\gamma^j\delta}$. D'où :

$$\begin{cases} (\varphi_i)_1 & = & \det((pf)_{\delta^i\gamma},pf) & = & \det((pf)_{\delta^{i-1}\gamma},pf) & = & (\varphi_{i-1})_1 \\ (\psi_j)_0 & = & \det(pg,(pg)_{\gamma^j\delta}) & = & \det(pg,(pg)_{\gamma^{j-1}\delta}) & = & (\psi_{j-1})_0 \end{cases}$$

- Si maintenant les fractions continues de $(pf)_{\delta^{i-1}}$ et $(pg)_{\gamma^{j-1}}$ ont un nombre de quotients partiels respectivement impair et pair, soit $(pf)_{\delta^{i-1}} = uv^a$ et $(pg)_{\gamma^{j-1}} = u'^b v'$ :

$$\begin{array}{rclcrcl} (pf)_{\delta^i} & = & v & \text{et} & (pg)_{\gamma^j} & = & u' \\ (pf)_{\delta^{i-1}\gamma} & = & uv^{a-1} & \text{et} & (pg)_{\gamma^{j-1}\delta} & = & u'^{b-1}v' \\ (pf)_{\delta^i\gamma} & = & u = v_\gamma & \text{et} & (pg)_{\gamma^j\delta} & = & v' = u'_\delta \end{array}$$

d'où cette fois :

$$\begin{cases} (\varphi_i)_1 & = & a(\varphi_{i-1})_1 & + & (a-1)(\varphi_{i-1})_0 \\ (\psi_j)_0 & = & b(\psi_{j-1})_0 & + & (b-1)(\psi_{j-1})_1 \end{cases}$$

L'algorithme est le suivant :

- **Initialisation.** $i = j = 0$, $\det(pf,pf) = \det(pg,pg) = 0$, $\varphi_0 = \psi_0 = 1$ ; $\det(pf,pg) = p$.
- **Boucle.** Aux étapes $i$ et $j$, soient $a$ et $b$ les derniers quotients partiels des fractions continues de $f_{\delta^{i-1}}$ et $g_{\gamma^{j-1}}$.
  - Si les fractions continues de $f_{\delta^{i-1}}$ et $g_{\gamma^{j-1}}$ possèdent un nombre respectivement impair et pair de quotients partiels :

$$\begin{pmatrix} (\varphi_i)_1 \\ (\varphi_i)_0 \end{pmatrix} = \begin{pmatrix} a & a-1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} (\varphi_{i-1})_1 \\ (\varphi_{i-1})_0 \end{pmatrix}$$

$$\begin{pmatrix} (\psi_j)_1 \\ (\psi_j)_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ b & b-1 \end{pmatrix} \begin{pmatrix} (\psi_{j-1})_1 \\ (\psi_{j-1})_0 \end{pmatrix}$$

– Si les fractions continues de $f_{\delta^{i-1}}$ et $g_{\gamma^{j-1}}$ possèdent un nombre respectivement pair et impair de quotients partiels :

$$\begin{pmatrix} (\varphi_i)_1 \\ (\varphi_i)_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} (\varphi_{i-1})_1 \\ (\varphi_{i-1})_0 \end{pmatrix}$$

et

$$\begin{pmatrix} (\psi_j)_1 \\ (\psi_j)_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} (\psi_{j-1})_1 \\ (\psi_{j-1})_0 \end{pmatrix}$$

Il faut ici souligner le fait que les deux cas cités ci-dessus regroupent en fait les quatre suivants : le nombre de quotients partiels des fractions continues de $f$ et $g$ est respectivement pair et impair ; impair et pair ; les deux sont pairs ; les deux sont impairs. On a pu regrouper en deux cas, suivant le résultat, puisque les parités des longueurs des deux fractions continues sont indépendantes. Ainsi :

$$\left\{ \begin{array}{lcl} \det(pf, (pf)_{\delta^i}) & = & (\varphi_i)_0 \\ \det((pg)_{\gamma^j}, pg) & = & (\psi_j)_1 \end{array} \right.$$

Puis :

$$\left\{ \begin{array}{lclcl} \det((pf)_{\delta^i}, pg) & = & \det((pf)_{\delta^{i-1}}, pg) & - & \det((pf)_{\delta^{i-1}\gamma}, pg) \\ \det(pf, (pg)_{\gamma^j}) & = & \det(pf, (pg)_{\gamma^{j-1}}) & - & \det(pf, (pg)_{\gamma^{j-1}\delta}) \end{array} \right.$$

## Bibliographie


[1] J.-P. Borel, F. Laubie, *Construction de mots de Christoffel*, C. R. Acad. Sci. Paris **313**, sér. 1 (1991), 483–485.

[2] J.-P. Borel, F. Laubie, *Quelques mots sur la droite projective réelle*, J. Théor. Nombres Bordeaux **5** (1993), 23–51.

[3] T.C. Brown, *Description of the characteristic sequence of an irrational*, Canad. Math. Bull. **36** (1993), 15–21.

[4] H. Cohen, *Multiplication par un entier d'une fraction continue périodique*, Acta arith. **26** (1974), 129–148.

[5] D. Crisp, W. Moran, A. Pollington, P. Shiue, *Substitution invariant cutting sequences*, J. Théor. Nombres Bordeaux **5** (1993), 123–137.

[6] M. Hall, *On the sum and product of continued fractions*, Ann. of Math. **48** (1947), 966–993.

[7] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*, Clarendon press, Oxford, 4th ed., 1960.

[8] F. Laubie, *Prolongements homographiques de substitutions de mots de Christoffel*, C. R. Acad. Sci. Paris **313**, sér. 1 (1991), 565–567

[9] F. Laubie, E. Laurier, *Calcul de multiples de mots de Christoffel*, C. R. Acad. Sci. Paris **320**, sér. 1 (1995), 765–768.

[10] É. Laurier, *Addition et multiplication par un entier des mots de Christoffel*, Thèse, Limoges, 1995.

[11] M. Lothaire, *Combinatorics on Words. Encyclopedia of mathematics and its applications*, Cambridge university press, 1983.

[12] R.C. Lyndon, *Equations in free groups*, Trans. Amer. math. soc. (96), 445–457.

[13] M. Mendès France, *Sur les fractions continues limitées*, Acta Arith. **23** (1973), 207–215.

[14] G.N. Raney, *On continued fractions and finite automata*, Math. Ann. **206** (1973), 265–283.

Éric Laurier
Lycée L. de Vinci
115 route des Petits-Ponts
93290 Tremblay, France
*E-mail* : eric.laurier@unilim.fr