Ann. Sc. Math. Québec, 1978, vol. II, No 2, pp. 289-304

SUR LA DÉCOMPOSITION DES OPÉRATIONS EN BITS ET EN PITS

Gilbert Labelle

1. INTRODUCTION

Soient p un nombre premier et $x \in \mathbb{N}$. Si l'écriture de x en base p est

$$x = x_0 + x_1 p + x_2 p^2 + \ldots \tag{1}$$

on conviendra de dire que x_i est le $i^{\text{ième}}$ pit de x (bit si $p = 2$).

Etant donnée une opération quelconque du type

$$f : \mathbb{N}^r \to \mathbb{N} , \quad z = f(x,y,\ldots) , \quad r \geq 0 \tag{2}$$

le problème général considéré ici est d'étudier et d'exprimer les pits z_i $(i = 0,1,2,\ldots)$ de z à l'aide des pits de $x,y,\ldots$. Comme on peut canoniquement identifier un pit quelconque à un élément du corps $\mathbb{F}_p$ des entiers modulo p, il est naturel de demander des expressions pour les z_i qui soient des éléments de l'anneau $\mathbb{F}_p[[x_0,x_1,x_2,\ldots,y_0,y_1,y_2,\ldots,\ldots]]$ des séries formelles à coefficients dans $\mathbb{F}_p$ en les variables $x_0,x_1,x_2,\ldots,y_0,y_1,y_2,\ldots,\ldots$. A cause du petit théorème de Fermat [6] qui dit que $a^p \equiv a \pmod p$ pour tout entier a, on ne perd aucune généralité en demandant, dans nos séries formelles, que chaque variable apparaisse avec un degré $\leq p - 1$. Remarquons aussi que la "substitution" est toujours "sommable" pour de tels types de séries formelles en ce sens que chaque fois que les variables $x_0,x_1,x_2,\ldots,y_0,y_1,y_2,\ldots,\ldots$ prennent simultènament les valeurs des pits de nombres naturels donnés $m,n,\ldots$ alors la somme obtenue ne contient qu'un nombre fini de termes non nuls.

Nous utiliserons à maintes reprises les nombres de Stirling [1] dans le présent texte. Rappelons donc l'une des définitions qu'on peut leur donner. Si on désigne par $x^{(n)}$ le polynôme $x(x-1)(x-2)\ldots(x-n+1)$ alors les suites $(x^{(n)})_{n\geq 0}$ et $(x^n)_{n\geq 0}$ forment chacune une base du $\mathbf{Z}$-module $\mathbf{Z}[x]$. Les nombres de Stirling sont des entiers décrivant les matrices (triangulaires inférieures infinies) de changements de bases associées. Plus précisément, les nombres de Stirling de la première espèce $\$_n^{(m)}$ et de la deuxième espece $\$\!\!\!\$_n^{(m)}$ sont donnés par les identités

$$x^{(n)} = \sum_{m\geq 0} \$_n^{(m)} x^m \quad \text{et} \quad x^n = \sum_{m\geq 0} \$\!\!\!\$_n^{(m)} x^{(m)} \ . \tag{3}$$

La notation $\binom{m}{n}$ désignera les coefficients du binôme habituels. Les résultats contenus dans le présent article généralisent, unifient et simplifient certains théorèmes que P. Camion [2] a obtenus pour le cas des bits $(p = 2)$. Dans ce même contexte binaire, ils recoupent aussi certains travaux de I. Rosenberg [9, 10]. Nous travaillerons surtout dans le cas où f est à deux variables $(r = 2)$. Le cas r quelconque s'obtient très facilement à partir de ce dernier.

2. FORMULES GÉNÉRALES

Dans ce qui suit, p est un nombre premier fixé et, pour ne pas alourdir inutilement les notations, nous allons désigner simplement par "$\equiv$" l'égalité dans $\mathbb{F}_p$ ainsi que dans tout anneau à "coefficients" dans $\mathbb{F}_p$ que l'on rencontrera. On omettra donc la mention mod p lorsque le contexte sera clair.

Trois matrices carrées A, B, C chacune d'ordre $p \times p$ et à coefficients dans $\mathbb{F}_p$ s'avèreront utiles. Les cases de ces matrices seront symbolisées par:

$$A \equiv (\binom{m}{\mu}) \ , \quad 0 \leq m \ , \quad \mu \leq p - 1 \tag{4}$$

$$B \equiv (\{\begin{matrix} m \\ \mu \end{matrix}\}) \ , \quad 0 \leq m \ , \quad \mu \leq p - 1 \tag{5}$$

$$C \equiv (\left[\begin{matrix} m \\ \mu \end{matrix}\right]) \ , \quad 0 \leq m \ , \quad \mu \leq p - 1 \tag{6}$$

Elles sont définies comme suit:

$$A \equiv \begin{bmatrix} \binom{0}{0} & 0 & 0 & \cdots & \binom{0}{\mu} & \cdots & 0 \\ \binom{1}{0} & \binom{1}{1} & 0 & \cdots & \binom{1}{\mu} & \cdots & 0 \\ \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & \cdots & \binom{2}{\mu} & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \binom{p-1}{0} & \binom{p-1}{1} & \binom{p-1}{2} & \cdots & \binom{p-1}{\mu} & \cdots & \binom{p-1}{p-1} \end{bmatrix}$$

$$B \equiv \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & -1^{-1} & -2^{-1} & \cdots & -\mu^{-1} & \cdots & -(p-1)^{-1} \\ 0 & -1^{-2} & -2^{-2} & \cdots & -\mu^{-2} & \cdots & -(p-1)^{-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & -1 & -1 & \cdots & -1 & \cdots & -1 \end{bmatrix}$$

$$C \equiv \begin{bmatrix} \frac{1}{0!}\$_1^{(0)} & \frac{1}{1!}\$_1^{(0)} & \frac{1}{2!}\$_2^{(0)} & \cdots & \frac{1}{\mu!}\$_\mu^{(0)} & \cdots & \frac{1}{p-1!}\$_{p-1}^{(0)} \\ 0 & \frac{1}{1!}\$_1^{(1)} & \frac{1}{2!}\$_2^{(1)} & \cdots & \frac{1}{\mu!}\$_\mu^{(1)} & \cdots & \frac{1}{p-1!}\$_{p-1}^{(1)} \\ 0 & 0 & \frac{1}{2!}\$_2^{(2)} & \cdots & \frac{1}{\mu!}\$_\mu^{(2)} & \cdots & \frac{1}{p-1!}\$_{p-1}^{(2)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & \cdots & \frac{1}{p-1!}\$_{p-1}^{(p-1)} \end{bmatrix}$$

Notre première représentation des pits de f s'appuie sur la matrice A et fait appel à un théorème de E. Lucas [8] [4], concernant les propriétés de congruences des coefficients du binôme.

Théorème L (E. Lucas). Soient $m,\mu \in \mathbb{N}$ deux entiers naturels. Si $m = \Sigma m_i p^i$ et $\mu = \Sigma \mu_i p^i$ sont leurs écritures en base p, alors

$$\binom{m}{\mu} \equiv \binom{m_0}{\mu_0}\binom{m_1}{\mu_1}\binom{m_2}{\mu_2} \ldots \pmod{p} . \tag{7}$$

Une conséquence immédiate de ce théorème est que les pits z_i d'un entier naturel z peuvent s'écrire sous la forme

$$z_i \equiv \binom{z}{p^i}, \quad i = 0,1,2,\ldots \tag{8}$$

Remarquons que pour $m \in \mathbb{N}$, le polynôme $\binom{x}{m} = x^{(m)}/m!$ est un élément de l'anneau $\mathbb{Q}[x]$ et que si $0 \leq m < p$ alors $\binom{x}{m}$ peut être considéré comme un élément de l'anneau $\mathbb{F}_p[x]$. En effet, dans ce dernier cas $m!$ est inversible dans $\mathbb{F}_p$. Ces considérations nous amènent à formuler notre première décomposition en pits.

Théorème I (première décomposition en pits). Si $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(z = f(x,y))$ et si p est un nombre premier, alors pour tout $i,m,n \in \mathbb{N}$, $\exists! \alpha_{m,n}(i) \in \mathbb{F}_p$ tel que

$$z_i \equiv \sum_{m,n\geq 0} \alpha_{m,n}(i)\binom{x_0}{m_0}\binom{x_1}{m_1}\binom{x_2}{m_2} \ldots \binom{y_0}{n_0}\binom{y_1}{n_1}\binom{y_2}{n_2} \ldots \tag{9}$$

De plus, chaque $\alpha_{m,n}(i)$ peut s'écrire sous la forme

$$\alpha_{m,n}(i) \equiv \sum_{\substack{0\leq\mu\leq m \\ 0\leq\nu\leq n}} (-1)^{m-\mu+n-\nu} \binom{m}{\mu}\binom{n}{\nu} (f(\mu,\nu))_i \tag{10}$$

où $(f(\mu,\nu))_i$ désigne le $i^{\text{ième}}$ pit du nombre $f(\mu,\nu)$.

Démonstration. La version discrète de Newton [5] de la formule de MacLaurin nous permet d'écrire pour chaque $k \geq 0$

$$\binom{z}{k} = \binom{f(x,y)}{k} = \sum_{m,n\geq 0} U_k^{m,n} \binom{x}{m}\binom{y}{n} \tag{11}$$

où les $U_k^{m,n} = U_k^{m,n}(f)$ sont des entiers donnés explicitement par

$$U_k^{m,n} = \Delta_x^m \Delta_y^n \left.\binom{f(x,y)}{k}\right|_{x=y=0} \tag{12}$$

et où Δ_x , Δ_y désignent les opérateurs classiques de différences relatifs aux variables x et y respectivement. Le développement binomial bien connu [5] de $\Delta^s = (E-I)^s$ où E désigne l'opérateur de translation nous donne alors

$$U_k^{m,n} = \sum_{\substack{0\leq\mu\leq m \\ 0\leq\nu\leq n}} (-1)^{n-\mu+n-\nu} \binom{m}{\mu}\binom{n}{\nu}\binom{f(\mu,\nu)}{k}. \tag{13}$$

On obtient (9) et (10) en posant $k = p^i$ dans (11) et en utilisant (7) et (8). On vérifie facilement l'unicité des $\alpha_{m,n}(i)$ et la sommabilité de (9).

Le calcul de (10) se simplifie grandement si on utilise la matrice A et le théorème de Lucas. De plus, on peut restreindre cette sommation aux seuls indices μ et ν tels que

$$0 \mathrel{.:} \mu \mathrel{.:} m \ , \quad 0 \mathrel{.:} \nu \mathrel{.:} n \tag{14}$$

où $a \mathrel{.:} b$ désigne la relation d'inégalité pit à pit (i.e. $(\forall i)\ a_i \leq b_i$) . En effet, on tire de (7) que pour les autres indices μ,ν le terme correspondant de (10) s'annule. On retrouve une utilisation de ce type d'inégalité pour le cas des bits ($p = 2$) dans I. Rosenberg [9] par exemple.

En remplaçant, dans (10), les coefficients du binôme en jeu par leurs produits associés selon (7) on obtient aussi la formule

$$\alpha_{m,n}(i) \equiv (E_x-I)^{m_0}(E_x^p-I)^{m_1}(E_x^{p^2}-I)^{m_2}\ldots(E_y-I)^{n_0}(E_y^p-I)^{n_1}(E_y^{p^2}-I)^{n_2}\ldots(f(0,0))_i. \tag{15}$$

La démonstration du théorème I montre que les nombres entiers $U_k^{m,n} = U_k^{m,n}(f)$ jouent un rôle fondamental dans la représentation (9) en ce sens que $\alpha_{m,n}(i) \equiv U_{p^i}^{m,n}$. Ces nombres $U_k^{m,n}$ ont des propriétés combinatoires intéressantes comme on le verra dans la section 3.

Pour le moment nous allons donner une récurrence permettant de les engendrer systématiquement.

Théorème R (Récurrence). Pour $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, les nombres entiers $U_k^{m,n}$ définis par

$$\binom{f(x,y)}{k} = \sum_{m,n\geq 0} U_k^{m,n} \binom{x}{m}\binom{y}{n} \tag{16}$$

satisfont la récurrence (sur k) suivante

i) $U_0^{m,n} = \delta_0^m \, \delta_0^n$

et

$$\begin{aligned} \text{ii)}\ U_{k+1}^{m,n} = \frac{1}{k+1} \{ &(f(m,n) - k)U_k^{m,n} + m(f(m,n) - f(m-1,n))U_k^{m-1,n} \\ &+ n(f(m,n) - f(m,n-1))U_k^{m,n-1} \\ &+ \ldots + \binom{m}{\mu}\binom{n}{\nu}(\Delta_x^\mu \, \Delta_y^\nu \, f(m-\mu\,,\, n-\nu))U_k^{m-\mu,n-\nu} + \ldots\} \end{aligned} \tag{17}$$

où δ_j^i désigne le symbole usuel de Kronecker.

Démonstration. La partie i) découle immédiatement du fait que $\binom{f(x,y)}{0} = 1$ pour tout $x,y \in \mathbb{N}$. La partie ii) est beaucoup plus difficile à établir. Nous allons esquisser les idées de base entrant dans sa formation. De l'identité binomiale

$$\binom{f(x,y)}{k+1} = \frac{f(x,y)-k}{k+1} \binom{f(x,y)}{k}$$

on peut écrire

$$\binom{f(x,y)}{k+1} = \frac{1}{k+1} \left(\sum_{m,n\geq 0} f(x,y) U_k^{m,n} \binom{x}{m}\binom{y}{n} \right) - \frac{k}{k+1} \binom{f(x,y)}{k} . \tag{18}$$

Appliquant maintenant à $f(x,y)$ la version discrète de Newton de la formule de MacLaurin mentionnée plus haut, on obtient

$$\binom{f(x,y)}{k+1} = \frac{1}{k+1} \left(\sum_{m,n,r,s} \sigma_{r,s} U_k^{m,n} \binom{x}{r}\binom{x}{m}\binom{y}{s}\binom{y}{n} \right) - \frac{k}{k+1} \binom{f(x,y)}{k} \tag{19}$$

où $\sigma_{r,s} = \Delta_x^r \Delta_y^s f(0,0)$. Réarrangeant les termes de la sommation (19) en utilisant l'identité (démontrable par induction)

$$t^{(u)}t^{(v)} = \sum_{i\geq 0} \frac{u^{(i)}v^{(i)}}{i!} t^{(u+v-i)} \quad , \quad u,v \in \mathbb{N}$$

on arrive à une expression de la forme

$$\binom{f(x,y)}{k+1} = \frac{1}{k+1}\left[\sum_{\mu,\nu,r,s} \sigma_{r,s} U_k^{\mu,\nu} \left(\sum_i a_{r,\mu,i}\binom{x}{r+\mu-i}\right)\left(\sum_j a_{s,\nu,j}\binom{y}{s+\nu-j}\right)\right] - \frac{k}{k+1}\binom{f(x,y)}{k}$$

où

$$a_{r,\mu,i} = \frac{(r+\mu-i)!}{i!(\mu-i)!(r-i)!} .$$

Une manipulation laborieuse, mais élémentaire, des indices en jeu ainsi que l'expression donnant les $\sigma_{r,s}$ conduit alors au résultat requis.

La deuxième décomposition en pits que nous allons donner a une saveur plus classique en ce sens qu'elle fait appel à une expression assez connue en théorie des nombres pour le symbole de Kronecker dans $\mathbb{F}_p$: Si $m \in \mathbb{F}_p$ et si x est une variable parcourant $\mathbb{F}_p$ alors

$$\delta_m^x \equiv \frac{x-x^p}{x-m} \equiv \sum_{i=0}^{p-1} \{^i_m\} x^i \in \mathbb{F}_p[x] \qquad (20)$$

où les $\{^i_m\}$ sont donnés par la matrice B mentionnée plus haut. On obtient immédiatement:

Théorème II (deuxième décomposition en pits). Si $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(z = f(x,y))$ et si p est un nombre premier alors pour tout $i \in \mathbb{N}$

$$z_i \equiv \sum_{m,n\geq 0} (f(m,n))_i \frac{x_0-x_0^p}{x_0-m_0} \cdot \frac{x_1-x_1^p}{x_1-m_1} \cdot \frac{x_2-x_2^p}{x_2-m_2} \cdots \frac{y_0-y_0^p}{y_0-n_0} \cdot \frac{y_1-y_1^p}{y_1-n_1} \cdot \frac{y_2-y_2^p}{y_2-n_2} \cdots \qquad (21)$$

où $(f(m,n))_i$ désigne le $i^{\text{ième}}$ pit du nombre $f(m,n)$.

Avant d'énoncer une troisième décomposition en pits *étendons* les symboles $\{^m_\mu\}$, $[^m_\mu]$ (préalablement définis pour $0 \leq m$, $\mu \leq p-1$ et à valeurs dans F_p) à

tous les naturels m, μ par

$$\left\{\begin{matrix} m \\ \mu \end{matrix}\right\} \equiv \left\{\begin{matrix} m_0 \\ \mu_0 \end{matrix}\right\} \left\{\begin{matrix} m_1 \\ \mu_1 \end{matrix}\right\} \left\{\begin{matrix} m_2 \\ \mu_2 \end{matrix}\right\} \ \ldots \in \mathbb{F}_p \tag{22}$$

$$\left[\begin{matrix} m \\ \mu \end{matrix}\right] \equiv \left[\begin{matrix} m_0 \\ \mu_0 \end{matrix}\right] \left[\begin{matrix} m_1 \\ \mu_1 \end{matrix}\right] \left[\begin{matrix} m_2 \\ \mu_2 \end{matrix}\right] \ \ldots \in \mathbb{F}_p \tag{23}$$

pour tous $m,\mu \in \mathbb{N}$. Ces définitions "forcent" ces nouveaux symboles à avoir une propriété analogue à celle des coefficients binomiaux du théorème de Lucas.

Théorème III (troisième décomposition en pits). Si $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(z = f(x,y))$ et si p est un nombre premier alors pour tous $i,m,n \in \mathbb{N}$, $\exists! \beta_{m,n}(i) \in \mathbb{F}_p$ tel que

$$z_i \equiv \sum_{m,n\geq 0} \beta_{m,n}(i)\ x_0^{m_0}\ x_1^{m_1}\ x_2^{m_2} \ \ldots\ y_0^{n_0}\ y_1^{n_1}\ y_2^{n_2} \ \ldots \tag{24}$$

De plus, chaque $\beta_{m,n}(i)$ peut s'écrire sous la forme

$$\beta_{m,n}(i) \equiv \sum_{\substack{0\leq\mu\leq m \\ 0\leq\nu\leq n}} \left\{\begin{matrix} m \\ \mu \end{matrix}\right\}\left\{\begin{matrix} n \\ \nu \end{matrix}\right\} \left(f(\mu,\nu)\right)_i \tag{25}$$

où $\left(f(\mu,\nu)\right)_i$ désigne le $i^{\text{ième}}$ pit du nombre $f(\mu,\nu)$.

Démonstration. On peut donner deux démonstrations de ce résultat. La première est assez immédiate. Elle fait appel à la formule (20) dans chacun des facteurs de chacun des termes de la somme (21) suivie d'un réarrangement de termes et d'une utilisation de (22). La deuxième est plus complexe et utilise un développement élaboré basé sur une analyse détaillée de la représentation binomiale du théorème I. Soulignons simplement qu'il est possible d'obtenir le sous-produit suivant la deuxième démonstration.

Les matrices A , B , C satisfont la congruence remarquable

$$C \equiv BA \pmod{p} . \tag{26}$$

Ce qui permet, par exemple, une vérification du calcul de ces trois matrices.

Si on définit les polynômes $\omega_m(x) \in \mathbb{F}_p[x]$ par

$$\omega_m(x) \equiv \sum_{\mu=0}^{p-1} \{{m \atop \mu}\} x^\mu , \quad 0 \le m \le p-1 \tag{27}$$

alors (25) et (22) permettent de conclure que pour tous $m,n \ge 0$

$$\beta_{m,n}(i) \equiv \omega_{m_0}(E_x)\omega_{m_1}(E_x^p)\omega_{m_2}(E_x^{p^2}) \ \dots \ \omega_{n_0}(E_y)\omega_{n_1}(E_y^p)\omega_{n_2}(E_y^{p^2}) \ \dots \ (f(0,0))_i \tag{28}$$

ce qui est un résultat similaire à (15).

La prochaine décomposition en pits fait cette fois appel directement à la matrice C. Elle fournira une écriture explicite des pits de la fonction "somme (ordinaire) des pits d'un nombre x". Plus précisément

Théorème IV. Si p est un nombre premier et si

$$z = x_0 + x_1 + x_2 + x_3 + \dots \quad \text{(somme ordinaire des pits de } x\text{)}$$

alors

$$z_i \equiv \sum_{m \ge 0} \gamma_m(i) \ x_0^{m_0} \ x_1^{m_1} \ x_2^{m_2} \ \dots \tag{33}$$

où les coefficients $\gamma_m(i) \in \mathbb{F}_p$ sont donnés explicitement par

$$\gamma_m(i) \equiv \sum_{\mu_0+\mu_1+\dots=p^i} [{m \atop \mu}] . \tag{34}$$

Démonstration. La formule combinatoire bien connue de Vandermonde qui se lit

$$\binom{a+b+c+\dots}{k} = \sum_{k_1+k_2+\dots=k} \binom{a}{k_1}\binom{b}{k_2}\binom{c}{k_3} \ \dots, k,a,b,c,\dots \ge 0 \tag{35}$$

donne

$$\binom{x_0+x_1+x_2+\dots}{k} = \sum_{\mu_0+\mu_1+\dots=k} \binom{x_0}{\mu_0}\binom{x_1}{\mu_1}\binom{x_2}{\mu_2} \ \dots \tag{36}$$

Comme, pour tous $i \ge 0$, $x_i \le p-1$ on obtient que (36) est congru à

$$\sum_{\mu_0+\mu_1\ldots=k}\left(\sum_{m_0=0}^{p-1}\frac{\$_{\mu_0}^{(m_0)}}{\mu_0!}x_0^{m_0}\right)\left(\sum_{m_1=0}^{p-1}\frac{\$_{\mu_1}^{(m_1)}}{\mu_1!}x_1^{m_1}\right)\ldots$$

$$\equiv \sum_{m\geq 0}\left(\sum_{\mu_0+\mu_1\ldots=k}\begin{bmatrix}m_0\\ \mu_0\end{bmatrix}\begin{bmatrix}m_1\\ \mu_1\end{bmatrix}\ldots\right)x_0^{m_0}\,x_1^{m_1}\,x_2^{m_2}\ldots$$

On conclue en posant $k = p^i$ et en utilisant (8) et (23) .

3. QUELQUES EXEMPLES

Dans le cas particulier des *bits* (i.e. $p = 2$) on a

$$A \equiv B \equiv \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$$

et les décompositions I et III se réduisent (compte tenu que $\binom{x_i}{m_i} \equiv x_i^{m_i}$ dans ce cas) à une seule et même formule

$$z_i \equiv \sum \alpha_{m,n}(i)\; x_0^{m_0}\,x_1^{m_1}\ldots y_0^{n_0}\,y_1^{n_1}\ldots \tag{37}$$

où

$$\alpha_{m,n}(i) \equiv \beta_{m,n}(i) \equiv \sum_{\substack{\mu.:m\\ \nu.:n}} (f(\mu,\nu))_i \tag{38}$$

Quant à la décomposition II elle devient

$$z_i \equiv \sum_{m,n\geq 0} (f(m,n))_i \prod_{m_j=1} x_j \prod_{m_j=0} (1+x_j) \prod_{n_j=1} y_j \prod_{n_j=0} (1+y_j) \tag{29}$$

comme on le vérifie directement.

Ces formules dégénérées sont donc, à quelques notations près, essentiellement les décompositions classiques décrites par P. Camion [2].

Pour le cas des pits la fonction "successeur" $z = x + 1$ se décompose comme suit

$$
\begin{aligned}
z_0 &\equiv x_0 + 1 \\
z_1 &\equiv x_1 - x_0^{(p-1)} \\
z_2 &\equiv x_2 + x_0^{(p-1)}\, x_1^{(p-1)} \\
&\vdots \\
z_i &\equiv x_i + (-1)^i\, x_0^{(p-1)}\, x_1^{(p-1)} \cdots x_{i-1}^{(p-1)} \\
&\vdots
\end{aligned}
\tag{30}
$$

Elle peut aussi être décrite par la récurrence

$$
z_i \equiv x_i + r_i \quad \text{où} \quad r_0 \equiv 1\,, \quad r_{i+1} \equiv -x_i^{(p-1)}\, r_i\,. \tag{31}
$$

La décomposition (30) se démontre par le même type d'argument qui donne la décomposition I. Plus précisément

$$
z_i \equiv \binom{x+1}{p}_i = \binom{x}{p}_i + \binom{x}{p}_{i-1} \equiv x_i + \binom{x_0}{p-1}\binom{x_1}{p-1}\binom{x_2}{p-1} \cdots \binom{x_{i-1}}{p-1}
$$

et il suffit ensuite d'appliquer le théorème bien connu de Wilson [6] qui dit que $(p-1)! \equiv -1 \pmod p$.

La fonction somme $z = x + y$ possède une structure évidemment beaucoup plus complexe. Remarquons d'abord que si x_i et y_i sont deux pits alors les formules de Wilson et de Vandermonde permettent d'écrire

$$
\begin{aligned}
\binom{x_i+y_j}{p} &\equiv -\frac{x_i^{(1)} y_j^{(p-1)}}{1} + \frac{x_i^{(2)} y_j^{(p-2)}}{2} - \frac{x_i^{(3)} y_j^{(p-3)}}{3} + \cdots + (-1)^{p-1} \frac{x_i^{(p-1)} y_j^{(1)}}{p-1} \qquad (32) \\
&\equiv (\text{polynôme de degré } p-1 \text{ en } x_i\,,\, y_j) \in F_p[x_i, y_j]\,.
\end{aligned}
$$

La somme se décompose alors selon le schéma

$$z_0 \equiv x_0 + y_0$$

$$z_1 \equiv x_1 + y_1 + \binom{x_0+y_0}{p}$$

$$z_2 \equiv x_2 + y_2 + \binom{x_1+y_1}{p} - \binom{x_0+y_0}{p}(x_1+y_1)^{(p-1)}$$

$$\vdots \qquad (39)$$

$$z_i \equiv \begin{cases} x_i + y_i + \binom{x_{i-1}+y_{i-1}}{p} - \binom{x_{i-2}+y_{i-2}}{p}(x_{i-1}+y_{i-1})^{(p-1)} \\ \\ + \ldots + (-1)^{i-1}\binom{x_0+y_0}{p}(x_1+y_1)^{(p-1)}(x_2+y_2)^{(p-1)} \ldots (x_{i-1}+y_{i-1})^{(p-1)} \end{cases}$$

$$\vdots$$

En effet, on a

$$z_r \equiv \binom{x+y}{p^r} = \sum_{a+b=p^r} \binom{x}{a}\binom{y}{b} \equiv x_r + y_r + \sum_{\substack{0<a,b<p^r \\ a+b=p^r}} \binom{x}{a}\binom{y}{b}$$

$$= x_r + y_r + f_r\,(x_0,x_1,\ldots,x_{r-1},y_0,y_1,\ldots,y_{r-1})$$

disons. Or

$$f_r = \sum_{i=1}^{r} \sum_{(a,b)\in E_i} \binom{x}{a}\binom{y}{b}$$

où

$$E_i = \{(a,b) \mid 0 < a < p^r\ ,\ 0 < b < p^r\ ,\ a+b = p^r\ ,\ a_0 = a_1 = \ldots = a_{i-2} = 0\ ,\ a_{i-1} \neq 0\}$$

$$= \{(a,b) \mid 0 < a < p^r\ ,\ 0 < b < p^r\ ,\ a+b = p^r\ ,\ b_0 = b_1 = \ldots = b_{i-2} = 0\ ,\ b_{i-1} \neq 0\}\ .$$

Si on définit alors

$$\Psi_i = \Psi_i\,(x_0,x_1,\ldots,x_{i-1},y_0,y_1,\ldots,y_{i-1})$$

$$= \sum_{(\alpha,\beta)\in F_i} \binom{x}{\alpha}\binom{y}{\beta}\ ,\quad i = 1,2,\ldots$$

avec

$$F_i = \{(\alpha,\beta) \mid 0 < \alpha < p^i \ , \ 0 < \beta < p^i \ , \ \alpha + \beta = p^i \ , \ \alpha_0 \neq 0 \neq \beta_0\}$$

$$= \{(\alpha,\beta) \mid \alpha_0 \neq 0 \neq \beta_0 \ , \ \alpha_0 + \beta_0 = p \ , \ \alpha_1 + \beta_1 = p-1, \ldots, \alpha_{i-1} + \beta_{i-1} = p-1\} \ ,$$

on vérifie alors sans peine que

$$f_r = \Psi_r + \Psi_{r-1} + \ldots + \Psi_1 \ . \tag{40}$$

On conclue en remarquant (via (7)) que

$$\Psi_i \equiv \sum_{(\alpha,\beta)\in F_i} \binom{x_0}{\alpha_0}\binom{x_1}{\alpha_1} \ldots \binom{x_{i-1}}{\alpha_{i-1}}\binom{y_0}{\beta_0}\binom{y_1}{\beta_1} \ldots \binom{y_{i-1}}{\beta_{i-1}}$$

$$\equiv \left(\sum_{\substack{\alpha_0+\beta_0=p \\ \alpha_0\neq 0\neq\beta_0}} \binom{x_0}{\alpha_0}\binom{y_0}{\beta_0} \right) \left(\sum_{\alpha_1+\beta_1=p-1} \binom{x_1}{\alpha_1}\binom{y_1}{\beta_1} \right) \ldots \left(\sum_{\alpha_{i-1}+\beta_{i-1}=p-1} \binom{x_{i-1}}{\alpha_{i-1}}\binom{y_{i-1}}{\beta_{i-1}} \right)$$

$$\equiv \binom{x_0+y_0}{p}\binom{x_1+y_1}{p-1} \ldots \binom{x_{i-1}+y_{i-1}}{p-1}$$

et en utilisant encore une fois le théorème de Wilson.

Incidemment (39) montre qu'on a ici la récurrence

$$z_i \equiv (x_i+y_i) + r_i \quad \text{où} \quad r_0 \equiv 0 \ , \quad r_{i+1} \equiv \binom{x_i+y_i}{p} - (x_i+y_i)^{(p-1)} \ r_i \ . \tag{40}$$

La fonction produit $z = xy$ peut évidemment se décomposer directement selon chacune des décompositions I , II ou III . Soulignons cependant que la décomposition I apparaît sous une forme purement combinatoire.

En effet, dans ce cas les nombres $U_k^{m,n}$ satisfont

$$\binom{xy}{k} = \sum_{m,n\geq 0} U_k^{m,n} \binom{x}{m}\binom{y}{n} \tag{42}$$

et on peut montrer, via la formule d'inversion de Möbius [3, 7] que $U_k^{m,n}$ est égal au nombre de parties à k éléments de $\{1,\ldots,m\} \times \{1,\ldots,n\}$ et qui sont *saturées*. Une partie $S \subseteq \{1,\ldots,m\} \times \{1,\ldots,n\}$ étant déclarée saturée si ses deux projections recouvrent complètement les "axes" $\{1,\ldots,m\}$ et $\{1,\ldots,n\}$.

De plus, la théorie des nombres de Stirling (ou encore, comme me l'a souligné verbalement Pierre Leroux, celle de l'inversion de Möbius) permet de montrer que ces $U_k^{m,n}$ ont aussi (en plus de (13)) la forme

$$U_k^{m,n} = \frac{m!n!}{k!} \sum_{\sigma=0}^{k} \$_k^{(\sigma)} \$_\sigma^{(m)} \$_\sigma^{(n)} \quad . \tag{43}$$

Quant au théorème R il produit ici la récurrence à 4 termes

$$U_0^{m,n} = \delta_0^m \, \delta_0^n \ ,$$

$$U_{k+1}^{m,n} = \frac{1}{k+1} \{(mn-k)U_k^{m,n} + mn\, U_k^{m-1,n} + mn\, U_k^{m,n-1} + mn\, U_k^{m-1,n-1}\} \ , \tag{44}$$

qui peut aussi se démontrer combinatoirement et qui rend plus aisé le calcul de ces nombres.

L'algorithme usuel de multiplication (en base p) permet une autre approche pour la décomposition en pits du produit de deux nombres naturels. Il la ramène, comme on peut s'en convaincre facilement, à une construction récursive faisant appel aux produits (plus simples) de deux pits et à la somme d'un nombre quelconque de pits. Cette somme s'évalue directement à l'aide du théorème IV et se ramène, dans le cas particulier des *bits*, à

$$z_0 \equiv x_0 + x_1 + x_2 + \ldots$$

$$z_i \equiv x_0x_1 + x_0x_2 + \ldots + x_ix_j + \ldots$$

$$z_2 \equiv x_0x_1x_2x_3 + \ldots + x_ix_jx_rx_s + \ldots$$

$$\vdots$$

$z_i \equiv$ somme des produits des bits de x pris 2^i à la fois.

$$\vdots$$

En effet, on vérifie directement à l'aide de la matrice C (qui a ici la forme $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$) que pour chaque m , i la somme

$$\gamma_m(i) \equiv \sum_{\mu_0+\mu_1+\ldots=2^i} \begin{bmatrix} m_0 \\ \mu_0 \end{bmatrix} \begin{bmatrix} m_1 \\ \mu_1 \end{bmatrix} \ldots$$

est nulle sauf dans le cas où m possède exactement 2^i bits non nuls (où elle vaut alors 1).

La formule (45) a été obtenue par Camion [2] à l'aide d'un procédé plus long et complètement différent.

Soulignons pour terminer que chaque fonction (e.g. y^x , $x!$, x^2 , ... etc.) possède une théorie particulière en regard des diverses formules développées dans le présent texte.

La fonction "monôme" $z = f(x,y,\ldots) = ax^r y^s \ldots$, par exemple, est intimement reliée au développement binomial

$$\binom{ax^r y^s \ldots}{k} = \sum_{\substack{0\le m\le kr \\ 0\le n\le ks \\ \cdot \\ \cdot \\ \cdot}} U_k^{m,n,\ldots} \binom{x}{m}\binom{y}{n} \ldots \qquad (46)$$

où les

$$U_k^{m,n,\ldots} = \frac{m!n!\ldots}{k!} \sum_{\sigma=0}^{k} a^\sigma \, \$_k^{(\sigma)} \, \$_{r\sigma}^{(m)} \, \$_{s\sigma}^{(n)} \ldots \qquad (47)$$

satisfont une récurrence (sur k) possédant $(r+1)(s+1)\ldots$ termes et peuvent aussi être interprétés combinatoirement via les parties saturées d'un pavé discret.

REMERCIEMENT

L'auteur désire remercier M. André Joyal pour lui avoir souligné les possibilités potentielles contenues dans la formule (8) découlant du théorème de E. Lucas.

RÉFÉRENCES

[1] Abramowitz, M., Stegun, I.A., Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables, National Bureau of Standards, Applied Mathema-

tics Series 55, U.S. Department of Commerce (1964).

[2] Camion, P., Une méthode de résolution par l'algèbre de Boole des problèmes combinatoires où interviennent des entiers, Cahier centre d'études rech. opér. 2 (1960), 234-289.

[3] Carlo-Rota, G.C., On the Foundations of Combinatorial Theory, I: Theory of Möbius Functions, Z. Wahrscheinlichkeitstheorie 2 (1964), 340-368.

[4] Fine, N.J., Binomial coefficients modulo a prime, Amer. Math. Monthly 54 (1947), 589-592.

[5] Guelfond, A.O., Calcul des différences finies, Coll. Univ. de mathématiques, Vol. 12, Dunod, Paris (1963).

[6] Hardy, G.H., Wright, E.M., An Introduction to the Theory of Numbers, Oxford Univ. Press, Fourth Edition (1960).

[7] Leroux, P., Les catégories de Möbius, Rapport 2^{e} colloque sur l'algèbre des catégories, Amiens (1975).

[8] Lucas, E., Sur les congruences des nombres eulériens et des coefficients différentiels, Bull. Soc. Math. de France, 6 (1878), 49-54.

[9] Rosenberg, I., Minimization of pseudo-boolean functions by binary development, Discrete Math. 7 (1974), 151-165.

[10] Rosenberg, I., Characteristic polynomials in GF(2) of zero-one inequalities and equations, Utilitas Mathematica, Vol. 7 (1975), 323-343.

Département de mathématiques
Université du Québec à Montréal
C.P. 888, Succ. A
Montréal, Québec
H3C 3P8

Manuscrit reçu le 1er septembre 1977.