Les séries de Poincaré pour les codes

V.E. Govorov

Institut des Machines Électroniques
B. Vousovski 3/12
Moscou
Russie

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
53225 Bonn
Germany

MPI / 93-73

Les series de Poincaré pour les codes

V.E.Govorov

Codes

Soit Z un ensemble de lettres, que nous nommerons *alphabet*. On note la longueur d'un mot z en *alphabet* Z par $|z|$. Nous noterons composé des mots a et b par ab et le composé $uu...u$ par u^n. Un mot u est appelé *préfixe* d'un mot v, s'il existe un mot w tel que $v = uw$.Un mot *appartient* à un autre mot v s'il existe les mots u_1 et u_2 tel que $w = u_1 v u_2$.

On dit que les mots u et u *se recouvrent* si la fin de u est le commencement de v, c'est-à-dire $u = ab, v = bc$.

On regarde ici un schema de la codification alphabétique, c'est-à-dire on regarde l'alphabet $Y = \{y_1, ..., y_n\}$ et à chaque symbole y_i on fait correspondre un mot v_i dans un autre alphabet $Z = \{z_1, \ldots, z_m\}$ et à chaque mot $z_{i1} z_{i2} ... z_{ik}$ correspond un mot $v_{i1} v_{i2} ... v_{ik}$ dans Z. Les mots $v_1, \ldots, v_n$ sont appelés *un code de la communication.*

Nous regarderons les classes suivant des dictionnaires:

1. Dictionnaire $uniforme$ avec les mots de longueur égales.

2. Dictionnaire à *préfix.* C'est un dictionnaire Z tel que aucun mot v_i n'est le commencemant d'un autre mot v_j de Z.

3. Dictionnaire *sans virgule.* C'est un dictionnaire dans lequel aucun mot v_i n'appartient à l'union des mot $v_k v_l$.

4. Dictionnaire *sans recoupement.* C'est un dictionnaire dans lequel toute paire de mots est sans des recoupements.

5. Dictionnaire *avec un préfixe synchronisant* .C'est un dictionnaire dans lequel chaque mot commence par le mot a et tel que le mot a n'est pas une partie propre du mot $av_i a$.

Algèbres

Soit k un corps, F un álgèbre associative libre avec une unité,engendrée par les éléments de l'alphabet Z. Les codes élémentaires engendrent un ideal P de l'algèbre F.Les éléments de l'alphabet Z engendrent un idéal I. On a $R = F/P$.

Les groupes d'homologie [1] de l'algèbre R sont les k-espaces vectoriels $H_n = H_n(R, k) = Tor_n^R(k, k)$.

La série de Poincaré (Hilbert) ([2],[4]) d'un espace vectoriel gradé $A = \Sigma_{i=0}^{\infty} A_i$ est la série $T(A) = \Sigma_{i=0}^{\infty} d_i t^i$, où $d_i = dim_k A_i$.

Toutes les démonstrations des proprietes suivantes peuvent se trouver dans [4],[5].

0.1 Pour deux espaces gradés A et B on a $T(A + B) = T(A) + T(B) - T(A \cap B)$.

0.2 Pour deux idéaux homogènes gradés A et B de l'algèbre libre F on a $T(AB) = = T(A)T(B)(1 - st)^{-1}$.

0.3 Pour l'algèbre libre F, $T(F) = (1 - st)^{-1}$.

0.4 Pour un idéal A de l'algèbre libre F, $T(AI) = T(IA) = T(A)st$.

0.5 Pour l'idéal I de l'algèbre F , $T(I) = st(1-st)^{-1}$

0.6 Pour toute suite exacte $0 \to A \to B \to C \to 0$ avec des morphismes de degré 0 on a $T(B) = T(A) + T(C)$.

0.7 En particulier, pour $0 \to P \to F \to R \to 0$ on a $T(R) = (1-st)^{-1} - T(P)$.

0.8 Pour deux espaces vectoriels A et B , $T(A \otimes B) = T(A)T(B)$.

0.9

$$H_{2l} = P^l \cap IP^{l-1}I/P^lI + IP^l$$

$$H_{2l+1} = P^l l \cap IP^l/P^{l+1} + IP^l$$

0.10 En particuilier

$$H_0 = k$$

$$H_1 = I/I^2$$

$$H_2 = P/PI + IP$$

$$H_3 = PI \cap IP/P^2 + IPI$$

0.11 On en déduit

$$T(H_0) = k$$

$$T(H_1) = st$$

$$T(H_2) = \Sigma t^{v_i}$$

0.12 $T(R) = (\Sigma(-1)^i T(Tor_i^R(k,k)))^{-1}$

On définit une relation entre les séries formelles : $\Sigma c_n \leq \Sigma d_n$ si pour tout n on a $c_n \leq d_n$

0.13 $T(R)(1 - st + T(H_2)) \geq 1$

La démonstration de cette proposition se trouve dans [2] théorème 8.

0.14 Le rayon r de la convergence de la série $T(R)$ est limité par $s^{-1} \leq r \leq 1$. Si $F \neq R$ on a $s^{-1} < r$.

Lemme 0.15 *Il existe un homomorpisme de degreé 0*

$$H_n \to H_{n-1} \otimes I/P \tag{1}$$

Preuve.- Soit $N = 2l+1$, et $u \in P^lI \cap IP^l \setminus P^{l-1} + IP^lI$ (d'après 0.9).Soit $v_1, v_2, ..., v_m$ un système génératrice de P. Le mot u est presenté sous forme $u = v_i a = bw$, où $a \in P^{l-1}$, $b \in I \setminus P$, $w \in P^l \setminus IP^l$. Si $|b| \geq |v_i|$ alors $v_i = bd$, $u = bda = bv$, d'où $u = da = w \in IP^{l-1}I \cap P^l$.

Montrons que l'image de u dans H_{2l} n'est pas 0. En effet,si $u_1 \in P^lI + IP^l$ alors $u_1 \in IP^l$ ou $u_1 \in P^lI$.

Si $u_1 \in IP^l$, on a $w = u_1 \in IP^l$ ce qui n'est pas possible d'après le choix de w.

Si $u_1 \in P^l$, on a $u = bu_1 \in IP^lI$, ce qui n'est pas posible d'après le choix de u.

Les classes $U = u_1 + P^l I + IP^l$,$B = b + P$ et le correspondance $u \to b \otimes U$ définissent l'homomorphisme (1). La démonstration pour $n = 2l$ est analogue.

Corollaire 0.16 *Si* $H_n = 0$ *alors* $H_m = 0$ *pour tout* $m \geq n$.

On note $v(f)$ la valuation de la série formelle. D'après lemme 0.15 on a

0.17 $v(T(H_i)) < v(T(H_j))$ $i < j$.

Les résultats

Lemme 1. $T(P^2/P^2 \cap IPI) = (1-st)^2 T(R) - (1 - st - T(H_2) + T(H_3))$.

Preuve.- En utilisant 0.1, 0.2, 0.4 et 0.9 on a

$T(P^2/P^2 \cap IPI) = T(P^2) - T(P^2 \cap IPI/P^2 I + IP^2) -$

$-T(P^2 I) - T(IP^2) + T(P^2 I \cap IP^2 I/P^3 + IP^2 I) +$

$+T(P^3) + T(IP^2 I) - T(P^3 \cap IP^2 I/P^3 I + IP^3) -$

$-T(P^3 I) + T(IP^3) - T(P^3 I \cap IP^3/P^4 + IP^3 I) + ... =$

$= T(P^2) - 2stT(P^3) + T(P^3) + s^2 t^2 T(P^2) -$

$-2stT(P^2) - 2stT(P^4) + s^2 t^2 T(P^3) - ... -$

$-T(H_4) + T(H_5) - T(H_6) + ... =$

$= (T(P^2) + T(P^3) + T(P^4) + ...)(1-st)^2 - T(H_4) + T(H_5) - T(H_6) + ... =$

$= T^2(P)(1-st) + T^3(P)(1-st)^2 + T^4(P)(1-st)^3 + ...)(1-st)^2 -$

$-T(H_4) + T(H_5) - T(H_6) + ... =$

$= ((1-st)^2 T(P)^2)/((1-st)^{-1} - T(P)) - 1 + st - T(H_2) + T(H_3) -$

$-T(H_4) + T(H_5) - T(H_6) + ... + 1 - st + T(H_2) - T(H_3)$

La substitution de 0.7 et 0.12 donne

$T(P^2/P^2 \cap IPI) = ((1-st)^2 T^2(P))/T(R) - (1/T(R)) +$

$+1 - st + T(H_2) - T(H_3) =$

$= ((1-st)^2 (T^2(P) - (1-st)^{-2}))T^{-1}(R) + 1 - st + T(H_2) - T(H_3) =$

$= (1-st)^2((1-st)^{-1} + T(P)) + 1 - st + T(H_2) - T(H_3) =$

$= -(1-st)^2 T(P) + T(H_2) - T(H_3) =$

$= -(1-st)^3((1-st)^{-1} - t(R)) + T(H_2) - T(H_3) =$

$= T(R)(1-st)^2 - (1 - st + T(H_2) - T(H_3))$.

Lemme 2. *Soit* Z *un dictionnaire uniforme de degreé* r, *alors* $deg(1 - st + T(H_2) - T(H_3)) < 2r$.

Preuve.- D'après 0.11 on a $deg(T(H_2)) = r$. Si $deg(T(H_3)) \geq 2r$ il existe un mot $w \in PI \cap IP \setminus P^2 + IPI$ (voir 0.10) $deg(w) \geq 2r$. Dans ce cas $w = v_i a = bv_j$, où $v_i, v_j \in V, a, b \in I$, mais $deg(v_i) = r$,donc $deg(a) \geq r$ et $a = cv_j$. La substitution de u dans w donne $w = v_i c v_j \in P^2$ ce qui n'est pas possible

Corollaire. *La fonction des coefficients de la serie de Poincaré* $f(n) = d_n s^{-n}$ *est une fonction "convexe" pour* $n > 2r$.

Preuve.- D'après le lemme 2 pour $n \geq 2r$ les coefficients de la série $(1-st)^2 T(R)$ ne sont pas negatif,parce qu'ils sont les coefficients de la serie $T(P^2/P^2 \cap IPI)$.L'inegalité $(1-st)^2 T(R) \geq 0$ est équivalent a un système d'inegalités

$d_n - 2sd_{n-1} + s^2 d_{n-2} \geq 0$, ou
$d_n s^{-n} - 2d_{n-1}s^{-(n-1)} + d_{n-2}s^{-n-2} \geq 0$
L'égalité est possible seulement pour $P = 0$ ou $P = I^2$.

Lemme 3. *Soit V un dictionnaire uniforme de degré r et de longueur m. Les termes initiaux de $T(R)$ sont les suivantes:*

$T(R) = 1 + st + s^2t^2 + ... + s^{r-1}t^{r-1} + (s^r - m)t^r + ...$

Preuve.- D'après 0.11 et 0.12 $T(R) = (1 - st + mT^r + ...)^{-1}$. La division achève la démonstration.

Théorème 1. *Pour un idéal P de l'algèbre libre F,engendré par un système réduit fini de mots les conditions suivantes sont équivalentes:*

1. *Un système de générateurs de P est un dictionnaire sans recoupements.*
2. $H_3(R, k) = 0$.
3. $PI \cap IP = P^2 + IPI$
4. $T(P^2/P^2 \cap IPI) = T^2(H_2)T(R)$
5. $T(R) = (1 - st + T(H_2))^{-1}$

Preuve.- $1 \Rightarrow 3$ .Soit u un mot de $PI \cap IP \setminus IPI$. Alors $u = v_i a = bv_j$,$v_i, v_j \in V$. Si $|a| < |v_j|$ on a $v_j = ca$, $v_i = bc$, mais c'est un recoupement, ce qui contredit hypothèse faite sur P. Si $|a| \geq |v_j|$ on a $a = cv_j$ et $u = v_i c v_j \in P^2$. On a demontré que $PI \cap IP \subset P^2 + IPI$. L'inclusion réciproque est évidente.

$3 \Rightarrow 1$. Par hypothèse$PI \cap IP = P^2 + IPI$. Soit v_i et v_j deux mot du dictionnaire V avec un recoupement maximal, c'est-à-dire $v_i = ab$, $v_j = bc$ et la longueur du mot abc est le plus petit possible.Alors $abc \in PI \cap IP = P^2 + IPI$. Si $abc \in P^2$ on a $abc = v_i c = pv_k q v_l r$, où $v_k, v_l \in V$.Attendu que $c \notin P$ la réduction à c donne $v_i = pv_k z$,ce que contredit a le fait que le système des générateurs de P est réduit. Si $abc \in IPI, v_i c = pv_k q, v_k \in V, p, q \in I$ il y a deux possibilités:

a)$|c| \leq |q|$. La reduction à c donne la contradiction avec le fait que le système des générateurs est réduit.

b)$|c| > |q|$. Aprés la réduction à q on a un recoupement des mot v_i et v_k plus grand que celui de v_i et v_j : $v_i c' = pv_k$. En effet $|v_i c'| = |v_i c| - |q| = |abc| - |q| < |abc|$. Donc le dictionnaire V est sans recoupement.

$2 \Leftrightarrow 3$. Voir 0.10.

$2 \Rightarrow 5$. Si $H_3 = 0$, alors d'après 0.16 pour tout $i \geq 3$ $H_i = 0$ et 5 résulte de 0.11 et 0.12.

$5 \Rightarrow 2$. D'après 5 et 0.12 on a $T(H_0) - T(H_1) + T(H_2) - T(H_3) + ... = T(H_0) - T(H_1) + Y(H_2)$. Donc $-T(H_3) + T(H_4) - T(H_5) + ... = 0$. D'après 0.17 c'est possible seulement dans le cas : $H_3 = H_4 = ... = 0$

$5 \Rightarrow 4$. La substitution de $T(R)$ dans le lemme 1 donne
$T(P^2/P^2 \cap IPI) = (1 - st)^2/(1 - st + T(H_2)) - (1 - st - T(H_2)) =$
$((1 - st)^2 - (1 - st)^2 + T^2(H_2))/(1 - st + T(H_3)) = T^2(H_2)T(R)$.

$4 \Rightarrow 1$. Définissons un homomorphisme d'espaces véctoriels:

$$\phi : H_2 \otimes R \otimes H_2 \rightarrow P^2/P^2 \cap IPI$$

par $\phi(v_i \otimes r + P \otimes v_j) = v_i r v_j + IPI$ où $r \in F \setminus P, v_i, v_j \in V$. Cette définition est correcte parce que $v_i P v_j \subset P^3 \subset IPI$. L'homomorphisme ϕ est surjectif puisque tout élément de P^2 n'est pas d'espèce $v_i r v_j$ appartient à $P^2 I + IP^2 \subset IPI$. D'après 0.3 on a $T(H_2 \otimes R \otimes H_2) = T^2(H_2)T(R)$ et d'après l'hypothèse $T(H_2 \otimes R \otimes H_2) = T(P^2/P^2 \cap IPI)$. Donc ϕ est un isomorphisme. Suposons qu'il existe un recoupement des mots v_i et v_j, c'est-à-dire $v_i = ab, v_j = bc, |b| > 0$. Alors $\phi(ab \otimes c + P \otimes ab) = abcab + IPI = av_i v_j + IPI \subset IP^2 + IPI \subset IPI$. Donc le noyaux de $\phi \neq 0$ ce qui n'est pas possible. Par conséquent le dictionnaire V est un sans recoupement.

Théorème 2. *Pour un idéal P d'algèbre libre F,engendré par un dictionnaire V uniforme de degré r et de longueur m les conditions suivantes sont équivalentes:*

1.*Le dictionnaire V est sans virgule.*

2. $v(H_4) > 2r$.

3. $v(P^2 \cap IPI/P^2 I + IP^2) > 2r$

4. *Le coefficient de t^{2r} dans la serie $T(P^2/P^2 \cap IPI)$ est m^2.*

5. $d_{2r} - 2sd_{2r-1} + s^2 d_{2r-2} = (s^2 - d_r)^2$.

Preuve.- 1 $\Rightarrow$ 3 .Soit $w \in P^2 \cap IPI/P^2 + IP^2$ un élément de valuation $\leq 2r$. Les générateurs sont de degré r, donc $v(w) = 2r$. Dans ce cas on a des relations: $w = v_i v_j = av_k b$, où $v_i, v_j, v_k \in V, a, b \in I$. Il en résulte que le dictionaire V n'est pas sans virgules.

3 $\Rightarrow$ 1 . Suposons que V n'est pas un dictionaire sans virgules. Dans ce cas il existe du mots $v_i, v_j, v_k \in V, a, b \in I$, tels que $w = v_i v_j = av_k b \in P^2 \cap IPI$. Le mot w n'appartient pas à $P^2 I + IP^2$ parce que la longueur $|w|$ de w est $2r$ et tous les mots de $P^2 I + IP^2$ ont une longueur supérieure à $2r$. Il en resulte que l'espace vectoriel $P^2 \cap IPI/P^2 I + IP^2$ possède des éléments de valuation $2r$.

3 $\Leftrightarrow$ 2. Voir 0.10.L'isomorphisme 0.10 fait de V une base de l'espase vectoriel $H_2 = P/PI + IP$. En utilisant ce isomorphisme définissons un homomorphisme d'espaces véctoriels:

$$\phi : H_2 \otimes H_2 \to P^2/P^2 \cap IPI$$

où $\phi(v_i \otimes v_j) = v_i v_j + IPI$.

Compte-tenu de la présentation des éléments de P^2 de degré $2r$ sous la form $v_i v_j$, ϕ est surjective.

4 $\Rightarrow$ 1 . D'après 0.8 on a $T(H_2 \otimes H_2) = T^2(H_2) = m^2$ Par hypothèse on a $T((P^2/P^2 \cap IPI)_{2r}) = m^2 = T(H_2 \otimes H_2)$, et ϕ est un isomorphisme en degrè $2r$. Si le dictionnaire V n'est pas sans virgules, il existe des mots $v_i, v_j, v_k \in V, a, b \in I$ tels que $v_i v_j = av_k b$. Mais dans ce cas $\phi(v_i \otimes v_j) = v_i v_j + IPI = av_k b + IPI \subset IPI$. Alors $ker\phi \neq 0$ et ϕ n'est pas un isomorphisme.

1 $\Rightarrow$ 4. Si $T((P^2/P^2 \cap IPI)_{2r}) < m^2 t^{2r} = T(H_2 \otimes H_2)$, il existe des mots $v_i, v_j \in V$ tels que $\phi(v_i \otimes v_j) = 0$, c'est-à-dire $v_i v_j \in P^2 \cap IPI$. Donc $v_i v_j = av_k b$ et V n'est pas un dictionnaire sans virgules.

4 $\Leftrightarrow$ 5. Compte-tenu du lemme 3 on a $d_r = s^r - m$, d'où $m^2 = (s^r - d_r)^2$. Il suffit de prouver que les coefficients des séries $T(P^2/P^2 \cap IPI)$ et $T(R)(1-st)^2$ sont égaux. D'apès lemme 1

$T(P^2/P^2 \cap IPI) = T(R)(1-st)^2 - (1 - st - T(H_2) + t(H_3))$

D'après le lemme 1 les derniers termes de cette relation ont des degrès supérieurs à $2r$, donc $T(P^2/P^2 \cap IPI)_{2r} = (T(R)(1-st)^2)_{2r}$.

Théorème 3. *Soit a un mot de longueur p et V un dictionnaire maximal avec le préfixe synchronisant a , forme de mots de longueuer $p+q$. Soit P l'idéal engendré par a. Alors le nombre des codes du dictionnaire V est egal au coefficient c_r de la série $T(R)(1-st)^2t^{-p}$ où $R = F/P$.*

Preuve.- Considérons les mots $w = aza$ tels que a n'appartient pas à l'intérieur de w. Ces mots engendrent l'espace $P^2/P^2 \cap IPI$, dont la série de Poincaré etait calculé au lemme 1. Soit W le dictionnaire intermèdiaire $W = \{ava \in P^2 \setminus P^2 \cap IPI\}$. Compte-tenu du lemme 2 le cardinal0 de l'ensemble des mots de W de la longueur $2p+q$ est égale au coeffcient à c_{2p+q} de la série $T(R)(1-st)^2$.

On peut definir le dictionnaire V de la façon suivante $V = \{av|ava \in W\}$, c'est-à-dire le cardinal de l'ensemble des mots de longueur $2p+q$ de W est egale au cardinal des mots de longueur $p+q$ de V.

Matrices

Soit F un algèbre libre sur un corps k, engendrée par les éléments d'un alphabet $Z = \{x_1, ..., x_s\}$. Soit P un ideal de F engendré par les codes élémentaires. Dans ce qui suit nous supposons que V est un dictionnaire uniforme de degré r. Soit $M = \{u_1, u_2, ..., u_l\}$ l'ensemble de mots de longueur $r-1$, et $l = s^{r-1}$. Designons par $M_n(u_i)$ l'ensemble des mots de longueur $n \geq l$, n'appartenant pas á l'ideál P avec le début u_i. Soit q_{ni} le nombre des éléments de l'ensemble $M_n(u_i)$. Alors les coefficient de la série de Poincaré $T(R)$ s'acrirent de la façon suivante:

$$d_n = \Sigma_{i=1}^{l} q_{ni} \tag{2}$$

Chacun produit $x_j M(u_k)$ appartient a l'ideál P (si $x_j u_k \in P$) ou á un des ensembles $M_{n+1}(u_k)$ (si $x_j u_k = u_i x_l \notin P$), donc

$$M_{n+1}(u_k) = \bigcup_{i \in T_j} x_i M_n(u_i) \tag{3}$$

où $T_j = \{i|u_j x_p = x_k u_i \notin P\}$. Comme les ensembles $x_k H_n(u_i)$ sont dèsjoints si les u_i sont distincts on a

$$q_{n+1,j} = \Sigma_{i \in T_j} q_{ni}$$

ou

$$q_{n+1,j} = \Sigma \lambda_{ij} q_{ni} \tag{4}$$

où $\lambda_{ij} = 1$ si $i \in T_j$ et $\lambda_{ij} = 0$ si $i \notin T_j$

Designons par A une matrice avec les éléments λ_{ij} et $X_n^T = \{q_{n1}, q_{n2}, ..., q_{nl}\}$ alors

$$X_{n+1}^T = X_n^T A \tag{5}$$

Designons par e^T le vecteur $(1, 1, ..., 1)$, alors (2) s'écrit

$$d_n = X_n^T A e$$

et en vertu de (5) on a

$$d_{n+i} = X_n^T A^{i+1} e$$

ou, comme $X_{r+1}^T = e^T$ on a

$$\left.\begin{aligned} d_r &= e^T A e \\ d_{r+1} &= e^T A^2 e \\ &\cdots \\ d_n &= e^T A^{n-r+1} e \end{aligned}\right\} \tag{6}$$

Soit $||A||$ le norme de la matrice A defini par $||A|| = \Sigma|a_{ij}|$. En utilisant cette notation déduit de (6) les relations suivantes:

$$\begin{aligned} d_r &= ||A|| \\ d_{r+1} &= ||A^2|| \\ &\cdots \\ d_n &= ||A^{n-r+1}|| \end{aligned}$$

Il en résulte

$$T(R) = 1 + st + ... + s^{r-1}t^{r-1} + \Sigma_{i=r}^{\infty}||A^{i-r+1}||t^i.$$

Comme $||A + B|| = ||A|| + ||B||$ pour les matrices non négatives,on a

$T(R) = 1 + st + ... + s^{r-2}t^{r-2} + ||E||t^{r-1} + \Sigma_{i=r}^{\infty}||A^{i-r+1}||t^i = 1 + st + ... + s^{r-2}t^{r-2} + ||(E - tA)^{-1}||t^{r-1} = (1 - s^{r-1}t^{r-1})/(1 - st) + ||(E - tA)^{-1}||t^{r-1}$.

Maintenant on peut construire la matrice A de la manière suivante. Indexons les lignes et les colonnes par les mots $u_1, u_2, ..., u_l$ de longuer $r - 1$. On met 1 à l'intersection de la $i-$éme ligne et de la $j-$éme colonne s'il existent des lettres de l'alphabet Z tels qu'on ait la relation $x_p u_j = u_i x_q$ et tel que cet élément n'appartienne pas au dictionnaire V. Les autres élćoefficint de A sont 0.

Example. Soit Z l'alphabet consistant des deux lettres a et b et V un dictionnaire consistant des trois mots a^3, a^2b, ab^2. Alors

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Pour un dictionnaire vide on a

$$Q = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Dans ce qui suit nous désignons par Q la matrice corespondante au code vide.Un matrice A est obtenue ce forme de Q en remplacant 1 par 0 pour les i et les j que $x_p u_j = u_i x_q \in P$.

Pour les dictionnaires de degré 2 la matrice Q a l'ordre s avec $q_{ij} = 1$ pour tout i et j.

Pour les relations de degré 3 on a

$$Q = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 1 & 1 & \dots & 1 \end{pmatrix}$$

On verifie immédiatement que $Q_3^2 = Z$,où Z est une matrice dont tous les éléments sont 1.

Les propriétés suivantes sont des conséquences immédiates de la définition de la matrice Q:

$$Q^{r-1} = Z \tag{8}$$

$$Q^{r-1+i} = s^i Z \tag{9}$$

$$Qe = se, e^T Q = se^T \tag{10}$$

$$e^T Q e = s^r \tag{11}$$

oú $e^T = (1, 1, ..., 1)$

Pour des matrices C et D avec les éléments non negatifss on a:

$$||QC|| = ||CQ|| = s||C|| \tag{13}$$

$||CZD|| = ||C||||D||$

Dans ce qui suit nous utiliserons une matrice $X = Q - A$, dont les éléments sont aussi 0 ou 1.

Théorème 4. *Pour un idéal P de l'algèbre libre F, engendré par un dictionnaire V uniforme de degré r et de longueur m les conditions suivantes sont équivalentes:*

1.*Le dictionnaire V est sans virgule.*

2. *La matrice $X = Q - A$ vérifie les relations suivantes : $XQ^iXQ^jX = 0, i+j = r-2$.*

3.*La matrice $X = Q - A$ vérifie la relation suivante : $X((Q - X)^{r-1} - Q^{r-1})X = 0$.*

Preuve.- 1 $\Longleftrightarrow$ 3. La relation 5 du téorème 2 peut s'écrire de la maniere suivante:

$$e^T(A^{2r-r+1} - 2sA^r + s^2A^{r-1})e = (s^r - d_r)^2 \tag{15}$$

En vertu de (11),(6),(12) on a $(s^r - d_r)^2 = (e^TQe - e^TAe)(e^tQe - e^TAe) = = e^T(Q - A)ee^T(Q - A)e = e^T(Q - A)Z(Q - A)e$

La partie gauche de (15) d'après (10) est $e^T(A^{r-1}(A-sE)^r)e = e^T(A-sE)A^{r-1}(A-sE)e = e^T(A-Q)A^{r-1}(A-Q)e$

La comparaison des deux expressions obtenus donne

$$e^T(Q-A)(Z-A^{r-1})(Q-A)e = 0$$

ou

$$e^T X(Q^{r-1} - (Q-X)^{r-1})Xe = 0 \tag{16}$$

Avec $Q > Q-X$,on a $Q^r > (Q-X)^r$ et $Q^{r-1} - (Q-X)^{r-1} \geq 0$.

Toutes les matrices de l'expression (16) n'ont pas des coefficient negatifs, donc (16) est équivalent á la condition 3 du théorème.

$2 \implies 3$. Comme $Q \geq X$ la relation

$$XQ^iXQ^jX = 0, i+j = r-2 \tag{17}$$

on voit qu'en remplaçant Q par X dans (17) on obtient zero. Comme la matrice $(Q-X)^{r-1} - Q^{r-1}$ est formé de produits de cette sort, elle est nulle.

$3 \implies 2$. Comme $Q \geq Q-X$,il en resulte
$Q^i(Q-X)Q^j \geq (Q-X)^{r-1}, i+j = r-2$.
D'où
$0 < X(Q^{r-1} - Q^i(Q-X)Q^j)X \leq X(Q^{r-1} - (Q-X)^{r-1})X$
Par hypothèse la partie gauche de cette relation est 0, donc $0 = X(Q^{r-1} - Q^i(Q-X)Q^j)X = X(Q^i(Q-Q+X)Q^j)X = QX^iQX^JX$

Théorème 5. *Pour un idéal P de l'algèbre libre F, engendré par un système reduit fini de mots, les conditions suivantes sont équivalentes:*

1. *Un système de générateurs de P est un dictionnaire sans recoupement.*
2. *La matrice $X = Q - A$, corespondant á l'algèbre $R = F/P$ vérifie les conditions $XQ^iX = 0, i = 0, 1, ...r-1$.*
3. *La matrice $X = Q - A$ vérifie les conditions: $X(Q^i - (Q-X)^i) = 0, i = 1, 2, ...r-1$*

Preuve. - $1 \iff 3$. Dans ce cas on a $T(H_2) = mt^r$ (voir (0.10)), et la condition 5 du théorème 1 peut s'écrire de la maniere suivante:

$T(R) = (1 - st + mt^r)^{-1}$.

Pour les coefficients de la série $T(R)$ cela signifie

$$d_n - sd_{n-1} + md_{n-r} = 0 \tag{18}$$

Les coefficients d_n et m on peuvent s'écrire de la maniere suivante;

$d_n = s^n$ pour $n \leq r-1$
$d_n = e^T A^{n-r+1} e$ pour $n < r-1$
$m = e^T(Q-A)e = e^T Xe$ (d'après (6)).

Considérons trois cas :

a) $n \leq r-1$. Les relations (18) se transforment en $d_n = sd_{n-1}$.

b) $r \leq n \leq 2r-1$. Soit $i = n-r$ alors les relations (18) ont la forme $e^T(A^{n-r+1} - QA^{n-r})e = -e^T Xes^i$. En remplaçant $Q-A$ par X et s^ie par Q^ie et en utilisant (10)

on a $e^T X A^{n-r} e = e^T X Q^i e$ ou $e^T X (Q^i - A^i) e = 0$ et car toute les matrices n'ont pas des coefficients negatifs, donc la relation est équivalente á la suivante :

$$X(Q^i - A^i) = 0 \qquad 1 \leq i \leq r-1 \tag{19}$$

c) $n > 2r, i = n - 2r + 1$.Dans ce cas la relation (18) peut s'écrire $e^T(A^{n-r+1} - QA^{n-r})e = e^T X e e^T A^{n-2r+1} e$

En vertu de (8),(12) $ee^T = Q^{r-1}$, donc $e^T(A^{r+i} - QA^{r+i-1} + XQ^{r-1}A^i)e$ ou $X(A^{r-1} - Q^{r-1})A^i = 0$.

Cette relation est un conséquence de (19) . Toutes les transformations sont invértibles, c'est-à-dire on peut écrire des relations entre matrices comme des relations de type (19).

2 $\Longleftrightarrow$ 3. Ecrivons les relations dont il faut démontrer l'équivalence.

$$\left.\begin{aligned} X^2 &= 0 \\ XQX &= 0 \\ &\cdots \\ XQ^{r-2}X &= 0 \end{aligned}\right\} \tag{20}$$

et

$$\left.\begin{aligned} XQ &= X(Q-X) \\ XQ^2 &= X(Q-X)^2 \\ &\cdots \\ XQ^{r-1} &= X(Q-X)^{r-1} \end{aligned}\right\} \tag{21}$$

Il est évidént, que les relations des premières lignes de (20) et (21) sont équivalentes. Supposons, qu'on a dèja démontré l'équivalence des i premieres relations.Alors,

$X(Q-X)^{i+1} = X(Q-X)^i(Q-X) = XQ^i(Q-X) = XQ^{i+1} - XQ^i X$.

Il en résulte que la relation

$X(Q-X)^{i+1} = XQ^{i+1} - XQ^i X = XQ^{i+1}$

est équivalente à

$XQ^i X = 0$.

Construction des codes sans recoupement

Soit V un code binaire, c'est-à-dire $V = \{a, b\}$. Cherchons un dictionnaire sans recupément ayant le type *aub*. Çela ne restreint pas le problème car les mots *aua*,*bub* recupént eux-même et les mots *aub* et *bva* recoupént mutiellement Avec cette restriction la matrice X est

$$Q = \begin{pmatrix} 0 & x_1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & x_2 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & x_p \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

où $x_i = 0, 1, p = 2^{r-2}$. Regardons le produit $XCX = D$ pour une matrice C. Les éléments de D peuvent s'écrire de la façon suivant :

$d_{ij} = x_i c_{2ij} x_j = x_i x_j c_{2ij}$

Considèrons les matrices

$$X^{(2)} = \begin{pmatrix} x_1x_1 & x_1x_2 & \dots & x_1x_p \\ x_2x_1 & x_2x_2 & \dots & x_2x_p \\ \vdots & \vdots & \ddots & \vdots \\ x_px_1 & x_px_2 & \dots & x_px_p \end{pmatrix}$$

et

$$C' = \begin{pmatrix} c_{21} & c_{22} & \dots & c_{2p} \\ c_{41} & c_{42} & \dots & c_{4p} \\ \vdots & \vdots & \ddots & \vdots \\ c_{2p1} & c_{2p2} & \dots & c_{2pp} \end{pmatrix}$$

Dans ce cas la matrice D s'écrit $D = X^{(2)} * C'$ où $*$ est la multiplication des matrices élément par élément.

Calculons les matrices E',Q',$(Q^2)'$,...$(Q^{r-2})'$:

$$E' = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

La structure des autres matrices est simple mais volumineuse,c'est pourquois je ne les donne que pour $n = 4$.

$$Q' = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$(Q^2)' = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Dans ce cas l'equation $X^2 = 0$ est équivalente au système suivante:

$$x_1x_2 = 0, x_2x_4 = 0, x_3x_6 = 0, x_4x_8 = 0$$

L'equation $XQX = 0$ est équivalente au système suivante:

$$x_1x_3 = 0, x_1x_4 = 0, x_2x_7 = 0, x_2x_8 = 0$$

$$x_5x_3 = 0, x_5x_6 = 0, x_6x_7 = 0, x_6x_8 = 0$$

et comme la solution consiste on des nombres non négatifs,on a

$$(x_1 + x_5)(x_3 + x_4) = 0$$

$$(x_2 + x_6)(x_7 + x_8) = 0$$

L'equation $XQ^2X = 0$ est équivalente au système suivant:

$$x_1x_5 = 0, x_1x_6 = 0, x_1x_7 = 0, x_1x_8 = 0$$

$$x_3x_5 = 0, x_3x_6 = 0, x_3x_7 = 0, x_3x_8 = 0$$

$$x_5x_5 = 0, x_5x_6 = 0, x_5x_7 = 0, x_5x_8 = 0$$

$$x_7x_5 = 0, x_7x_6 = 0, x_7x_7 = 0, x_7x_8 = 0$$

où $(x_1 + x_3 + x_5 + x_7)(x_5 + x_6 + x_7 + x_8) = 0$

Dans le cas général, notons

$$G_1(x_1, x_2, y_1, y_2) = x_1y_2,$$

$$G_2(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) = (x_1 + x_3)(y_3 + y_4) + x_1 y_2 + x_2 y_4,$$

et par récurrence, si

$$G_N(x_1, x_2, \ldots, x_p, y_1, y_2, \ldots, y_p)$$

est déja définie, posons

$$G_{N+1}(x_1, x_2, \ldots, x_{2p}, y_1, y_2, \ldots, y_{2p}) =$$

$$= G_N(x_1 + x_{p+1}, x_2 + x_{p+2}, \ldots, x_p + x_{2p}, y_1 + y_2, y_3 + y_4, \ldots, y_{2p-1} + y_{2p}) +$$

$$+ x_1 y_2 + x_2 y_4 + \cdots + x_p y_{2p}.$$

Le système des equations pour trouver des dictionnaires sans recoupément est le suivant :

$$G_N(X, X) = 0 \tag{24}$$

où les composantes de X sont 0 ou 1.

Comme nous nous intéressons aux matrices, dont les éléments sont 0 ou 1, c'est plus commode d'utilizer les fonctions boolienne. Avec cette notation on a

$$L_1(x_1, x_2, y_1, y_2) = x_1 y_2$$

$$L_2(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) = (x_1 \vee x_3)(y_3 \vee y_4) \vee x_1 y_2 \vee x_2 y_4$$

$$L_{N+1}(x_1, x_2, \ldots, x_{2p}, y_1, y_2, \ldots, y_{2p}) =$$

$$L_N(x_1 \vee x_{p+1}, x_2 \vee x_{p+2}, \ldots, x_p \vee x_{2p} y_1 \vee y_2, y_3 \vee y_4, \ldots, y_{2p-1} \vee y_{2p})$$

$$+ x_1 y_2 \vee x_2 y_4 \vee \cdots \vee x_p y_{2p}.$$

La relation (24) est équivalente á

$$L_N(X, X) = 0 \tag{25}$$

La forme normale conjonctive de la fonction $L_N(X, X)$ donne tous les dictionnaires sans recoupement. Enumerons tous les mots comme des nombres decimaux. Par example, un code {7,18,23} corespondent á {000111 , 010011 , 010111}.Tout les codes sans recoupements de degré 6 sont les suivants:

{1},{31},
{3,5},{15,23},
{11,13,15},{7,11,13},{5,7,13},{5,13,15},{7,19,23},
{7,11,19},{3,19,23} {3,11,19}.

Il y a à peu près 100 dictionnaires sans recoupéments de degré 7. Pour trouver un dictionnaire on peut fixer un partie des variables. Par example, si $x_{2i+1} = 0$,$y_{2^k - j} = 0$ pour $j < 2k - 2$ alors

$$L_4 = x_6 y_{12}$$

$$L_5 = (x_6 \vee x_{12})(y_{23} \vee y_{24}) \vee x_6 y_{15} \vee x_{10} y_{20} \vee x_{12} y_{24}.$$

$$L_6 = (x_6 \vee x_{22} \vee x_{38} \vee x_{54})(y_{45} \vee y_{46} \vee y_{47} \vee y_{48}) \vee$$

$$(x_6 \vee x_{38})(y_{23} \vee y_{24}) \vee (x_{10} \vee x_{42})(y_{39} \vee y_{40}) \vee$$

$$(x_{12} \vee x_{44})(y_{47} \vee y_{48}) \vee x_6 y_{12} \vee x_{10} y_{20} \vee x_{12} y_{24} \vee$$

$$x_{18} y_{36} \vee x_{20} y_{40} \vee x_{22} y_{44} \vee x_{24} y_{46}$$

Une telle L_6 est accessible pour trouver sa forme conjonctive. Un dictionnaire trouvé par ce moyen est le suivant:

{ 3,19,23,35,43,67,75,83}

Enfin,le problème se trouver des dictionnaires sans recoupement peut se regarder comme le problème de trouver $max(\Sigma x_i)$ pour $G_N(X,X) = 0$. Un dictionnaire de degré 10 , trouvé par ce moyen est le suivant:

{341,343,347,349,351,361,365,367,373,375,379,381,383,427,429,431,437,439,443, 445,447,469,471,475,477,479,491,493,495,501,503,507,509,511}.

Remerciements: Je remercie cordiellement Emmanuel Peyre pour son assistance.

Bibliographie

1.Cartan H.,Eilenberg S., Homological algebra.Princeton Univ.Press 1956.

2.Herstein I., Noncommutative rings. NY,1968.

3.Markov A.A. Introduction in code theory,M.,1982(Russian).

4.Govorov V.E., Dimension and multiplicity of graded algebras. Sibirsk.Mat. Ž (1973),840-845.

5.Govorov V.E., Graded algebras.Mat.Zametki,12(1972) 197-204.