COLLOQUE NATIONAL SUR LE TRAITEMENT DU SIGNAL
ET SES APPLICATIONS

NICE du 26 au 30 AVRIL 1977

# Systèmes linéaires à coefficients entiers et codage algébrique d'éléments non-inversibles

Y. ROUCHALEAU

Ecole Nationale Supérieure des Mines de Paris SOPHIA ANTIPOLIS - 06560 VALBONNE

## RESUME

Cet article rassemble un certain nombre de résultats de la théorie algébrique des systèmes linéaires, applicables au codage de nombres entiers.

## SUMMARY

This article summarizes a number of developments in algebraic system theory applicable to the coding of integers.

# Systèmes linéaires à coefficients entiers et codage algébrique d'éléments non-inversibles

Le but de cet exposé est de présenter certains résultats récents en théorie algébrique des systèmes susceptibles d'être intéressants pour le codage algébrique.

Les travaux de MASSEY (1968) et SAIN (1977) ont mis en évidence de façon claire le lien étroit existant entre certaines méthodes de codage et décodage algébrique et les problèmes fondamentaux de la théorie des systèmes linéaires. En effet, le codage convolutionnel revient à faire passer le message à coder dans un système linéaire dont l'espace de sortie a une dimension plus élevée que l'espace d'entrée (en initialisant le système à l'état zéro), tandis que le codage cyclique peut être interprété en termes de systèmes linéaires à entrée nulle.

Plus précisément, l'étape essentielle du décodage d'un code cyclique (la solution de ce que BERLEKAMP (1968) appelle "the key equation") revient à rechercher deux polynomes a(z) et b(z) (ce dernier monique) tels que le degré de b(z) soit supérieur à celui de a(z), que les r premiers termes du développement en série de $\frac{a(z)}{b(z)}$ suivant les puissances décroissantes de z soient égaux à r termes donnés (le syndrome) et que le polynome b(z) soit de degré aussi faible que possible. Alors le numérateur indique la valeur des erreurs, le dénominateur leur emplacement.

C'est le même problème que celui de la réalisation minimale d'une suite d'entrée/sortie partielle en théorie des systèmes linéaires : étant donné les r premiers termes d'une suite d'entrée/sortie, trouver un système linéaire en temps discret (X, F, G, H) de dimension minimale dont les r premiers termes de la réponse impulsionnelle soient identiques aux r termes donnés (rappelons qu'un système linéaire (X, F, G, H) peut être interprété comme le système d'équations

$$\begin{cases} x_{n+1} = Fx_n + Gu_n \\ y_{n+1} = Hx_{n+1} \end{cases}$$

où $u_r$ appartient à $R^m$ (l'espace d'entrée), $y_r$ à $R^p$ (l'espace de sortie) $x_n$ à X (l'espace d'état), X étant lui-même un module sans torsion sur le domaine R. La suite d'entrées/sorties d'un tel système est sa réponse impulsionnelle

$$A = HG, \quad A_2 = HFG, \quad ---, \quad A_n = HF^{n-1}G, --- \quad )$$

On peut noter que, dans leur formulation habituelle, le codage cyclique correspond à des systèmes à une seule sortie (systèmes dits scalaires), tandis que le codage convolutionnel introduit des systèmes multivariables (le nombre d'entrées et de sorties dépendant du taux de redondance désiré).

Des algorithmes bien sûr existent dans chaque discipline pour résoudre ces divers problèmes (c. f. par exemple, BERLEKAMP (1968) pour le décodage d'un code cyclique ou KALMAN (1968) pour la construction de réalisations partielles minimales). Ces algorithmes classiques ne sont toutefois valables que lorsque les coefficients manipulés appartiennent à un corps.

.../...

# Systèmes linéaires à coefficients entiers et codage algébrique d'éléments non-inversibles

Des résultats nouveaux ont été obtenus ces dernières années dans le langage des systèmes linéaires, qui permettent d'étendre considérablement les résultats habituels de la théorie au cas où les coefficients appartiennent à un domaine d'intégrité (ou plus généralement à un anneau ne possédant pas d'éléments nilpotents). Le parallèle évident entre systèmes dynamiques et codage rappelé précédemment laisse espérer que ces généralisations pourront s'avérer utiles en codage également.

Nous allons voir successivement trois types de résultats différents, concernant respectivement le polynome de récurrence minimal d'une suite d'entrée/sortie, la dimension minimale de l'espace d'état d'une réalisation, et les modifications que l'adjonction d'une boucle de réaction peuvent amener dans le fonctionnement d'un système.

Nous nous limiterons à exposer ces résultats dans le cas où l'anneau est un domaine d'intégrité, la généralisation au cas d'anneaux réguliers (pas d'éléments nilpotents) étant immédiate.

## I - Le polynome de récurrence minimal d'une séquence.

Les résultats qui vont être mentionnés dans ce paragraphe - ainsi d'ailleurs que dans les suivants - relèvent d'un problème de "descente" : étant donné une suite dont les coefficients appartiennent à un domaine et qui satisfait à certaines relations sur le corps quotient de ce domaine, quand vérifie-t-elle des relations analogues sur l'anneau lui-même ?

En somme, nous cherchons à montrer que le passage au corps quotient n'est pas toujours nécessaire et que l'on peut souvent obtenir les mêmes résultats sur l'anneau lui-même.

(1.1) THEOREME - Soit R un domaine d'intégrité noethérien, K son corps quotient. Soit S une suite de matrices pxm dans R dont les coefficients satisfont une relation de récurrence à coefficients dans K. Alors ils vérifient aussi une relation de récurrence monique à coefficients dans R (c'est-à-dire représentable par un polynome de R[z] dont le terme de plus haut degré est égal à I).

PREUVE : voir ROUCHALEAU, WYMAN and KALMAN [1972]

Il ressort de ce théorème que si une suite d'entrée/sortie dans l'anneau est réalisable sur le corps quotient, elle l'est aussi par un système à coefficients dans l'anneau. Ou bien, en d'autres termes, si l'on sait qu'une suite - de nombres entiers par exemple - a été obtenue par convolution avec un polynome à coefficients rationnels (ou réels, ou dans n'importe quel corps d'extension des nombres entiers), elle aurait pu l'être par convolution avec un polynome à coefficients entiers.

Ce résultat garantit donc l'existence d'une récurrence sur l'anneau. Mais il ne dit rien sur la taille de cette récurrence. Elle pourrait être beaucoup plus longue que celle qui existe sur le corps. On va voir qu'en général il n'en est rien. Mais tout d'abord une

.../...

(1.2) DEFINITION : Soient R un domaine, A une R - algèbre. On dit qu'un élément x de A est intégral sur R s'il est racine d'un polynome monique à coefficient dans R :

$$x^n + a_1 x^{n-1} + \text{-----} + a_n = 0 \qquad , a_i \in R$$

Un domaine R est intégralement clos si tout élément de son corps quotient K qui est intégral sur R appartient à R.

Notons que tout anneau factoriel est intégralement clos, et donc en particulier que les nombres entiers et les polynomes à coefficients réels ou entiers forment des anneaux noethériens intégralement clos.

Cette hypothèse intervient dans notre problème à cause du théorème suivant

(1.3) THEOREME : Soient R un anneau intégralement clos, K son corps quotient. Soient f(z) et g(z) deux polynomes moniques de K[z], h(z) leur produit. Si h(z) appartient à R[z], il en est nécessairement de même de f(z) et g(z).

PREUVE : voir BOURBAKI [Algèbre Commutative, Chap. 5, § 1, n° 3, corollaire de la proposition 11]. □

C'est là l'outil essentiel pour établir le

(1.4) THEOREME : Soient R un anneau noethérien intégralement clos, K son corps quotient, S une suite de matrices pxm sur K. Supposons que f(z) soit le polynome de récurrence monique de plus faible degré dans K[z] satisfait par S. Alors f(z) est nécessairement dans R[z].

PREUVE : L'ensemble des polynomes de récurrence dans K[z] vérifiés par S est un idéal J. D'après (1.1), comme R est noethérien, cet idéal contient un polynome monique h(z) de R[z]. K[z] étant un anneau principal, J est généré par un polynome monique de degré minimal f(z). f(z) divise h(z) dans K[z], et donc, d'après (1.3), appartient à R[z]. □

Une condition nécessaire et suffisante pour que (1.4) soit vrai est que l'anneau R soit complètement intégralement clos (voir CAHEN et CHABERT [1972]). Ainsi donc on ne perd rien en ce qui concerne l'existence et la dimension d'une relation de récurrence, que l'on travaille sur un anneau noethérien intégralement clos ou sur son corps quotient. Il reste à voir dans quelle mesure cela peut influer sur le nombre d'éléments mémoire nécessaires pour réaliser la suite d'entrées/sorties S, c'est-à-dire sur la taille du module d'état du système dynamique linéaire réalisant S.

## II - Dimension minimale du système réalisant une suite S

Rappelons tout d'abord le résultat fondamental de la théorie classique des systèmes linéaires : un système est dit complètement atteignable si tout état peut être atteint à partir de l'état 0 par une suite d'entrées, complètement observable si le

.../...

système partant de deux états différents ne donne pas toujours la même sortie qu'elle que soit la suite d'entrées ; si ces deux propriétés sont vérifiées, le système est appelé canonique.

Alors, si les coefficients appartiennent à un corps, le système est canonique si et seulement si la dimension de son espace d'état est minimale parmi tous les systèmes ayant la même suite d'entrées/sorties. De plus, cette dimension est égale au rang de la matrice de HANKEL associée à la suite d'entrées/sorties :

$$B = \begin{pmatrix} A_1 & A_2 & A_3 & \cdots \\ A_2 & A_3 & A_4 & \cdots \\ \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \end{pmatrix}$$

Si nous essayons de généraliser cela au cas où les coefficients sont dans un anneau, nous devons introduire une distinction suivant le nombre d'entrées et de sorties.

(2.1) THEOREME : Soit R un anneau noethérien intégralement clos, K son corps quotient, S une suite d'entrée/sortie sur R à une seule entrée (m = 1) dont la matrice de HANKEL associée a rang n (donc réalisable sur K par un système de dimension minimale n). Alors il existe un système sur R qui réalise cette séquence , qui est canonique et dont le module d'état est libre de rang n.
Si le système a une seule sortie (p = 1), on peut encore garantir l'existence d'une réalisation libre de rang n sur R ; mais elle n'est plus nécessairement complètement atteignable.

PREUVE : Ce sont des conséquences directes du théorème (1.4) □

(2.2) THEOREME : Soit R un anneau principal, K son corps quotient, S une suite d'entrée/sortie multivariable sur R dont la matrice de HANKEL associée a rang n. Alors il existe un système sur R qui réalise cette suite, qui est canonique et dont le module d'états est libre de rang n.

PREUVE : Voir ROUCHALEAU [1972] □

(2.3) THEOREME : Soit D un anneau principal, R = D[x] l'anneau de polynomes en une indéterminée sur D, S une suite d'entrée/sortie multivariable sur R dont la matrice de HANKEL associée a rang n. Alors il existe un système sur R qui réalise cette suite et dont le module d'états est libre de rang n. Mais ce système n'est pas nécessairement complètement atteignable.

PREUVE : Voir ROUCHALEAU et SONTAG [1977] □

Ainsi donc, dans de nombreux cas (nombres entiers, polynomes à 1 ou 2 indéterminées), il ne sert à rien d'élargir le domaine des coefficients admissibles pour construire un système ayant un comportement déterminé : il est impossible d'abaisser la dimension minimale en utilisant des éléments du corps quotient, ou d'ailleurs de tout autre corps contenant l'anneau.

.../...

Une distinction a été introduite entre les réalisations minimales dont on peut garantir qu'elles sont canoniques et les autres. L'importance de cette distinction va apparaître maintenant.

## III - Modification de la dynamique par boucle de réaction

La théorie classique des systèmes linéaires garantit qu'il est possible de modifier arbitrairement les propriétés spectrales d'un système par réaction d'état si, et seulement si, le système est complètement atteignable. Ce résultat est particulièrement important pour la synthèse de systèmes comportant des boucles de réaction. Dans le cas qui nous intéresse (nombres entiers ou polynomes), nous pouvons aussi énoncer

(3.1) THEOREME : Soient R un anneau principal, (X, F, G, H) un système de dimension n sur R. Etant donné n éléments arbitraires $a_1$, ---, $a_n$ de R, il existe une matrice K telle que le polynôme caractéristique de F - GK soit $z^n + a_1 z^{n-1} + \cdots + a_n$ si et seulement si le système est complètement atteignable.

PREUVE : Voir MORSE [1974] □

Il est facile de montrer par localisation aux idéaux maximaux de l'anneau R que cette condition est nécessaire quel que soit R.

## IV - Applications

Nous avions vu dans l'introduction que deux problèmes étaient particulièrement intéressants pour le codage : la réalisation partielle de suites à une entrée et une sortie, et l'inversion de systèmes linéaires multivariables. Nous pouvons donc, à titre d'illustration des résultats précédents, citer les deux résultats suivants :

(4.1) THEOREME : Soit R un anneau intégralement clos. Le module d'états d'une réalisation d'une dimension minimale sur R est toujours monogénique. Si n est sa dimension, la matrice formée des n premières lignes et n premières colonnes de sa matrice de HANKEL a rang n.

Ainsi donc, l'orsqu'on examine les colonnes de la matrice de HANKEL associée à une suite partielle pour déterminer le rang de sa réalisation minimale, on peut s'arrêter dès que l'on a trouvé la première dépendance intégrale parmi ces colonnes : ce sera là le polynôme minimal du système, et son degré sera le rang du système.

(4.2) THEOREME : Soient R un anneau principal, K son corps quotient. Soit S un système sur R dont l'inverse existe sur K (c. f. par exemple WONHAM Linear Multivariable Systèms, p. 103 ) et a dimension n. Il existe alors un système S' sur R de dimension n tel que la composition de S' avec S soit un multiple scalaire de l'identité.

Le système S' est donc un pseudo-inverse de S, en ce sens qu'il suffit de le

.../...

faire suivre par une division par un nombre particulier pour obtenir l'inverse de S.

J'espère que cette présentation aura montré à quel point les propriétés des systèmes linéaires à coefficients entiers étaient riches et pourra contribuer à leur application.

## BIBLIOGRAPHIE

BERLEKAMP
(1968) Algebraic Coding Theory, Mc GRAW-HILL

BOURBAKI
(1967) Algèbre Commutative, HERMANN

CAHEN et CHABERT
(1972) "Eléments quasi-entiers et extensions de FATOU", Queens Math. Preprint n° 1972-22, Queens University, KINESTON, ONTARIO.

FLIESS
(1971) "Deux applications de la représentation matricielle d'une série rationnelle non-commutative", J. of Algebra, 19, pp. 344-353.

KALMAN
(1968) Lectures on Controllability and Observability, CIME notes.

MASSEY
(1969) "Shift register synthesis and BCH decoding", I. E. E. E. Trans. Inform. Th., 15, pp. 122-127.

MORSE
(1974) "Ring models for delay-differential systems", Proc. IFAC Symp. on Multivariable Technological Systems, MANCHESTER

ROUCHALEAU
(1972) Linear, discrete, finite dimensional, dynamical systems over some classes of commutative rings, Ph. D. dissertation, STANFORD.

ROUCHALEAU, WYMAN and KALMAN
(1972) "Algebraic structure of linear dynamical systems III : Realization theory over a commutative ring", Proc. Nat. Acad. Sci. U. S. A. 69, pp. 3404-3406.

.../...

ROUCHALEAU and SONTAG

(1977) "On the existence of minimal realizations of linear, dynamical systems over Noetherian integral domains", à paraître

SAIN

(1977) "Minimal torsion spaces and the partial imput/output problem", à paraître

WONHAM

(1974) Linear Multivariable Control : a Geometric Approach, SPRINGER