UNIVERSITÉ DE NEUCHÂTEL
INSTITUT DE MICROTECHNIQUE

# Contribution à la théorie des suites aléatoires binaires

THÈSE

PRÉSENTÉE À LA FACULTÉ DES SCIENCES
POUR OBTENIR LE GRADE DE DOCTEUR ÈS SCIENCES

PAR

Giancarlo Duella

# IMPRIMATUR POUR LA THÈSE

*Contribution à la théorie des suites binaires aléatoires*

de M*onsieur Giancarlo Duella*

UNIVERSITÉ DE NEUCHATEL

FACULTÉ DES SCIENCES

La Faculté des sciences de l'Université de Neuchâtel, sur le rapport des membres du jury,

*MM. les professeurs A. Shah, U. Suter, H. Mey (Berne) et J. Massey (EPF-Zurich)*

autorise l'impression de la présente thèse.

Neuchâtel, le *13 mars 1986*

Le doyen:

François Sigrist

*François Sigrist*

RESUME.

De nouveaux outils facilitant l'étude des caractéristiques statistiques des variables et suites aléatoires binaires ont été développés. Nous avons tiré avantage des propriétés de la transformation de Walsh, transformation qui permet, en particulier, de relier probabilités conjointes et moments conjoints correspondants de k variables aléatoires binaires.

Nous nous sommes ensuite penchés sur l'étude des chaînes de Markov binaires qui forment une sous-classe importante des suites aléatoires binaires. Nous en avons examiné leurs moments conjoints ainsi que la multiplication de telles chaînes, indépendantes l'une de l'autre. Il est à noter que le résultat de ladite multiplication n'est en général pas une chaîne de Markov binaire.

Enfin, nous avons étudié quelques aspects des suites pseudo-aléatoires binaires, de période maximale, en tant que cas limite de chaînes de Markov binaires. En appliquant quelques-uns des concepts développés précédemment, il nous a été possible de dériver de nouvelles propriétés caractérisant ces suites.

TABLE DES MATIERES.

LISTE DES NOTATIONS.

$E_\beta$: ensemble {0,1}.

$E_\xi$: ensemble {+1,-1}.

$N$: ensemble des nombres entiers $\geq 0$.

$R$: ensemble des nombres réels.

$|J|$: cardinal de l'ensemble J.

$\Phi$: ensemble vide.

U: réunion d'ensembles.

$I_r$: matrice identité de dimension $2^r \times 2^r$.

$A^T$: transposée de la matrice A.

diag $\{d_1\ d_2\ \text{---}\ d_n\}$: matrice diagonale.

$H_k$: matrice de Walsh-Hadamard de dimension $2^r \times 2^r$.

$\Pi_r = \{\pi_{00}\ \pi_{12}\ \text{---}\ \pi_{i2i\bmod 2^r}\ \text{---}\ \pi_{2^r-1 2^r-2}\}$: matrice des probabilités de transition d'une chaîne de Markov binaire d'ordre r (voir IV.1).

$e_r = [1\ 1\ \text{---}\ 1]^T$: vecteur $2^r \times 1$.

$\bigotimes_{l=1}^{n} A_l = A_1 \otimes A_2 \otimes \text{---} \otimes A_n$: produit de Kronecker.

$\prod_{l=1}^{n}{}^{o} A_l = A_1 o A_2 o \text{---} o A_n$: produit de Schur.

det A: déterminant de la matrice A.

$\binom{k}{\nu}$: coefficient binômial.

$\tilde{\nu}_k = \nu_1 + \nu_2 + \text{---} + \nu_k$, $\nu_l \in N$.

$b_1 \oplus b_2$: somme modulo 2 de deux éléments appartenant au corps de Galois GF(2).

$\sum_{l=1}^{n} b_l = b_1 \oplus b_2 \oplus \text{---} \oplus b_n$.

SBSM $\pi$: source binaire sans mémoire telle que $P\{\alpha(n) = 0\} = \pi$.

SPAB: suite pseudo-aléatoire binaire.

# I. INTRODUCTION.

Supposons qu'un signal représente, pour nous, la variation temporelle d'une grandeur physique comme par exemple une tension ou un courant électrique.

Souvent, le signal entrant dans un système donné n'est pas déterministe mais aléatoire. Il est alors impossible de prédire exactement quelle sera la forme du signal de sortie. Cependant, nous pouvons observer expérimentalement que certaines propriétés moyennes de ces signaux aléatoires sont raisonnablement régulières.

La régularité statistique des moyennes est un phénomène vérifiable expérimentalement dans beaucoup de situations impliquant des quantités variant de manière aléatoire. Nous sommes alors motivés pour construire un modèle nous permettant d'étudier de tels phénomènes. C'est une branche des mathématiques que l'on appelle la théorie des probabilités. Une des notions fondamentales de cette théorie est celle de variable aléatoire. On appelle variable aléatoire (discrète ou continue) une grandeur qui peut, dans une expérience, prendre l'une quelconque des valeurs possibles, inconnue d'avance [57]. Le signal aléatoire que nous avons rencontré ci-dessus peut être défini par une succession (dans le temps) de variables aléatoires. C'est ce qu'on appelle un processus stochastique [18]

Durant ces dernières années, l'utilisation de systèmes numériques s'est considérablement étendue dans les domaines tels que le traitement du signal ou les télécommunications. Ces systèmes numériques sont constitués par un ensemble de cellules de base inter-connectées ne réagissant qu'à deux niveaux d'excitation notés communément par les symboles 0 et 1.

Si les techniques nous permettant d'analyser le comportement de systèmes continus stimulés par des processus stochastiques sont bien connues [e.g. 46], il n'est pas dit qu'elles s'appliquent directement dans le contexte de systèmes numériques. Etant donné la structure interne de ces derniers, les processus stochastiques particuliers auxquels nous avons fréquemment affaire sont représentés par l'ensemble des suites aléatoires binaires. L'étude de leurs propriétés statistiques est donc importante puisqu'elle devrait permettre de développer de nouveaux outils adaptés à l'analyse de situations comme celles décrites ci-dessus.

Pourtant, il n'existe pas, à notre connaissance, de monographe traitant d'une théorie des probabilités spécifique aux variables aléatoires binaires ainsi que les transformations qu'elles subissent en traversant un système numérique (Cox [12] par contre propose une étude sur l'analyse statistique de données binaires).

Fire [19] examine les effets statistiques de transformations booléennes opérées sur des chaînes de Markov binaires. Il en considère deux:

- addition modulo 2, du type série-série, de deux chaînes de Markov binaires indépendantes,

- traitement d'une chaîne de Markov binaire par un filtre numérique. Par filtre numérique, on entend un filtre séquentiel binaire, linéaire ou non par rapport aux opérations sur le champ de Galois GF(2), traitant des variables binaires.

Le principal résultat de cette étude est représenté par un ensemble de théorèmes qui spécifient, dans les deux situations décrites ci-dessus, sous quelles conditions les suites aléatoires binaires qui s'ensuivent sont aussi des chaînes de Markov binaires (nous discuterons, au chapitre IV, de la validité d'un des théorèmes importants contenus dans cette étude).

Booth [7] généralise le concept de chaîne de Markov en introduisant une nouvelle classe de processus aléatoires qu'il désigne sous le nom de processus linéairement dépendants. Ces derniers sont aussi, comme d'ailleurs toute chaîne de Markov, caractérisés par une matrice des probabilités de transition. Elle devient de plus en plus complexe lorsqu'elle représente un processus linéairement dépendant résultant d'une combinaison booléenne d'un nombre croissant de tels processus (indépendants). En plus, il nous semble difficile de relier ce type de processus à une situation physique quelconque. C'est peut être pour cela qu'il ne nous a pas été possible de trouver de référence postérieure à celle déjà citée.

La fonction d'autocorrélation (ou moment conjoint du second ordre) joue un rôle important dans l'étude de toute suite aléatoire binaire. Notons que dans ce cadre, il n'est pas possible de générer n'importe quelle fonction d'autocorrélation et que l'on peut définir une classe U à laquelle elles appartiennent toutes [38,39].

Mentionnons le fait que la fonction d'autocorrélation est un paramètre utilisé pour analyser certains systèmes de communication [26,48] ainsi que pour tester la sécurité de techniques cryptographiques spéciales [54]. Remarquons que l'on peut tirer avantage de la transformation de Walsh [34] pour calculer la fonction d'autocorrélation d'une suite aléatoire binaire générée par un filtre numérique récursif couplé à une source binaire sans mémoire (cas particulier d'une chaîne de Markov binaire) [58].

Shah [50,51] examine quelques sous-classes de suites aléatoires binaires comme, en particulier, celle formée d'éléments générés à partir de la détection de la polarité de processus stochastiques gaussiens stationnaires. Il tire ensuite les conséquences de quelques transformations booléennes simples qu'il leur fait subir. Shah décrit également, en détail, les propriétés statistiques du premier et second ordre des suites aléatoires binaires. Il conjecture un théorème reliant probabilités conjointes et moments conjoints correspondants par une transformation de Walsh.

Quelques-uns de ces concepts ont été appliqués dans le but d'analyser les performances d'un démodulateur digital DPSK (Differential Phase Shift Keying ou Saut de Phase Différentiel) lorsque le cannal de transmission est perturbé par un bruit gaussien blanc [16]. Ici, les processus stochastiques considérés ne sont plus stationnaires mais cyclo-stationnaires (ses propriétés statistiques varient de manière périodique) [22] ce qui complique l'analyse en question.

Enfin, un des domaines dans lequel il se fait actuellement, comme d'ailleurs par le passé, beaucoup de recherche est celui des suites pseudo-aléatoires binaires générées par une classe particulière de machines séquentielles finies: les filtres numériques récursifs (Fig. 1.1).

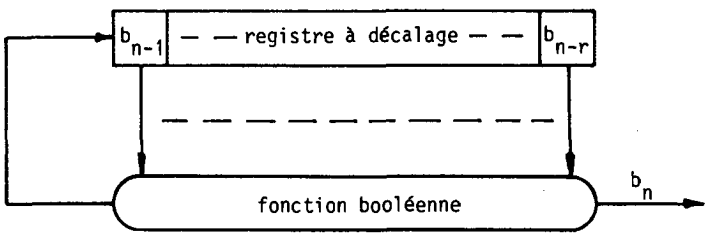



*Fig. 1.1: Filtre numérique récursif générant une suite pseudo-aléatoire binaire.*

Ces suites sont évidemment déterministes et périodiques mais possèdent un caractère suffisamment aléatoire pour jouer le rôle du "hasard" dans de nombreuses applications qui en nécessitent [23]. En vue d'optimiser les performances de ces machines, on s'intéresse surtout à celles dont la structure permet de produire des suites de période maximale.

Nous ne donnerons pas ici une liste exhaustive de la littérature concernant ce sujet tant elle est longue. Toutefois, citons les quelques références suivantes:

- Le livre de Golomb [23] est un manuel essentiel pour qui veut étudier ce sujet. On y trouve une description détaillée de la théorie relative aux suites pseudo-aléatoires binaires générées par des filtres numériques récursifs linéaires. Quelques propriétés des suites produites par des systèmes non linéaires y sont aussi décrites.

- Massey [40] développe un algorithme efficace permettant, à partir d'une suite pseudo-aléatoire binaire quelconque, de trouver le filtre numérique récursif linéaire de longueur minimale générant ladite suite.

- Groth [25] et Key [35] étudient la classe des filtres numériques récursifs linéaires ayant pour sortie une combinaison booléenne quelconque entre les cellules des registres à décalage constituant ces filtres.

- Fredricksen [20] décrit différents algorithmes permettant de générer une suite pseudo-aléatoire binaire de période maximale ou suite de de Bruijn.

Notons finalement qu'une suite pseudo-aléatoire binaire ainsi générée (Fig. 1.1) n'est qu'un cas limite d'une chaîne de Markov binaire [23].

Le but du présent travail est de développer de nouveaux outils propres à l'étude des variables et suites aléatoires binaires. Nous allons aussi considérer quelques opérations booléennes effectuées sur un ensemble de variables ou suites aléatoires binaires indépendantes.

Sommaire.

*Chapitre I :* Introduction et motivations.

*Chapitre II :* Contient les définitions de base utilisées tout au long de cet exposé.

*Chapitre III:* Traite des caractéristiques statistiques des variables et suites aléatoires binaires. Démonstration d'un théorème reliant probabilités conjointes et moments conjoints par une transformation de Walsh. Extension de la notion d'indépendance stastistique de variables aléatoires binaires. Etude détaillée de la multiplication (ou somme modulo 2) de suites aléatoires binaires indépendantes et probabilités conjointes limites.

*Chapitre IV :* Traite des chaînes de Markov binaires. Calcul des moments conjoints et plus spécialement de la fonction d'autocorrélation. Etude de la multiplication (ou somme modulo 2) de chaînes de Markov binaires indépendantes. On montre que la résultat de cette multiplication n'est pas toujours une chaîne de Markov.

*Chapitre V :* Aspects des suites pseudo-aléatoires binaires comme cas limite de chaînes de Markov binaires. Correspondance entre matrice des probabilités de transition et filtres numériques récursifs. Déduction de quelques propriétés nécessaires à tout filtre numérique récursif générant une suite de de Bruijn. Calcul de la fonction d'autocorrélation en utilisant certains résultats contenus dans les chapitres III et IV.

*Chapitre VI :* Conclusions.

## II. DEFINITIONS DE BASE.

Nous allons donner ici quelques définitions de base qui nous seront utiles tout au long des chapitres suivants.

Les références principales concernant ce chapitre sont les livres de Papoulis [46], Métivier [43] et Feller [18]. Les définitions contenues dans ces livres sont générales et s'appliquent donc aux cas particuliers des variables aléatoires binaires et des suites aléatoires binaires.

### II.1. Variables aléatoires binaires.

Considérons l'espace probabilisé $(\Omega,F,P)$ ayant les propriétés suivantes:

- l'ensemble $\Omega$ des événements élémentaires est du type: $\Omega = \{\omega_1,\omega_2\}$,

- les événements possibles (F) sont représentés par les quatre ensembles:

$$\Phi,\ \{\omega_1\},\ \{\omega_2\},\ \Omega.$$

Les événements $\{\omega_1\}$ et $\{\omega_2\}$ sont mutuellement exclusifs et $\{\omega_1\} \cup \{\omega_2\} = \Omega$. Il s'ensuit que:

$$P\{\omega_1\} + P\{\omega_2\} = P(\Omega) = 1,$$

où $P\{\omega_1\}$, $P\{\omega_2\}$ et $P(\Omega)$ sont respectivement les probabilités des événements $\{\omega_1\}$, $\{\omega_2\}$ et $\Omega$.

Définition 2.1:

*On appelle variable aléatoire binaire à valeurs dans l'ensemble fini, disons* $E = \{e_1,e_2\}$, *définie sur l'espace probabilisé* $(\Omega,F,P)$, *toute application* $\chi$ *de* $\Omega$ *dans* E *telle que pour tout* $e \in E$, *l'événement* $\{\omega: \chi(\omega) = e\}$ *(en abrégé* $\{\chi = e\}$*) appartienne à* F.

Par la suite, nous ne considérerons que les variables aléatoires binaires $\beta$ à valeurs dans l'ensemble {0,1} et les variables aléatoires binaires $\xi$ à valeurs dans l'ensemble {+1,-1}.

Dorénavant, nous dénoterons l'ensemble {0,1} par le symbole $E_\beta$ et l'ensemble {+1,-1} par le symbole $E_\xi$.

Si b et x sont respectivement les réalisations des variables aléatoires binaires $\beta$ et $\xi$, il existe une application linéaire telle que:

Définition 2.2:

$$L: E_\beta \longrightarrow E_\xi$$
$$b \longmapsto x = 1-2b.$$

La fonction $L(\beta)$ est aussi une variable aléatoire binaire définie via la variable aléatoire binaire $\beta$ et la fonction L(b). Sachant cela, nous écrirons: $\xi = L(\beta)$

L'algèbre de Boole et l'algèbre linéaire sur le corps de Galois GF(2) [44] sont des méthodes connues pour décrire les systèmes logiques combinatoires. Parfois, l'application L nous sera très utile pour déterminer certains paramètres statistiques liés aux fonctions de sortie de ces systèmes lorsque leurs entrées auront un caractère aléatoire.

En utilisant la définition 2.2, on trouve facilement les correspondances données dans la table 2.1. On constate que les opérations effectuées sur l'ensemble $E_\xi$ sont les opérations du corps des nombres réels.

| Algèbre de Boole | GF(2) | $E_\xi$ |
|---|---|---|
| Inversion: $\bar{b}$ | $1 \oplus b$ | $-x$ |
| AND : $b_1 b_2$ | $b_1 b_2$ | $\max\{x_1, x_2\}$ |
| OR : $b_1 + b_2$ | $b_1 \oplus b_2 \oplus b_1 b_2$ | $\min\{x_1, x_2\}$ |
| XOR : $b_1\bar{b}_2 + \bar{b}_1 b_2$ | $b_1 \oplus b_2$ | $x_1 x_2$ |

*Table 2.1: Correspondance entre opérations de l'algèbre de Boole, sur GF(2) et sur $E_\xi$.*

Soient $\xi_0, \xi_1, ---, \xi_{k-1}$ k variables aléatoires binaires à valeurs dans l'ensemble $E_\xi$. On définit une variable aléatoire $\xi$ à valeurs dans l'ensemble $E_\xi^k$ en posant:

$$\xi = (\xi_0, \xi_1, ---, \xi_{k-1}).$$

Pour tout point $(x_0, x_1, ---, x_{k-1}) \in E_\xi^k$, on a:

$$\{\xi = (x_0, x_1, ---, x_{k-1})\} = \{\xi_0 = x_0, \xi_1 = x_1, ---, \xi_{k-1} = x_{k-1}\}.$$

Définition 2.3:

*La loi de probabilité de $\xi$ est appelée probabilité conjointe des variables aléatoires binaires $\xi_0, \xi_1, ---, \xi_{k-1}$:*

$$P\{\xi = (x_0, x_1, ---, x_{k-1})\} = P\{\xi_0 = x_0, \xi_1 = x_1, ---, \xi_{k-1} = x_{k-1}\}.$$

Remarquons qu'il existe $2^k$ différentes probabilités conjointes de ces k variables aléatoires binaires.

Définition 2.4:

*On appelle probabilité marginale, la probabilité:*

$$P\{\xi_0 = x_0, ---, \xi_{i-1} = x_{i-1}, \xi_{i+1} = x_{i+1}, ---, \xi_{k-1} = x_{k-1}\} =$$

$$= \sum_{x_i \in E_\xi} P\{\xi_0 = x_0, ---, \xi_i = x_i, ---, \xi_{k-1} = x_{k-1}\}.$$

En faisant la somme sur tous les points $(x_0, x_1, ---, x_{k-1}) \in E_\xi^k$, on obtient:

$$\sum_{(x_0, ---, x_{k-1}) \in E_\xi^k} P\{\xi_0 = x_0, \xi_1 = x_1, ---, \xi_{k-1} = x_{k-1}\} = 1.$$

Définition 2.5:

*Etant donné l'événement* $\{\xi_i = x_i, \text{---}, \xi_{k-1} = x_{k-1}\}$ *de probabilité non nulle, on appelle probabilité conditionnelle de l'événement* $\{\xi_0 = x_0, \text{---}, \xi_{i-1} = x_{i-1}\}$ *sachant* $\{\xi_i = x_i, \text{---}, \xi_{k-1} = x_{k-1}\}$, *ou encore probabilité conditionnelle de* $\{\xi_0 = x_0, \text{---}, \xi_{i-1} = x_{i-1}\}$ *par rapport à* $\{\xi_i = x_i, \text{---}, \xi_{k-1} = x_{k-1}\}$, *le nombre défini par:*

$$P\{\xi_0 = x_0, \text{---}, \xi_{i-1} = x_{i-1} | \xi_i = x_i, \text{---}, \xi_{k-1} = x_{k-1}\} =$$

$$= \frac{P\{\xi_0 = x_0, \xi_1 = x_1, \text{---}, \xi_{k-1} = x_{k-1}\}}{P\{\xi_i = x_i, \text{---}, \xi_{k-1} = x_{k-1}\}}.$$

Définition 2.6:

*k variables aléatoires binaires* $\xi_0, \xi_1, \text{---}, \xi_{k-1}$ *à valeurs dans l'ensemble* $E_\xi$ *sont statistiquement indépendantes, ou plus simplement indépendantes, si:*

$$P\{\xi_0 = x_0, \xi_1 = x_1, \text{---}, \xi_{k-1} = x_{k-1}\} = \prod_{i=0}^{k-1} P\{\xi_i = x_i\}.$$

Définition 2.7:

*L'espérance mathématique du produit de k variables aléatoires binaires* $\xi_0, \xi_1, \text{---}, \xi_{k-1}$ *à valeurs dans l'ensemble* $E_\xi$ *s'appelle le moment conjoint d'ordre k de ces variables aléatoires binaires:*

$$m_{\xi_0\xi_1\text{----}\xi_{k-1}} = E\{\xi_0\xi_1 \text{ --- } \xi_{k-1}\} =$$

$$= \sum_{(x_0, \text{---}, x_{k-1}) \in E_\xi^k} x_0 \cdot \text{ --- } x_{k-1} \cdot P\{\xi_0 = x_0, \text{---}, \xi_{k-1} = x_{k-1}\}.$$

Supposons que ces k variables aléatoires binaires forment un ensemble. Il est alors possible de définir $2^k$ différents moments conjoints entre les éléments de cet ensemble. En effet, nous pouvons les définir par l'espérance mathématique suivante:

$$m_{\xi_0^{d_0}\xi_1^{d_1}\text{----}\xi_{k-1}^{d_{k-1}}} = E\{\xi_0^{d_0}\xi_1^{d_1} \text{ --- } \xi_{k-1}^{d_{k-1}}\}, \quad (d_0, d_1, \text{---}, d_{k-1}) \in E_\xi^k.$$

Pour simplifier la notation, nous écrirons souvent ces moments conjoints:

$$m_j = E\left\{\prod_{i=0}^{k-1} \xi_i^{d_i}\right\} \quad \text{où} \quad j = \sum_{i=0}^{k-1} d_i \cdot 2^{k-1-i}, \quad 0 \leq j \leq 2^k - 1.$$

L'ordre du moment conjoint considéré sera donné par: $\sum_{i=0}^{k-1} d_i$.

Il y aura donc $\binom{k}{s}$ moments conjoints d'ordre s, $0 \leq s \leq k$.

Exemple 2.1:

Voyons le cas de trois variables aléatoires binaires $\xi_0$, $\xi_1$ et $\xi_2$ à valeurs dans l'ensemble $E_\xi$. Les huit différents moments conjoints définis entre ces trois variables aléatoires binaires sont les suivants:

| $d_0$ | $d_1$ | $d_2$ | moment conjoint |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | $m_{\xi_2}$ |
| 0 | 1 | 0 | $m_{\xi_1}$ |
| 0 | 1 | 1 | $m_{\xi_1\xi_2}$ |
| 1 | 0 | 0 | $m_{\xi_0}$ |
| 1 | 0 | 1 | $m_{\xi_0\xi_2}$ |
| 1 | 1 | 0 | $m_{\xi_0\xi_1}$ |
| 1 | 1 | 1 | $m_{\xi_0\xi_1\xi_2}$ |

Dans cet exemple, on constate qu'entre trois variables aléatoires binaires à valeurs dans l'ensemble $E_\xi$, on peut définir un moment conjoint d'ordre zéro, trois moments conjoints d'ordre un, trois moments conjoints d'ordre deux et un moment conjoint d'ordre trois.

Les deux grandeurs définies ci-dessous jouent un rôle important dans l'étude des variables aléatoires binaires.

Définition 2.8:

*La moyenne* $m_\xi$ *de la variable aléatoire binaire* $\xi$ *à valeurs dans l'ensemble* $E_\xi$ *est égale à son espérance mathématique:*

$$m_\xi = E\{\xi\}.$$

Définition 2.9:

*On définit la covariance* $C_{\xi_1\xi_2}$ *entre deux variables aléatoires binaires* $\xi_1$ *et* $\xi_2$ *à valeurs dans l'ensemble* $E_\xi$ *de la manière suivante:*

$$C_{\xi_1\xi_2} = E\{(\xi_1 - m_{\xi_1})(\xi_2 - m_{\xi_2})\}.$$

On trouve facilement que: $C_{\xi_1\xi_2} = m_{\xi_1\xi_2} - m_{\xi_1} m_{\xi_2}$.

Dans le cadre des variables aléatoires binaires à valeurs dans l'ensemble $E_\xi$, la covariance $C_{\xi_1\xi_2}$ est égale au coefficient de corrélation $\rho_{\xi_1\xi_2}$ puisque par définition:

$$\rho_{\xi_1\xi_2} = \frac{C_{\xi_1\xi_2}}{\sqrt{E\{\xi_1^2\}E\{\xi_2^2\}}} = C_{\xi_1\xi_2} \quad \text{car} \quad E\{\xi_1^2\} = E\{\xi_2^2\} = 1.$$

*Remarque:*

Nous pouvons appliquer strictement les définitions 2.3 à 2.9 aux variables aléatoires binaires à valeurs dans l'ensemble $E_\beta$.

## II.2. Suites aléatoires binaires.

Il s'agit de représenter par un modèle mathématique l'état d'un système dépendant d'un paramètre et du hasard. Ici, nous faisons intervenir le hasard sous la forme de l'espace probabilisé $(\Omega,F,P)$ défini dans le sous-chapitre II.1, alors que n désigne un paramètre de temps discret, $n \in N$.

Le modèle mathématique cherché se présente donc naturellement comme une fonction

$$(n,\omega) \longmapsto \chi(n,\omega)$$

définie sur $N \times \Omega$ à valeurs dans l'ensemble $E = \{e_1,e_2\}$.

L'état du système, pour la valeur n du paramètre, dépendant uniquement du hasard est une variable aléatoire binaire $\chi(n,\omega)$.

Ceci nous amène donc à la définition suivante:

Définition 2.10:

*On appelle suite aléatoire binaire, notée* $\{\chi(n)\}$, *une famille de variables aléatoires binaires* $\chi(n)$ *(nous omettrons de mentionner sa dépendance en* $\omega$*),* $n \in N$, *(n est un paramètre de temps discret) définies sur* $(\Omega,F,P)$.

Par la suite, nous ne considérerons que des suites aléatoires binaires stationnaires, c'est-à-dire des suites aléatoires binaires dont la statistique n'est pas modifiée par un décalage de l'origine du temps.

Exemple 2.2:

Nous pouvons construire une suite aléatoire binaire $\Xi = \{\xi(n)\}$ en faisant passer un processus normal stationnaire échantillonné $\{\gamma(n)\}$ dans un détecteur de polarité (Fig. 2.1).

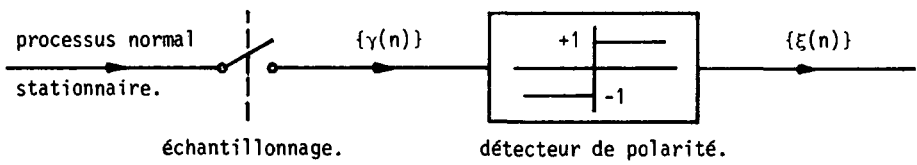



*Fig. 2.1: Construction d'une suite aléatoire binaire à partir d'un processus normal stationnaire.*

Nous pouvons appliquer strictement les définitions 2.3 à 2.9 aux suites aléatoires binaires, ces dernières étant des familles de variables aléatoires binaires.

Si nous avons affaire à une seule suite aléatoire binaire, disons $\Xi = \{\xi(n)\}$, il nous suffit d'identifier $\xi_0$ et $\xi(n)$, $\xi_1$ et $\xi(n+\nu_1)$, ---, $\xi_{k-1}$ et $\xi(n+\nu_1+ \text{---} +\nu_{k-1})$, $\nu_i \geq 0$, $1 \leq i \leq k-1$.

Puisque $\Xi$ est stationnaire, notons que sa moyenne $m_\xi = E\{\xi(n)\}$ est constante (définition 2.8) et que le moment conjoint d'ordre k des variables aléatoires binaires $\xi(n)$, $\xi(n+\nu_1)$, ---, $\xi(n+\nu_1+ \text{---} +\nu_{k-1})$ (à valeurs dans l'ensemble $E_\xi$) ne dépend que des différences temporelles $\nu_1$, $\nu_2$, ---, $\nu_{k-1}$. Nous le désignerons par:

$$m_{\xi\xi\text{----}\xi}(\nu_1,\nu_2, \text{---} ,\nu_{k-1}) = \\ = E\{\xi(n)\xi(n+\nu_1) \text{---} \xi(n+\nu_1+ \text{---} +\nu_{k-1})\}. \qquad (2.1)$$

Si nous avons affaire à plusieurs suites aléatoires binaires, disons $\Xi_0 = \{\xi_0(n)\}$, $\Xi_1 = \{\xi_1(n)\}$, ---, $\Xi_{k-1} = \{\xi_{k-1}(n)\}$, il nous suffit d'identifier $\xi_0$ et $\xi_0(n)$, $\xi_1$ et $\xi_1(n+\nu_1)$, ---, $\xi_{k-1}$ et $\xi_{k-1}(n+\nu_1+ \text{---} +\nu_{k-1})$, $\nu_i \geq 0$, $1 \leq i \leq k-1$. Ici aussi, ces k suites aléatoires binaires étant stationnaires, leurs moyennes $m_{\xi_i} = E\{\xi_i(n)\}$, $0 \leq i \leq k-1$, sont constantes et le moment conjoint d'ordre k des variables aléatoires binaires $\xi_0(n)$, $\xi_1(n+\nu_1)$, ---, $\xi_{k-1}(n+\nu_1+ \text{---} +\nu_{k-1})$ (à valeurs dans l'ensemble $E_\xi$) ne dépend que des différences temporelles $\nu_1$, $\nu_2$, ---, $\nu_{k-1}$. Nous le désignerons par:

$$m_{\xi_1\xi_2\text{----}\xi_{k-1}}(\nu_1,\nu_2, \text{---} ,\nu_{k-1}) = \\ = E\{\xi_0(n)\xi_1(n+\nu_1) \text{---} \xi_{k-1}(n+\nu_1+ \text{---} +\nu_{k-1})\}. \qquad (2.2)$$

Définition 2.11:

*On appelle fonction d'autocorrélation le moment conjoint d'ordre 2 de deux variables aléatoires binaires appartenant à la même suite aléatoire binaire.*

*Par exemple, si* $\xi(n)$ *et* $\xi(n+\nu)$ *sont deux variables aléatoires binaires à valeurs dans l'ensemble* $E_\xi$, *alors:*

$$R_{\xi\xi}(\nu) = E\{\xi(n)\xi(n+\nu)\}.$$

Définition 2.12:

*On appelle fonction d'intercorrélation le moment conjoint d'ordre 2 de deux variables aléatoires binaires chacune d'elles appartenant à une suite aléatoire binaire différente.*

*Par exemple, si* $\xi_1(n)$ *et* $\xi_2(n+\nu)$ *sont deux variables aléatoires binaires à valeurs dans l'ensemble* $E_\xi$, *alors:*

$$R_{\xi_1\xi_2}(\nu) = E\{\xi_1(n)\xi_2(n+\nu)\}.$$

Pour terminer, nous allons définir une sous-classe de suites aléatoires binaires qui reviendra souvent dans les chapitres ultérieurs.

Définition 2.13:

*On appelle une suite de Bernoulli une famille de variables aléatoires binaires indépendantes.*

## III. CARACTERISTIQUES STATISTIQUES DES SUITES ALEATOIRES BINAIRES.

Dans ce chapitre, nous allons examiner quelques caractéristiques fondamentales des variables et suites aléatoires binaires.

Supposons que nous ayons affaire à k variables aléatoires binaires, $k \in N$. Nous avons vu au chapitre II que l'on peut leur associer respectivement $2^k$ probabilités et moments conjoints différents (définitions 2.3 et 2.7). Ces grandeurs peuvent être considérées comme étant les composantes de deux vecteurs que nous appellerons respectivement vecteur des probabilités conjointes et vecteur des moments conjoints.

Nous allons montrer que ces deux vecteurs sont liés par une transformation de Walsh. En l'étudiant, nous serons en mesure de dégager quelques propriétés intéressantes des variables (et suites) aléatoires binaires.

Mais avant cela, consacrons les deux premiers sous-chapitres à l'introduction de concepts bien connus qui nous seront utiles dans les développements à venir.

### III.1. Matrices de Walsh-Hadamard.

Les matrices de Hadamard sont des matrices orthogonales dont les éléments appartiennent à l'ensemble $E_\xi$. Nous nous intéresserons plus particulièrement à certaines d'entre elles: les matrices de Walsh-Hadamard qui ont pour lignes les fonctions échantillonnées de Walsh [27]. Une matrice de Walsh-Hadamard $H_k$ est une matrice $2^k \times 2^k$, k entier, dont les éléments h(b,j) sont définis par:

$$h(b,j) = (-1)^{\sum_{l=0}^{k-1} b_l j_l}, \qquad (3.1)$$

où b et j sont deux nombres entiers, $0 \leq b,j \leq 2^k-1$, $b_l$ et $j_l$ étant les k coefficients de leur développement binaire, donnés par:

$$b = \sum_{l=0}^{k-1} b_l \, 2^{k-1-l}, \quad j = \sum_{l=0}^{k-1} j_l \, 2^{k-1-l} \; ; \; b_l, j_l \in E_\beta. \qquad (3.2)$$

Exemple 3.1:

La matrice $H_2$ est donnée par:

$$H_2 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}.$$

*Propriétés:*

En examinant (3.1), nous voyons immédiatement que:

$$H_k = H_k^T , \tag{3.3}$$

$H_k^T$ étant la matrice transposée de la matrice $H_k$.

Considérons maintenant le produit $H_k \cdot H_k^T$. Puisque $H_k$ est une matrice orthogonale, ce produit sera du type:

$$A_k = H_k \cdot H_k^T = \text{diag } \{a_0\ a_1\ \text{---}\ a_{2^k-1}\},$$

où diag $\{a_0\ a_1\ \text{---}\ a_{2^k-1}\}$ est une matrice diagonale dont chaque élément vaut:

$$a_b = \sum_{j=0}^{2^k-1} h(b,j) \cdot h(j,b) = 2^k \quad , \quad 0 \leq b \leq 2^k-1.$$

Donc: $H_k \cdot H_k^T = 2^k \cdot I_k$, $I_k$ étant la matrice identité de dimension $2^k \times 2^k$. Ainsi:

$$\frac{1}{2^k} H_k \cdot H_k^T = I_k \Longrightarrow H_k^{-1} = \frac{1}{2^k} H_k^T = \frac{1}{2^k} H_k . \tag{3.4}$$

On peut aussi facilement démontrer que [36]:

$$H_{k+1} = H_1 \circledcirc H_k , \tag{3.5}$$

où $\circledcirc$ dénote le produit de Kronecker (ou produit direct) [5,8].

## III.2. Fonction caractéristique de Walsh [47].

Commençons par la définition de la transformation de Walsh.

**Définition 3.1:**

*Soient* $\underline{b} = (b_0, b_1, ---, b_{k-1})$ *et* $\underline{j} = (j_0, j_1, ---, j_{k-1})$ *deux éléments appartenant à l'ensemble* $E_\beta^k$. *Définissons leur produit scalaire par:*

$$\underline{b}\cdot\underline{j} = \sum_{l=0}^{k-1} b_l j_l .$$

*Soit une fonction réelle* $f(\underline{b})$ *dont le domaine est l'ensemble* $E_\beta^k$. *Alors, la transformation de Walsh [34] de* $f(\underline{b})$ *est définie comme suit:*

$$F(\underline{j}) = \sum_{\underline{b} \in E^k} f(\underline{b})\ (-1)^{\underline{b}\cdot\underline{j}} .$$

$F(\underline{j})$ *est aussi une fonction réelle dont le domaine est l'ensemble* $E_\beta^k$.

Supposons que $\iota$ soit une variable aléatoire discrète, à valeurs dans l'ensemble $\{0, 1, ---, 2^k-1\}$, dont la loi de probabilité est $P\{\iota=b\}$. Chaque entier b possède un développement binaire tel que celui défini en (3.2). Les coefficients $b_0, b_1, ---, b_{k-1}$ sont considérés comme les réalisations de respectivement k variables aléatoires binaires $\beta_0, \beta_1, ---, \beta_{k-1}$ à valeurs dans l'ensemble $E_\beta$.

On exprime la fonction caractéristique de Walsh $p_j^*$, j entier, $0 \leq j \leq 2^k-1$, comme étant l'espérance mathématique de la grandeur $h(\iota,j)$ définie par (3.1) où l'on a remplacé l'entier b par la variable aléatoire discrète $\iota$:

$$p_j^* = E\{h(\iota,j)\} = \sum_{b=0}^{2^k-1} (-1)^{\sum_{l=0}^{k-1} b_l j_l} P\{\iota = b\} , \qquad (3.6)$$

où les $j_l$ sont les k coefficients du développement binaire de l'entier j, comme défini en (3.2).

Il est évident que:

$$P\{\iota = b\} = P\{\beta_0 = b_0, \beta_1 = b_1, \text{---}, \beta_{k-1} = b_{k-1}\} \tag{3.7}$$

ce qui nous conduit à la définition équivalente de la fonction caractéristique de Walsh:

$$p_j^* = E\{h[(\beta_0, \beta_1, \text{---}, \beta_{k-1}),j]\}. \tag{3.8}$$

Nous voyons donc que $p_j^*$ n'est autre que la transformation de Walsh de la probabilité conjointe $P\{\beta_0 = b_0, \beta_1 = b_1, \text{---}, \beta_{k-1} = b_{k-1}\}$ (définition 3.1).

Définition 3.2:

*On appelle vecteur des probabilités conjointes le vecteur* $P_k$ *dont les composantes sont les probabilités conjointes des k variables aléatoires binaires* $\beta_0$, $\beta_1$, ---, $\beta_{k-1}$ *à valeurs dans l'ensemble* $E_\beta$. *Posons:*

$$p_b = P\{\beta_0 = x_0, \beta_1 = x_1, \text{---}, \beta_{k-1} = x_{k-1}\}$$

*où:*
$$b = \sum_{l=0}^{k-1} b_l 2^{k-1-l}.$$

*Donc:*
$$P_k = [p_0\ p_1\ \text{---}\ p_{2^k-1}]^T.$$

Définition 3.3:

*On appelle vecteur des fonctions caractéristiques de Walsh le vecteur* $P_k^*$ *dont les composantes sont les fonctions caractéristiques de Walsh* $p_j^*$, $0 \leq j \leq 2^k-1$.

*Donc:*
$$P_k^* = [p_0^*\ p_1^*\ \text{---}\ p_{2^k-1}^*]^T.$$

En combinant (3.1) et (3.8) ainsi que les définitions 3.2 et 3.3, nous obtenons:

$$P_k^* = H_k \cdot P_k. \tag{3.9}$$

## III.3. Relation entre probabilités conjointes et moments conjoints.

Nous allons démontrer un théorème important, conjecturé par Shah [50,51], reliant le vecteur des probabilites conjointes au vecteur correspondant des moments conjoints de k variables aléatoires binaires $\xi_0$, $\xi_1$, ---, $\xi_{k-1}$ à valeurs dans l'ensemble $E_\xi$.

Définition 3.4:

*On appelle vecteur des moments conjoints le vecteur* $M_k$ *dont les composantes sont les moments conjoints existant entre k variables aléatoires binaires* $\xi_0$, $\xi_1$, ---, $\xi_{k-1}$ *à valeurs dans l'ensemble* $E_\xi$ *(définition 2.7, voir exemple 2.1).*

En utilisant les définitions 2.2 et 3.2, nous trouvons que:

$$\begin{bmatrix} P_0 \\ P_1 \\ \vdots \\ P_{2^k-1} \end{bmatrix} = \begin{bmatrix} P\{\beta_0 = 0, \text{---}, \beta_{k-1} = 0\} \\ P\{\beta_0 = 0, \text{---}, \beta_{k-1} = 1\} \\ \vdots \\ P\{\beta_0 = 1, \text{---}, \beta_{k-1} = 1\} \end{bmatrix} = \begin{bmatrix} P\{\xi_0 = +1, \text{---}, \xi_{k-1} = +1\} \\ P\{\xi_0 = +1, \text{---}, \xi_{k-1} = -1\} \\ \vdots \\ P\{\xi_0 = -1, \text{---}, \xi_{k-1} = -1\} \end{bmatrix}.$$

Théorème 3.1:

Le vecteur des probabilités conjointes $P_k$ et le vecteur correspondant des moments conjoints $M_k$ de k variables aléatoires binaires, à valeurs dans l'ensemble $E_\xi$, sont reliés par une transformation de Walsh:

$$M_k = H_k \cdot P_k .$$

Démonstration:

Notons d'abord que: $(-1)^{b_l j_l} = (1-2b_l)^{j_l}$ ; $b_l, j_l \in E_\beta$.

Ensuite, grâce à la fonction $L(b_l) = 1-2b_l = x_l$ (définition 2.2), nous constatons que:

$$(-1)^{b_l j_l} = (1-2b_l)^{j_l} = x_l^{j_l} \quad , \quad x_l \in E_\xi. \tag{3.10}$$

Enfin, si $b_l$ est une réalisation de la variable aléatoire binaire $\beta_l$ (à valeurs dans l'ensemble $E_\beta$) et $x_l$ une réalisation de la variable aléatoire binaire $\xi_l$ (à valeurs dans l'ensemble $E_\xi$), alors, en employant (3.8) et (3.10), nous trouvons que:

$$p_j^* = E\{h[(\beta_0, \beta_1, ---, \beta_{k-1}),j]\} = E\left\{(-1)^{\sum_{l=0}^{k-1} \beta_l j_l}\right\} =$$

$$= E\left\{\prod_{l=0}^{k-1} (-1)^{\beta_l j_l}\right\} = E\left\{\prod_{l=0}^{k-1} \xi_l^{j_l}\right\} = m_j \text{ (définition 2.7).}$$

Les deux vecteurs $P_k^*$ et $M_k$ sont donc équivalents.

*CQFD.*

Puisque $\xi_l$ est une variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$, il est évident que:

$$|m_j| \leq 1 \quad , \quad 0 \leq j \leq 2^k-1. \tag{3.11}$$

*Remarque:*

Un processus stochastique est dit gaussien (limitons-nous au cas réel et stationnaire) si toutes les probabilités finies conjointes associées au processus sont des lois de Gauss. Autrement dit, pour tout système fini d'instants $t_0, t_1, ---, t_{k-1}$, la variable k-dimensionnelle $(\gamma_{t_0}, \gamma_{t_1}, ---, \gamma_{t_{k-1}})$ a une distribution de de Gauss. La donnée de la moyenne et de la fonction d'autocorrélation $R_{\gamma\gamma}(|t_i-t_j|)$ détermine de façon unique ce type de distribution [43].

Cela n'est pas vrai, en général, pour une suite aléatoire binaire (bien que ce genre de suite aléatoire semble pourtant très simple). Pour s'en convaincre, il suffit d'examiner le théorème 3.1.

Corollaire 3.1:

$$p_j = \frac{1}{2^k}\ ,\ 0 \leq j \leq 2^k-1 \iff m_j = 0\ ,\ 1 \leq j \leq 2^k-1.$$

Démonstration:

a) *Implication dans le sens* $\Longrightarrow$ *:*

En utilisant le théorème 3.1 ainsi que les relations (3.3) et (3.4), nous obtenons:

$$M_k^T \cdot M_k = 2^k\, P_k^T \cdot P_k.$$

Ainsi:

$$\sum_{j=0}^{2^k-1} m_j^2 = 2^k \sum_{j=0}^{2^k-1} p_j^2 = 2^k \sum_{j=0}^{2^k-1} \left[\frac{1}{2^k}\right]^2 = 1.$$

Donc:

$$m_0^2 + \sum_{j=1}^{2^k-1} m_j^2 = 1.$$

Puisque $m_0 = 1$ et $m_j^2 \geq 0 \Longrightarrow m_j = 0\ ,\ 1 \leq j \leq 2^k-1.$

b) *Implication dans le sens* $\Longleftarrow$ *:*

En utilisant le théorème 3.1 ainsi que la relation (3.4), nous obtenons:

$$P_k = \frac{1}{2^k} H_k \cdot M_k.$$

Ainsi:

$$P_k = \frac{1}{2^k} H_k \cdot \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Nous savons que toute matrice $H_k$ est telle que:

$$H_k = \begin{bmatrix} 1 & & \\ 1 & & \\ | & * & \\ | & & \\ 1 & & \end{bmatrix}.$$

Donc:

$$P_k = \frac{1}{2^k}\begin{bmatrix} 1 & & \\ 1 & & \\ | & * & \\ | & & \\ 1 & & \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ | \\ | \\ 0 \end{bmatrix} = \frac{1}{2^k}\begin{bmatrix} 1 \\ 1 \\ | \\ | \\ 1 \end{bmatrix}.$$

CQFD.

Définition 3.5:

*On appelle vecteur k-équiprobable tout vecteur des probabilités conjointes tel que:*

$$P_k = [\frac{1}{2^k} \quad \frac{1}{2^k} \quad \text{---} \quad \frac{1}{2^k}]^T.$$

Considérons la fonction caractéristique de Walsh donnée par la relation (3.6) et définissons un ensemble J tel que:

$$J = \left\{ j \mid \sum_{l=0}^{k-1} j_l = \text{un nombre impair} \right\}, \text{ cardinal de J: } |J| = 2^{k-1}.$$

Supposons que les composantes du vecteur des probabilités conjointes (définition 3.2) soient telles que:

$$p_b = p_{2^k-1}, \quad 0 \leq b \leq 2^k-1,$$

ou de manière équivalente:

$$P\{\beta_0 = b_0, \text{---}, \beta_{k-1} = b_{k-1}\} = P\{\beta_0 = \overline{b}_0, \text{---}, \beta_{k-1} = \overline{b}_{k-1}\}$$

pour toute réalisation $(b_0, \text{---}, b_{k-1}) \in E_\beta^k$, $\overline{b}_1$ étant l'inverse de $b_1$ (voir table 2.1).

Si $m_j$ est une composante du vecteur des moments conjoints (définition 3.4), alors:

Corollaire 3.2:

$$p_b = p_{2^k-1-b}, \quad 0 \leq b \leq 2^k-1 \Longleftrightarrow m_j = 0 \quad \text{pour tout } j \in J.$$

Démonstration:

*a) Implication dans le sens $\Longrightarrow$ :*

Le théorème 3.1 implique:

$$m_j = \sum_{(b_0, \text{---}, b_{k-1}) \in E_\beta^k} (-1)^{\sum_{l=0}^{k-1} b_l j_l} P\{\beta_0 = b_0, \text{---}, \beta_{k-1} = b_{k-1}\},$$

où les $j_l$ sont les k coefficients du développement binaire de l'entier j, comme défini en (3.2).

Décomposons cette somme en deux parties et posons (pour simplifier la notation) $\underline{b}' = (b_1, \text{---}, b_{k-1})$:

$$m_j = \sum_{\underline{b}' \in E_\beta^{k-1}} \left\{ (-1)^{\sum_{l=1}^{k-1} b_l j_l} P\{\beta_0 = 0, \beta_1 = b_1, \text{---}, \beta_{k-1} = b_{k-1}\} + \right.$$

$$\left. + (-1)^{j_0 + \sum_{l=1}^{k-1} \overline{b}_l j_l} P\{\beta_0 = 1, \beta_1 = \overline{b}_1, \text{---}, \beta_{k-1} = \overline{b}_{k-1}\} \right\}.$$

Puisque $\bar{b}_l = 1-b_l$ et $(-1)^{\sum_{l=0}^{k-1} b_l j_l} = (-1)^{-\sum_{l=0}^{k-1} b_l j_l}$, nous obtenons:

$$m_j = \sum_{\underline{b}' \in E_\beta^{k-1}} (-1)^{\sum_{l=1}^{k-1} b_l j_l} \left\{1 + (-1)^{\sum_{l=0}^{k-1} j_l}\right\} \cdot$$

$$\cdot P\{\beta_0 = 0, \beta_1 = b_1, ---, \beta_{k-1} = b_{k-1}\}.$$

Nous constatons donc que $m_j = 0$ pour tout $j \in J$.

b) *Implication dans le sens* $\Longleftarrow$:

Pour tout $j \in J$, nous avons:

$$m_j = \sum_{(b_0, ---, b_{k-1}) \in E_\beta^k} (-1)^{\sum_{l=0}^{k-1} b_l j_l} P\{\beta_0 = b_0, ---, \beta_{k-1} = b_{k-1}\} = 0.$$

Décomposons cette somme en deux parties:

$$m_j = \sum_{\underline{b}' \in E_\beta^{k-1}} \left\{(-1)^{\sum_{l=1}^{k-1} b_l j_l} P\{\beta_0 = 0, \beta_1 = b_1, ---, \beta_{k-1} = b_{k-1}\} + \right.$$

$$\left. + (-1)^{j_0 + \sum_{l=1}^{k-1} \bar{b}_l j_l} P\{\beta_0 = 1, \beta_1 = \bar{b}_1, ---, \beta_{k-1} = \bar{b}_{k-1}\}\right\} = 0.$$

Par Hypothèse, $(-1)^{\sum_{l=0}^{k-1} j_l} = -1$. Ainsi:

$$\sum_{\underline{b}' \in E_\beta^{k-1}} (-1)^{\sum_{l=1}^{k-1} b_l j_l} \left\{ P\{\beta_0 = 0, \beta_1 = b_1, \ldots, \beta_{k-1} = b_{k-1}\} - \right.$$

$$\left. - P\{\beta_0 = 1, \beta_1 = \bar{b}_1, \ldots, \beta_{k-1} = \bar{b}_{k-1}\} \right\} = 0.$$

L'expression ci-dessus doit être vraie pour tout $j \in J$. En l'écrivant sous forme matricielle, nous obtenons (puisque $|J| = 2^{k-1}$):

$$H_{k-1} \cdot P'_{k-1} = 0 \tag{3.12}$$

où:

$$P'_{k-1} = \begin{bmatrix} P\{\beta_0 = 0, \beta_1 = 0, \ldots, \beta_{k-1} = 0\} - P\{\beta_0 = 1, \beta_1 = 1, \ldots, \beta_{k-1} = 1\} \\ P\{\beta_0 = 0, \beta_1 = 0, \ldots, \beta_{k-1} = 1\} - P\{\beta_0 = 1, \beta_1 = 1, \ldots, \beta_{k-1} = 0\} \\ \vdots \\ P\{\beta_0 = 0, \beta_1 = 1, \ldots, \beta_{k-1} = 1\} - P\{\beta_0 = 1, \beta_1 = 0, \ldots, \beta_{k-1} = 0\} \end{bmatrix}.$$

En utilisant la relation (3.5) ainsi que le théorème [5]:

$$\left.\begin{array}{l} A: \text{matrice } n \times n \\ B: \text{matrice } m \times m \end{array}\right\} \Longrightarrow \det(A \odot B) = (\det A)^m \, (\det B)^n,$$

nous trouvons que:

$$\det H_{k-1} \neq 0 \quad \text{puisque} \quad \det H_1 = -2.$$

L'unique solution du système (3.12) est donc la suivante:

$$P\{\beta_0 = b_0, \ldots, \beta_{k-1} = b_{k-1}\} = P\{\beta_0 = \bar{b}_0, \ldots, \beta_{k-1} = \bar{b}_{k-1}\}.$$

CQFD.

Définition 3.6:

*On appelle vecteur des probabilités conjointes symétrique tout vecteur des probabilités conjointes, associé à k variables aléatoires binaires, dont les composantes sont telles que:*

$$p_b = p_{2^k-1-b} \quad , \quad 0 \leq b \leq 2^k - 1 \quad \textit{(définition 3.2)}.$$

En mots, la signification du corollaire 3.2 est la suivante:

Vecteur des probabilités conjointes symétrique. $\Longleftrightarrow$ Les moments d'ordre impair (composantes du vecteur des moments conjoints correspondant) sont nuls.

Exemple 3.2:

Considérons le cas de trois variables aléatoires binaires $\xi_0$, $\xi_1$, $\xi_2$, à valeurs dans l'ensemble $E_\xi$, dont le vecteur des probabilités conjointes est symétrique.

Alors:

$$P_3 = \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \\ p_3 \\ p_2 \\ p_1 \\ p_0 \end{bmatrix} \Longleftrightarrow M_3 = \begin{bmatrix} 1 \\ m_{\xi_2} \\ m_{\xi_1} \\ m_{\xi_1\xi_2} \\ m_{\xi_2} \\ m_{\xi_0\xi_2} \\ m_{\xi_1\xi_2} \\ m_{\xi_0\xi_1\xi_2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 2(p_0-p_1-p_2+p_3) \\ 0 \\ 2(p_0-p_1+p_2-p_3) \\ 2(p_0+p_1-p_2-p_3) \\ 0 \end{bmatrix}.$$

III.4. Indépendance statistique.

Rappelons que k variables aléatoires discrètes sont statistiquement indépendantes si leur probabilité conjointe est la probabilité produit de leurs probabilités respectives [43].

Dans le cadre des variables aléatoires binaires, l'indépendance statistique (définition 2.6) peut être étendue par le théorème suivant:

Théorème 3.2:

Soient k variables aléatoires binaires $\xi_0, \xi_1, ---, \xi_{k-1}$ à valeurs dans l'ensemble $E_\xi$. Alors:

$$\left.\begin{array}{l} P\{\xi_0 = x_0, ---, \xi_{k-1} = x_{k-1}\} = \\ = \prod_{l=0}^{k-1} P\{\xi_l = x_l\} \end{array}\right\} \Longleftrightarrow \left\{\begin{array}{l} E\{\xi_0^{d_0} \cdot --- \cdot \xi_{k-1}^{d_{k-1}}\} = \prod_{l=0}^{k-1} E\{\xi_l^{d_l}\}, \\ \text{pour tout } (d_0, ---, d_{k-1}) \in E_\beta^k. \end{array}\right.$$

Démonstration:

a) *Implication dans le sens* $\Longrightarrow$ :

Cette partie de la démonstration est évidente.

b) *Implication dans le sens* $\Longleftarrow$ :

En utilisant le théorème 3.1 ainsi que la relation (3.4), nous obtenons:

$$P_k = \frac{1}{2^k} H_k \cdot M_k.$$

Puisque, par hypothèse, chaque composante du vecteur des moments conjoints s'exprime comme produit de moments du premier ordre, alors:

$$M_k = \bigotimes_{l=0}^{k-1} \begin{bmatrix} 1 \\ m_{\xi_l} \end{bmatrix} = \bigotimes_{l=0}^{k-1} M_{1_l}, \quad \text{où:} \quad \bigotimes_{l=0}^{k-1} A_l = A_0 \otimes --- \otimes A_{k-1}.$$

Nous savons aussi, par la relation (3.5), que:

$$H_k = \bigotimes_{l=0}^{k-1} H_1 .$$

Ainsi:

$$P_k = \frac{1}{2^k}\left\{\bigotimes_{l=0}^{k-1} H_1\right\}\cdot\left\{\bigotimes_{l=0}^{k-1} M_1\right\}. \qquad (3.13)$$

En utilisant la loi du produit mixte [8] en plus du théorème 3.1, la relation (3.13) devient:

$$P_k = \bigotimes_{l=0}^{k-1} \frac{1}{2} H_1 \cdot M_1 = \bigotimes_{l=0}^{k-1} P_1 , \qquad (3.14)$$

où $P_1 = [P\{\xi_1 = +1\} \;\; P\{\xi_1 = -1\}]^T$. Ainsi, chaque composante du vecteur des probabilités conjointes $P_k$ s'exprime comme suit:

$$P\{\xi_0 = x_0, \text{---}, \xi_{k-1} = x_{k-1}\} = \prod_{l=0}^{k-1} P\{\xi_l = x_l\}.$$

*CQFD.*

Exemple 3.3:

Considérons deux variables aléatoires binaires $\xi_0$ , $\xi_1$ à valeurs dans l'ensemble $E_\xi$. Par le théorème 3.1, nous avons:

$$\begin{bmatrix} 1 \\ m_{\xi_1} \\ m_{\xi_0} \\ m_{\xi_0\xi_1} \end{bmatrix} = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix} \cdot \begin{bmatrix} P\{\xi_0 = +1, \xi_1 = +1\} \\ P\{\xi_0 = +1, \xi_1 = -1\} \\ P\{\xi_0 = -1, \xi_1 = +1\} \\ P\{\xi_0 = -1, \xi_1 = -1\} \end{bmatrix}.$$

Si $m_{\xi_0\xi_1} = m_{\xi_0}\, m_{\xi_1}$, alors:

$$\begin{bmatrix} 1 \\ m_{\xi_1} \\ m_{\xi_0} \\ m_{\xi_0\xi_1} \end{bmatrix} = \begin{bmatrix} 1 \\ m_{\xi_0} \end{bmatrix} \circledast \begin{bmatrix} 1 \\ m_{\xi_1} \end{bmatrix}.$$

Ici, en applicant la relation (3.14), nous obtenons:

$$\begin{bmatrix} P\{\xi_0 = +1,\ \xi_1 = +1\} \\ P\{\xi_0 = +1,\ \xi_1 = -1\} \\ P\{\xi_0 = -1,\ \xi_1 = +1\} \\ P\{\xi_0 = -1,\ \xi_1 = -1\} \end{bmatrix} = \begin{bmatrix} P\{\xi_0 = +1\} \\ P\{\xi_0 = -1\} \end{bmatrix} \circledast \begin{bmatrix} P\{\xi_1 = +1\} \\ P\{\xi_1 = -1\} \end{bmatrix} =$$

$$= \begin{bmatrix} P\{\xi_0 = +1\}\ P\{\xi_1 = +1\} \\ P\{\xi_0 = +1\}\ P\{\xi_1 = -1\} \\ P\{\xi_0 = -1\}\ P\{\xi_1 = +1\} \\ P\{\xi_0 = -1\}\ P\{\xi_1 = -1\} \end{bmatrix}.$$

Les variables aléatoires $\xi_0$ et $\xi_1$ sont donc indépendantes (suivant la définition 2.6).

Définition 3.7:

*Nous dirons que k variables aléatoires binaires sont k-non corrélées si:*

$$E\{\chi_{i_0} \cdot \chi_{i_1} \cdot \text{---} \cdot \chi_{i_{m-1}}\} = \prod_{l=0}^{m-1} E\{\chi_{i_l}\}$$

*pour tout* $0 \leq i_0 < \text{---} < i_{m-1} \leq k-1$ *et* $1 \leq m \leq k$.

*Lorsque k = 2, nous dirons simplement qu'elles sont non corrélées.*

Nous constatons donc que dans le cas de k variables aléatoires binaires, leur k-non corrélation est équivalente à leur indépendance.

Bien que cela soit aussi vrai pour k variables aléatoires gaussiennes (leur matrice de covariance est diagonale) [e.g. 46], la k-non corrélation n'est pas équivalente à l'indépendance pour d'autres types de variables aléatoires (voir les contre-exemples données dans [57 p. 169], [46 p. 212] et [18 p. 236]).

Notons que si k variables aléatoires sont indépendantes, elles sont toujours k-non corrélées.

Corollaire 3.3:

Soient k variables aléatoires binaires indépendantes $\xi_0, \xi_1, ---, \xi_{k-1}$ à valeurs dans l'ensemble $E_\xi$. Soit $\xi$ une variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$.
Alors, $\xi, \xi_0, \xi_1, ---, \xi_{k-1}$ sont indépendantes si et seulement si $\xi$ est indépendante du produit $\xi_0^{d_0}.\xi_1^{d_1}. --- .\xi_{k-1}^{d_{k-1}}$ pour tout $(d_0, ---, d_{k-1}) \in E_\beta^k$.

Démonstration:

Immédiate par le théorème 3.2.

*CQFD.*

*Remarque:*

Xiao et Massey [60] démontrent le lemme suivant: $\chi$ est une variable aléatoire discrète, $\xi_0, \xi_1, ---, \xi_{k-1}$ sont k variables aléatoires binaires indépendantes à valeurs dans l'ensemble $E_\xi$ et $P\{\xi_l = +1\} = 0.5$, $0 \leq l \leq k-1$. Alors, $\chi, \xi_0, \xi_1, ---, \xi_{k-1}$ sont indépendantes si et seulement si $\chi$ est indépendante du produit $\xi_0^{d_0}.\xi_1^{d_1}. --- .\xi_{k-1}^{d_{k-1}}$ pour tout $(d_0, ---, d_{k-1}) \in E_\xi^k$.

Le corollaire 3.3 est une généralisation de ce lemme lorsque $\chi$ est une variable aléatoire binaire.

## III.5. Fonction d'autocorrélation d'une suite aléatoire binaire.

La fonction d'autocorrélation joue un rôle fondamental dans l'étude des systèmes physiques perturbés par du bruit [e.g. 6]. Elle est largement utilisée dans les domaines tels que la théorie des communications [e.g. 59] ou les systèmes linéaires en général [e.g. 4,31].

Nous donnerons ici quelques propriétés de la fonction d'autocorrélation $R_{\xi\xi}(\nu)$ d'une suite aléatoire binaire $\Xi = \{\xi(n)\}$, $\xi(n)$ étant une variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$.

Notons qu'une telle suite ne peut pas générer n'importe quelle fonction d'autocorrélation. Aussi, il est possible de définir une classe U contenant toutes celles ainsi générées.

Les éléments de la classe U ont les propriétés suivantes [38,39]:

a) Si $R_{1\xi\xi}(\nu)$, $R_{2\xi\xi}(\nu) \in U$, alors $R_{1\xi\xi}(\nu)\cdot R_{2\xi\xi}(\nu) \in U$ et $a\cdot R_{1\xi\xi}(\nu) + (1-a)\cdot R_{2\xi\xi}(\nu) \in U$ pour tout $a \in [0,1]$.

b) Si $R_{k\xi\xi}(\nu) \in U$, $k \in N$, et $\lim_{k \to \infty} R_{k\xi\xi}(\nu) = R_{\xi\xi}(\nu)$ pour tout $\nu \in N$ alors $R_{\xi\xi}(\nu) \in U$.

c) $R_{\xi\xi}(\nu) \in U$ si et seulement si $R_{\xi\xi}(0) = 1$ et $R_{\xi\xi}(\nu) = R_{\xi\xi}(-\nu)$ avec $|R_{\xi\xi}(\nu)| \leq R_{\xi\xi}(0)$.

Examinons maintenant la relation existant entre la fonction d'autocorrélation $R_{\xi\xi}(\nu)$ d'une suite aléatoire binaire $\Xi = \{\xi(n)\}$ et la probabilité $P\{\xi(n) = +1\}$.

En utilisant le théorème 3.1, nous montrons facilement que:

$$R_{\xi\xi}(\nu) = P\{\xi(n) = +1,\ \xi(n+\nu) = +1\} - P\{\xi(n) = +1,\ \xi(n+\nu) = -1\} - P\{\xi(n) = -1,\ \xi(n+\nu) = +1\} + P\{\xi(n) = -1,\ \xi(n+\nu) = -1\}. \quad (3.15)$$

La relation (3.15) peut s'écrire sous la forme:

$$\left.\begin{aligned} R_{\xi\xi}(\nu) &= 1 - 4\,P\{\xi(n) = +1\} + 4\,P\{\xi(n) = +1,\ \xi(n+\nu) = +1\}, \\ R_{\xi\xi}(\nu) &= 1 - 4\,P\{\xi(n) = +1,\ \xi(n+\nu) = -1\} = \\ &= 1 - 4\,P\{\xi(n) = -1,\ \xi(n+\nu) = +1\}, \\ R_{\xi\xi}(\nu) &= -3 + 4\,P\{\xi(n) = +1\} + 4\,P\{\xi(n) = -1,\ \xi(n+\nu) = -1\}. \end{aligned}\right\} \quad (3.16)$$

Considérons les probabilités conjointes $P\{\xi(n) = x_n,\ \xi(n+\nu) = x_{n+\nu}\}$ comme des paramètres.

Théorème 3.3:

Soit $R_{\xi\xi}(\nu)$ la fonction d'autocorrélation de la suite aléatoire binaire $\Xi = \{\xi(n)\}$. Alors, le domaine de définition de $R_{\xi\xi}(\nu)$ comme fonction de la probabilité $P\{\xi(n) = +1\}$ correspond au triangle (dans $R^2$) dont les sommets sont donnés par les points (0,1), (0.5,-1) et (1,1).

Démonstration:

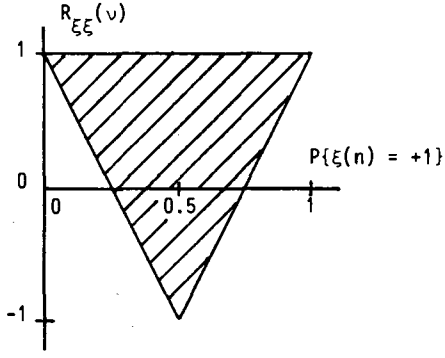
Les relations (3.11)' et (3.16) nous conduisent aux inégalités suivantes:

$$-1 \leq 1 - 4\ P\{\xi(n) = +1\} \leq R_{\xi\xi}(\nu) \leq 5 - 4\ P\{\xi(n) = +1\} \leq 1,$$

$$-1 \leq R_{\xi\xi}(\nu) \leq 1,$$

$$-1 \leq -3 + 4\ P\{\xi(n) = +1\} \leq R_{\xi\xi}(\nu) \leq 1 + 4\ P\{\xi(n) = +1\} \leq 1.$$

Puisque ces trois inégalités doivent être satisfaites simultanément, le domaine cherché est donc le suivant:




Il est facile de constater que les points (0,1), (0.5,-1) et (1,1) peuvent être atteints. Ainsi, puisque la classe U est convexe (propriété a), tous les points du domaine sont atteignables.

CQFD.

III.6. Produit de suites aléatoires binaires indépendantes: théorème limite.

Considérons k suites aléatoires binaires indépendantes $\Xi_0 = \{\xi_0(n)\}$, $\Xi_1 = \{\xi_1(n)\}$, ---, $\Xi_{k-1} = \{\xi_{k-1}(n)\}$, $\xi_0(n)$, $\xi_1(n)$, ---, $\xi_{k-1}(n)$ étant k variables aléatoires binaires à valeurs dans l'ensemble $E_\xi$.

Construisons une nouvelle suite aléatoire binaire $z = \{\zeta(n)\}$ telle que (Fig. 3.1):

$$z = \{\zeta(n)\} = \{\xi_0(n)\cdot\xi_1(n)\cdot \text{ --- } \cdot\xi_{k-1}(n)\}.$$

$\zeta(n)$ est donc aussi une variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$.

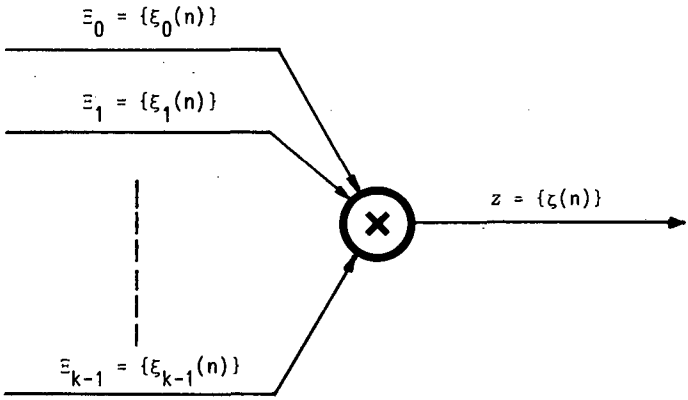



*Fig. 3.1: Produit de k suites aléatoires binaires indépendantes.*

Posons : $\tilde{\nu}_1 = \nu_1+\nu_2+ \text{ --- } +\nu_1$.

Appelons respectivement $P_i(\Xi_1)$ et $P_i(z)$ les vecteurs des probabilités conjointes de i variables aléatoires binaires $\xi_1(n)$, $\xi_1(n+\tilde{\nu}_1)$, ---, $\xi_1(n+\tilde{\nu}_{i-1})$ et $\zeta(n)$, $\zeta(n+\tilde{\nu}_1)$, ---, $\zeta(n+\tilde{\nu}_{i-1})$ tirées des suites aléatoires binaires $\Xi_1$, $0 \leq 1 \leq k-1$, et z.

Définition 3.8:

*Soient deux matrices* $n \times m$, $A = [a_{ij}]$ et $B = [b_{ij}]$. *Leur produit de Schur est défini comme suit [31]:*

$$A \circ B = [a_{ij} b_{ij}].$$

Par exemple, pour deux vecteurs:

$$x \circ y = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{bmatrix} \circ \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{k-1} \end{bmatrix} = \begin{bmatrix} x_0 y_0 \\ x_1 y_1 \\ \vdots \\ x_{k-1} y_{k-1} \end{bmatrix}.$$

Théorème 3.4:

Les vecteurs des probabilités conjointes $P_i(z)$ et $P_i(\Xi_l)$, $0 \leq l \leq k-1$, sont liés par la relation:

$$P_i(z) = \frac{1}{2^i} H_i \cdot \left\{ \bigodot_{l=0}^{k-1} H_i \cdot P_i(\Xi_l) \right\}, \text{ pour tout entier } i,$$

où $\bigodot_{l=0}^{k-1} H_i \cdot P_i(\Xi_l)$ représente le produit de Schur des k vecteurs $H_i \cdot P_i(\Xi_l)$.

Démonstration:

Les k suites aléatoires binaires $\Xi_0$, $\Xi_1$, ---, $\Xi_{k-1}$ sont indépendantes, alors:

$$M_i(z) = \bigodot_{l=0}^{k-1} M_i(\Xi_l), \tag{3.17}$$

où $M_i(\Xi_l)$ et $M_i(z)$ sont respectivement les vecteurs des moments conjoints des i variables aléatoires binaires $\xi_l(n)$, $\xi_l(n+\tilde{v}_1)$, ---, $\xi_l(n+\tilde{v}_{i-1})$ et $\zeta(n)$, $\zeta(n+\tilde{v}_1)$, ---, $\zeta(n+\tilde{v}_{i-1})$ tirées des suites aléatoires binaires $\Xi_l$, $0 \leq l \leq k-1$, et $z$.

En applicant le théorème 3.1 ainsi que les relations (3.4) et (3.17), nous obtenons:

$$P_i(z) = \frac{1}{2^i} H_i \cdot \left\{ \prod_{l=0}^{k-1} H_i \cdot P_i(\Xi_l) \right\}.$$

*CQFD.*

Corollaire 3.4:

Si pour tout $i \in N$, un des vecteurs des probabilités conjointes $P_i(\Xi_l)$, $0 \leq l \leq k-1$, est un vecteur k-équiprobable (définition 3.5), alors $P_i(z)$ est aussi un vecteur k-équiprobable.

Démonstration:

Immédiate par le théorème 3.4 et le corollaire 3.1.

*CQFD.*

Corollaire 3.5:

Si pour tout $i \in N$, un des vecteurs des probabilités conjointes $P_i(\Xi_l)$, $0 \leq l \leq k-1$, est un vecteur des probabilités conjointes symétrique (définition 3.6), alors $P_i(z)$ est aussi un vecteur des probabilités conjointes symétrique.

Démonstration:

Immédiate par le théorème 3.4 et le corollaire 3.2.

*CQFD.*

*Théorème limite.*

Supposons que le nombre k de suites aléatoires binaires indépendantes $\Xi_l$ augmente indéfiniment.

Le vecteur des probabilités conjointes $P_i(z)$ tend alors, sous certaines conditions, vers une limite comme le montre le théorème suivant:

Théorème 3.5:

Si toute composante $m_j(\Xi_l)$ des vecteurs des moments conjoints $M_i(\Xi_l)$, $l \in N$, est telle que:

$$|m_j(\Xi_l)| < R < 1, \quad 1 \leq j \leq 2^i - 1,$$

alors:

$$\lim_{k \to \infty} P_i(z) = \frac{1}{2^i} e_i, \text{ pour tout entier } i,$$

où $e_i = [1\ 1\ \text{---}\ 1]^T$ est un vecteur $2^i \times 1$.

Démonstration:

Toutes les suites aléatoires binaires $\Xi_l$, $l \in N$, sont indépendantes. Donc, par hypothèse, nous obtenons:

$$\lim_{k \to \infty} |M_i(z)| < \lim_{k \to \infty} \begin{bmatrix} 1 \\ R^k \\ \vdots \\ R^k \end{bmatrix}. \tag{3.18}$$

Mais, R est, par hypothèse, strictement plus petit que un. En passant à la limite, (3.18) devient:

$$\lim_{k \to \infty} |M_i(z)| = [1\ 0\ \text{---}\ 0]^T. \tag{3.19}$$

En utilisant (3.19) ainsi que le corollaire 3.1, nous obtenons le résultat cherché:

$$\lim_{k \to \infty} P_i(z) = \frac{1}{2^i} [1\ 1\ \text{---}\ 1]^T = \frac{1}{2^i} e_i,$$

et ceci pour tout entier i.

*CQFD.*

Notons que la contrainte du théorème 3.5 n'est pas trop restrictive puisque nous savons, par la relation (3.11), que $|m_j(\Xi_1)| \leq 1$, $1 \leq j \leq 2^i-1$, $1 \in N$.

*Remarque:*

La conclusion du théorème 3.5 est aussi vraie si nous relâchons légèrement la contrainte qu'il contient en admettant, lorsque k augmente indéfiniment, qu'un nombre fini de composantes $m_j(\Xi_1)$, $1 \leq j \leq 2^i-1$, $1 \in N$, valent plus ou moins un. En effet, si:

$$Q_j = \{m_j(\Xi_1) \mid |m_j(\Xi_1)| = 1,\ j \text{ fixe}\},\quad c_j = |Q_j| < \infty.$$

L'inégalité (3.18) devient ici (en groupant toutes les composantes $m_j(\Xi_1) \in Q_j$):

$$\lim_{k \to \infty} |M_i(z)| < \lim_{k \to \infty} \begin{bmatrix} 1 \\ R^{k-c_1} \\ \vdots \\ R^{k-c_{2^i-1}} \end{bmatrix}.$$

En passant à la limite, nous retrouvons la relation (3.19).

Le théorème 3.5 signifie que le vecteur des probabilités conjointes de i variables aléatoires binaires tirées d'une suite aléatoire binaire produit de k suites aléatoires binaires indépendantes converge vers un vecteur i-équiprobable pour k tendant vers l'infini.

Le fait de relâcher légèrement la contrainte dudit théorème nous permet, sans y modifier sa conclusion, d'inclure dans la multiplication un nombre fini de suites déterministes (comme par exemple les suites binaires pseudo-aléatoires).

Le théorème 3.5 généralise le théorème 3 démontré par Fire [19] qui ne considère que la loi de probabilité limite d'une variable aléatoire binaire résultant de la multiplication de variables aléatoires binaires indépendantes et identiquement distribuées.

Exemple 3.4:

Examinons le cas où i = 1 et les variables aléatoires binaires $\xi_0(n)$, $\xi_1(n)$, ---, $\xi_{k-1}(n)$, --- sont indépendantes et identiquement distribuées.

Posons:

$$P\{\xi_1(n) = +1\} = p, \; 1 \in N.$$

La contrainte du théorème 3.5 devient ici (théorème 3.1):

$$0 < 0.5(1-R) < p < 0.5(1+R) < 1. \tag{3.20}$$

Considérons les k premières variables aléatoires binaires $\xi_0(n)$, $\xi_1(n)$, ---, $\xi_{k-1}(n)$. En utilisant le théorème 3.4, nous obtenons:

$$\begin{bmatrix} P\{\zeta(n) = +1\} \\ \\ P\{\zeta(n) = -1\} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 + \prod_{1=0}^{k-1} (2P\{\xi_1(n) = +1\} - 1) \\ \\ 1 - \prod_{1=0}^{k-1} (2P\{\xi_1(n) = +1\} - 1) \end{bmatrix} =$$

$$= \frac{1}{2} \begin{bmatrix} 1 + (2p-1)^k \\ \\ 1 - (2p-1)^k \end{bmatrix}. \tag{3.21}$$

Les relations (3.20) et (3.21) nous conduisent à l'inégalité suivante:

$$\frac{1}{2} \begin{bmatrix} 1-R^k \\ \\ 1-R^k \end{bmatrix} < \begin{bmatrix} P\{\zeta(n) = +1\} \\ \\ P\{\zeta(n) = -1\} \end{bmatrix} < \frac{1}{2} \begin{bmatrix} 1+R^k \\ \\ 1+R^k \end{bmatrix}.$$

Mais, R est strictement plus petit que un. Donc, en passant à la limite, nous obtenons ($P\{\zeta(n) = z_n\} \geq 0$):

$$\lim_{k \to \infty} \begin{bmatrix} P\{\zeta(n) = +1\} \\ \\ P\{\zeta(n) = -1\} \end{bmatrix} = \begin{bmatrix} 0.5 \\ \\ 0.5 \end{bmatrix}.$$

La figure 3.2 illustre les variations de la probabilité $P\{\zeta(n) = +1\}$ en fonction de p et k suivant la relation (3.21).

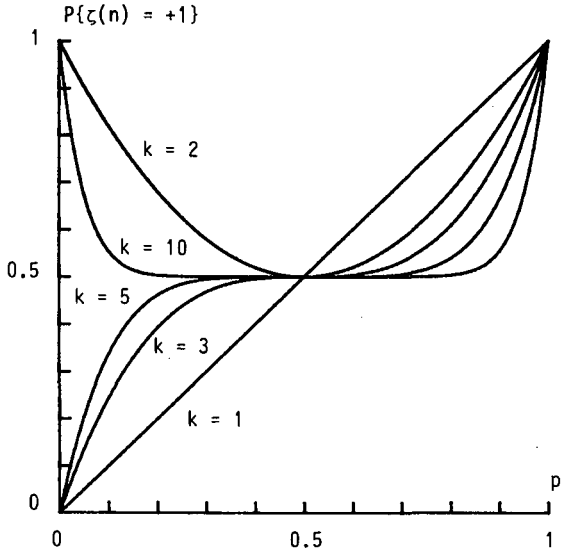



*Fig. 3.2: Variations de $P\{\zeta(n) = +1\}$ en fonction de p et k.*

III.7. Sous-classe particulière de suites aléatoires binaires.

Nous avons vu (théorème 3.1) qu'il n'est pas possible, en général, de déterminer de façon unique les caractéristiques statistiques d'une suite aléatoire binaire si nous n'avons à disposition qu'un nombre limité de moments conjoints.

Cette propriété n'est donc pas faite pour faciliter l'étude de telles suites.

Ainsi, essayons de délimiter une sous-classe PP de suites aléatoires binaires dont les moments conjoints d'ordre k, k = 4, 6, ---, de chacun de ses membres ne soient fonction que de leurs moments conjoints du second ordre (les moments conjoints d'ordre impair pouvant être annulés en ne considérant que les vecteurs des probabilités conjointes symétriques, voir corollaire 3.2).

Nous lui demandons, en plus, d'avoir la propriété suivante:

Si $\Xi = \{\xi(n)\}$ et $H = \{\eta(n)\}$ sont deux suites aléatoires binaires indépendantes appartenant à PP, alors $z = \{\zeta(n)\} = \{\xi(n)\cdot\eta(n)\}$ appartient aussi à PP, $\xi(n)$, $\eta(n)$ et $\zeta(n)$ sont des variables aléatoires binaires à valeurs dans l'ensemble $E_\xi$.

Nous proposons cette condition parce que la multiplication de deux variables aléatoires binaires à valeurs dans l'ensemble $E_\xi$ correspond à la somme modulo 2 de deux variables aléatoires binaires à valeurs dans l'ensemble $E_\beta$ ( voir table 2.1). Nous avons donc affaire à une opération linéaire dans GF(2), celle-ci étant très utilisée en pratique.

Examinons donc quelles sont les formes possibles des composantes du vecteur des moments conjoints $M_k$ de k variables aléatoires binaires tirées d'une suite aléatoire binaire quelconque appartenant à la sous-classe PP.

Commençons par l'étude du moment conjoint d'ordre quatre. on peut définir entre quatre variables aléatoires binaires, six moments conjoints d'ordre deux (Fig. 3.3).

Pour simplifier la notation, posons : $\chi(n+\tilde{\nu}_i) = \chi_i$ où $\tilde{\nu}_i = \nu_1 + \nu_2 + \text{---} + \nu_i$, $\chi(n)$ étant une variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$.

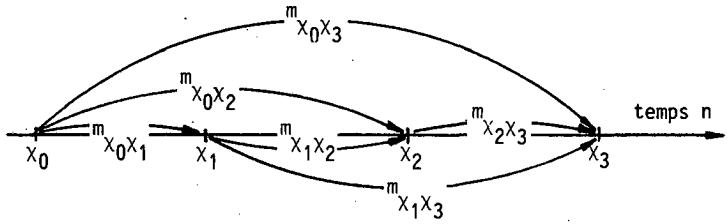



*Fig. 3.3: Définition des six moments d'ordre deux existant entre quatre variables aléatoires binaires.*

Soient deux suites aléatoires binaires $\Xi = \{\xi(n)\}$ et $H = \{\eta(n)\}$ indépendantes appartenant à la sous-classe PP. Si $z = \{\zeta(n)\} = \{\xi(n)\cdot\eta(n)\}$, alors:

$$m_{\zeta_i\zeta_j} = m_{\xi_i\xi_j} m_{\eta_i\eta_j} \quad ; \; i,j = 0, 1, 2, 3, \; i < j, \tag{3.22}$$

$$m_{\zeta_0\zeta_1\zeta_2\zeta_3} = m_{\xi_0\xi_1\xi_2\xi_3} m_{\eta_0\eta_1\eta_2\eta_3}. \tag{3.23}$$

Par définition, le moment conjoint d'ordre quatre de toute suite aléatoire binaire appartenant à la sous-classe PP est une fonction f de ses six moments conjoints d'ordre deux. Donc, les relations (3.22) et (3.23) nous conduisent à:

$$f(m_{\xi_0\xi_1} m_{\eta_0\eta_1}, m_{\xi_0\xi_2} m_{\eta_0\eta_2}, \text{---}, m_{\xi_2\xi_3} m_{\eta_2\eta_3}) =$$

$$= f(m_{\xi_0\xi_1}, m_{\xi_0\xi_2}, \text{---}, m_{\xi_2\xi_3}) \cdot f(m_{\eta_0\eta_1}, m_{\eta_0\eta_2}, \text{---}, m_{\eta_2\eta_3}). \tag{3.24}$$

Nous avons affaire à une équation fonctionnelle. En admettant que f soit une fonction réelle continue, les solutions de (3.24) sont les fonctions produit de fonctions du type (voir appendice A):

$$\left.\begin{aligned} &f(m_{\xi_i\xi_j}) = |m_{\xi_i\xi_j}|^{c_{ij}}, \; c_{ij} \geq 0, \\ &f(m_{\xi_i\xi_j}) = |m_{\xi_i\xi_j}|^{c_{ij}} \cdot \text{signe}(m_{\xi_i\xi_j}), \; c_{ij} > 0 \; (\text{signe}(0) = 0), \\ &f(m_{\xi_i\xi_j}) = 0, \\ &c_{ij}: \text{ constantes réelles.} \end{aligned}\right\} \tag{3.25}$$

La généralisation du résultat précédent à tout ordre k, k = 6, 8, ---, est immédiate. Les équations fonctionnelles résultantes sont analogues à celles décrites par (3.24). Leurs solutions sont les fonctions produit de fonctions du type (3.25).

Exemple 3.5:

1) Les suites de Bernoulli (définition 2.13) font partie de la sous-classe PP puisque pour tout nombre k de variables aléatoires binaires $\chi_0$, $\chi_1$, ---, $\chi_{k-1}$, à valeurs dans l'ensemble $E_\xi$, nous avons:

$$E\{\chi_0\chi_1 \text{ --- } \chi_{k-1}\} = [E\{\chi\}]^k,$$

où $E\{\chi\} = E\{\chi_l\}$, $0 \leq l \leq k-1$, représente la moyenne de la suite en question.

2) Nous verrons au chapitre IV que le moment conjoint d'ordre k, k pair, d'une chaîne de Markov binaire du premier ordre avec matrice des probabilités de transition doublement stochastique est donné par:

$$E\{\chi_0\chi_1 \text{ --- } \chi_{k-1}\} = E\{\chi_0\chi_1\}E\{\chi_2\chi_3\} \text{ --- } E\{\chi_{k-2}\chi_{k-1}\}.$$

où $\chi_0$, $\chi_1$, ---, $\chi_{k-1}$ sont k variables aléatoires binaires à valeurs dans l'ensemble $E_\xi$. Ainsi, toute chaîne de Markov binaire de ce type appartient à la sous-classe PP.

Considérons une suite aléatoire binaire $\Xi = \{\xi(n)\}$, $\xi(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$, appartenant à la sous-classe PP et traversant un circuit logique séquentiel comme celui représenté dans la figure 3.4.

Malheureusement, il n'est pas difficile de constater que la suite aléatoire binaire $z = \{\zeta(n)\}$, $\zeta(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$, à la sortie de ce circuit n'appartient pas à la sous-classe PP.

Ce fait limite forcément l'application pratique de cette sous-classe PP de suites aléatoires binaires.

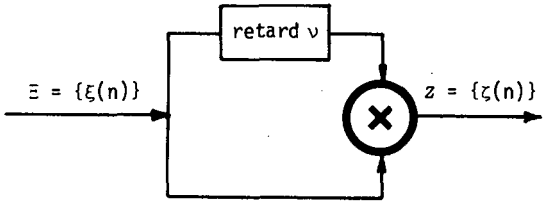



*Fig. 3.4: Filtrage numérique d'une suite aléatoire binaire .*

## IV. CHAINES DE MARKOV BINAIRES.

Les chaînes de Markov binaires forment une sous-classe importante des suites aléatoires binaires. En ce qui concerne l'art de l'ingénieur en életronique, on en trouve des applications importantes dans les théories du codage [e.g. 30,37] et des automates [e.g. 7].

Nous ne serons pas concernés, dans ce travail, par la théorie classique des chaînes de Markov, c'est-à-dire la théorie telle qu'on la trouve dans un grand nombre d'ouvrages [e.g. 18,29,33].

Nous traiterons plutôt de quelques questions plus pratiques que se posent les ingénieurs comme:

- De quel type est la fonction d'autocorrélation de cette chaîne de Markov binaire ?

- Est-ce-que le produit, ou de manière équivalente (voir table 2.1), la somme modulo 2 de deux chaînes de Markov binaires reste une chaîne de Markov binaire ?

Mais avant cela, définissons quelques concepts que nous utiliserons dans le présent chapitre.

### IV.1. Définitions.

Les références principales concernant ce sous-chapitre sont les livres de Feller [18], d'Isaacson et Madsen [29] ainsi que de Karlin et Taylor [33]. Les définitions générales qu'ils contiennent sont adaptées au cas binaire.

Considérons une suite aléatoire binaire $\Xi = \{\xi(n)\}$, $\xi(n)$ est une variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$, et la probabilité conditionnelle $P\{\xi(k) = x_k | \xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}, \text{---}, \xi(0) = x_0\}$.

Définition 4.1:

*La suite aléatoire binaire* $\Xi$ *est appelée une chaîne de Markov binaire d'ordre r si pour toute valeur de* $k \geq r$:

$$P\{\xi(k) = x_k | \xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}, \text{---}, \xi(0) = x_0\} =$$
$$= P\{\xi(k) = x_k | \xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\},$$

*r étant le plus petit entier vérifiant cette relation.*

Puisque nous ne considérons que des suites aléatoires binaires stationnaires, cela implique:

$$P\{\xi(k) = x_k | \xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\} =$$
$$= P\{\xi(k+\nu) = x_k | \xi(k+\nu-1) = x_{k-1}, \text{---}, \xi(k+\nu-r) = x_{k-r}\}$$

pour toute valeur entière positive de $\nu$.

Définition 4.2:

*Les* $2^r$ *événements possibles* $\{\xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\}$ *sont appelés les états de la chaîne.*

*La probabilité conjointe* $P\{\xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\}$ *représente la probabilité que la chaîne se trouve (au temps k-1) dans l'état* $\{\xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\}$. *Nous l'appellerons la probabilité de l'état* $\{\xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\}$.

Définition 4.3:

*On appelle probabilité de transition de l'état* $\{\xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\}$ *à l'état* $\{\xi(k) = x_k, \text{---}, \xi(k-r+1) = x_{k-r+1}\}$ *la probabilité conditionnelle* $P\{\xi(k) = x_k | \xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\}$.

*Notation:*

Pour ne pas alourdir la notation, représentons l'état $\{\xi(k-1) = x_{k-1}, \text{---}, \xi(k-r) = x_{k-r}\}$ par un entier i, $0 \leq i \leq 2^r-1$, tel que:

$$i = \sum_{l=1}^{r} \frac{1}{2}(1-x_{k-l})\, 2^{l-1} \quad , \quad x_{k-l} \in E_\xi .$$

Nous désignerons la probabilité conjointe $P\{\xi(k-1) = x_{k-1}, ---, \xi(k-r) = x_{k-r}\}$ par le symbole $p_i$, l'état $\{\xi(k-1) = x_{k-1}, ---, \xi(k-r) = x_{k-r}\}$ correspondant à l'état i, et la probabilité de transition $P\{\xi(k) = x_k | \xi(k-1) = x_{k-1}, ---, \xi(k-r) = x_{k-r}\}$ par le symbole $\pi_{ij}$, l'état $\{\xi(k) = x_k, ---, \xi(k-r+1) = x_{k-r+1}\}$ correspondant à l'état j.

Définition 4.4:

*On appelle vecteur des probabilités des états le vecteur:*

$$\underline{p}_r = [p_0\ p_1\ ---\ p_{2^r-1}].$$

Celui-ci correspond au vecteur transposé des probabilités conjointes (définition 3.2) de r variables aléatoires binaires successives.

Il est évident que $p_1 \geq 0$, $0 \leq 1 \leq 2^r-1$, et $\sum_{1=0}^{2^r-1} p_1 = 1$.

Nous pouvons arranger les probabilités de transition $\pi_{ij}$, $0 \leq \pi_{ij} \leq 1$, $0 \leq i,j \leq 2^r-1$, dans une matrice carrée $2^r \times 2^r$ que l'on dénotera par $\Pi_r$.

Si la chaîne se trouve dans l'état i, elle doit nécessairement transiter dans un des $2^r$ états j possibles. Ceci implique:

$$\sum_{j=0}^{2^r-1} \pi_{ij} = 1 \quad , \quad 0 \leq i \leq 2^r-1.$$

En utilisant les définitions 2.4 et 2.5 en plus du fait que les chaînes de Markov binaires que nous considérons sont stationnaires, nous trouvons:

$$\underline{p}_r = \underline{p}_r \cdot \Pi_r^\nu \quad , \quad \nu \in N. \tag{4.1}$$

*Remarque:*

On démontre [49] que la solution $\underline{p}_r$ de l'équation (4.1) est unique.

Définition 4.5:

*On appelle matrice stochastique toute matrice dont les éléments sont non négatifs et la somme de ceux-ci sur chaque ligne vaut un.*

$\Pi_r$ est donc une matrice stochastique pour toute valeur de r.

Etant donné la structure d'une chaîne de Markov binaire, chaque ligne et chaque colonne de la matrice des probabilités de transition $\Pi_r$ ne peuvent contenir au plus que deux éléments non nuls.

En effet, considérons l'état $\{\xi(k-1) = x_{k-1}, ---, \xi(k-r) = x_{k-r}\}$. Les deux seules transitions possibles sont:

$$\{\xi(k-1) = x_{k-1}, ---, \xi(k-r) = x_{k-r}\} \begin{cases} \nearrow \{\xi(k) = +1, ---, \xi(k-r+1) = x_{k-r+1}\} \\ \searrow \{\xi(k) = -1, ---, \xi(k-r+1) = x_{k-r+1}\} \end{cases}.$$

Il n'y a donc au plus que deux probabilités de transition non nulles dans chaque ligne de la matrice $\Pi_r$.

De la même manière, l'état $\{\xi(k) = x_k, ---, \xi(k-r+1) = x_{k-r+1}\}$ ne peut provenir que des deux transitions:

$$\begin{cases} \{\xi(k-1) = x_{k-1}, ---, \xi(k-r) = +1\} \searrow \\ \{\xi(k-1) = x_{k-1}, ---, \xi(k-r) = -1\} \nearrow \end{cases} \{\xi(k) = x_k, ---, \xi(k-r+1) = x_{k-r+1}\}.$$

Il n'y a donc au plus que deux probabilités de transition non nulles dans chaque colonne de la matrice $\Pi_r$.

Exemple 4.1:

Considérons une chaîne de Markov d'ordre 2. Les quatre états de la chaîne sont les suivants:

état 0 $\hat{=}$ état$\{\xi(k-1) = +1, \xi(k-2) = +1\}$,

état 1 $\hat{=}$ état$\{\xi(k-1) = -1, \xi(k-2) = +1\}$,

état 2 $\hat{=}$ état$\{\xi(k-1) = +1, \xi(k-2) = -1\}$,

état 3 $\hat{=}$ état$\{\xi(k-1) = -1, \xi(k-2) = -1\}$.

La matrice des probabilités de transition $\Pi_2$ est de la forme:

$$\Pi_2 = \begin{bmatrix} \pi_{00} & \pi_{01} & 0 & 0 \\ 0 & 0 & \pi_{12} & \pi_{13} \\ \pi_{20} & \pi_{21} & 0 & 0 \\ 0 & 0 & \pi_{32} & \pi_{33} \end{bmatrix},$$

avec: $\pi_{00}+\pi_{01} = \pi_{12}+\pi_{13} = \pi_{20}+\pi_{21} = \pi_{32}+\pi_{33} = 1$.

Une chaîne de Markov binaire d'ordre r possède donc une matrice des probabilités de transition du type:

$$\Pi_r = \begin{bmatrix} \pi_{00} & 1-\pi_{00} & & & & \\ & & \ddots & & & \\ & & & & \pi_{2^{r-1}-1 2^r-2} & 1-\pi_{2^{r-1}-1 2^r-2} \\ \pi_{2^{r-1}0} & 1-\pi_{2^{r-1}0} & & & & \\ & & \ddots & & & \\ & & & & \pi_{2^r-1 2^r-2} & 1-\pi_{2^r-1 2^r-2} \end{bmatrix}. \qquad (4.2)$$

On constate donc qu'il n'y a que $2^r$ éléments non nuls indépendants.

*Remarque:*

Une chaîne de Markov binaire d'ordre 0 est une suite de Bernoulli.

*Notation:*

Souvent, nous utiliserons la notation abrégée (contenant tous les éléments non nuls et indépendants de la matrice des probabilités de transition $\Pi_r$):

$$\Pi_r = \{\pi_{00}\ \pi_{12}\ \cdots\ \pi_{i2i \bmod 2^r}\ \cdots\ \pi_{2^r-1 2^r-2}\}.$$

Certaines matrices des probabilités de transition possèdent en plus la propriété: $\sum_{i=0}^{2^r-1} \pi_{ij} = 1.$

Définition 4.6:

*On appelle matrice doublement stochastique toute matrice stochastique dont la somme des éléments sur chaque colonne vaut un.*

On montre facilement que:

- Le produit de deux matrices stochastiques est une matrice stochastique.

- Le produit de deux matrices doublement stochastiques est une matrice doublement stochastique.

- Si $\Pi_r^{\nu_1} = [\pi_{ij}(\nu_1)]$ et $\Pi_r^{\nu_2} = [\pi_{ij}(\nu_2)]$, alors, par la relation (4.1), nous obtenons (équations de Chapman-Kolmogorov):

$$\Pi_r^{\nu_1+\nu_2} = \Pi_r^{\nu_1} \cdot \Pi_r^{\nu_2},$$

$$\pi_{ij}(\nu_1+\nu_2) = \sum_{l=0}^{2^r-1} \pi_{il}(\nu_1)\pi_{lj}(\nu_2) \quad , \nu_1, \nu_2 \in N.$$

Dans ce chapitre, nous ne traiterons (sauf mentionné) que des chaînes de Markov binaires étant:

- Irréductibles, c'est-à-dire que chaque état peut être atteint à partir de tout autre état.

- Apériodiques, c'est-à-dire que chaque état de la chaîne est de période d = 1, l'état i étant de période d si d est le plus grand commun diviseur de tout entier $\nu \geq 1$ pour lequel $\pi_{ii}(\nu) > 0$, $\nu \in N$.

## IV.2. Valeurs propres de la matrice des probabilités de transition.

Nous allons examiner quelques propriétés liées aux valeurs propres de la matrice des probabilités de transition $\Pi_r$.

$\Pi_r$ étant une matrice stochastique, elle fait donc partie de la famille des matrices non négatives [49].

**Théorème de Gerschgorin [56]:**

Toute valeur propre d'une matrice $n \times n$ $A = [a_{ij}]$ se trouve au moins dans un des cercles $C_1$, ---, $C_i$, ---, $C_n$, $C_i$ ayant pour centre l'élément $a_{ii}$ et pour rayon la grandeur $R_i = \sum_{j \neq i} |a_{ij}|$.

Le théorème de Gerschgorin appliqué à la matrice stochastique $\Pi_r$ nous montre que toutes ses valeurs propres sont situées dans le disque unité du plan complexe (Fig. 4.1).

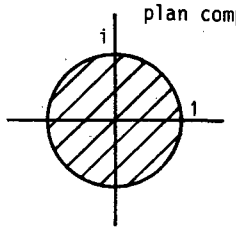



*Fig. 4.1: Disque unité du plan complexe contenant toutes les valeurs propres de la matrice $\Pi_r$.*

**Définition 4.7[49]:**

*Une matrice carrée A non négative est appelée primitive s'il existe un entier positif $\nu$ tel que tous les éléments de $A^\nu$ soient strictement positifs.*

Etant donné que nous avons affaire à des chaînes de Markov binaires d'ordre r irréductibles et apériodiques, il existe un entier $\nu \geq r$ tel que tous les éléments de la matrice des probabilités de transition $\Pi_r^{\nu}$ soient strictement positifs. $\Pi_r$ est donc par définition une matrice primitive.

Théorème de Perron-Frobenius pour matrices primitives [49]:

Soit A une matrice $n \times n$ primitive. Alors, il existe une valeur propre $\lambda_{PF}$ telle que:

a) $\lambda_{PF}$ est réelle, $\lambda_{PF} > 0$,

b) le vecteur propre associé à $\lambda_{PF}$ est strictement positif,

c) $\lambda_{PF}$ est de multiplicité un,

d) $\lambda_{PF} > |\lambda|$ pour toute valeur propre $\lambda \neq \lambda_{PF}$.

En examinant l'équation $\Pi_r \cdot u = \lambda u$, on trouve facilement qu'une de ses solutions nous est donnée par:

$$\lambda_0 = 1 \text{ et } u_0 = e_r = [1\ 1\ \text{---}\ 1]^T \text{ (vecteur } 2^n \times 1).$$

Si nous combinons les théorèmes de Gerschgorin et de Perron-Frobenius, nous constatons que $\lambda_0 = 1$ est la valeur propre $\lambda_{PF}$ de la matrice $\Pi_r$ et $u_0$ son vecteur propre associé.

Corollaire 4.1:

Soit $p(\lambda) = \det|\Pi_r - \lambda I| = \sum_{l=0}^{2^r} \alpha_l \lambda^l$ le polynôme caractéristique de la matrice des probabilités de transition $\Pi_r$. Alors: $\sum_{l=0}^{2^r} \alpha_l = 0$.

Démonstration:

Puisque $\lambda_0 = 1$ est une solution de $p(\lambda)$, nous obtenons:

$$\sum_{l=0}^{2^r-1} \alpha_l = 0.$$

CQFD.

Comportement asymptotique.

Etudions le comportement asymptotique de la matrice des probabilités de transition: $\lim_{\nu \to \infty} \Pi_r^\nu$. Nous savons qu'une telle limite existe puisque $\lambda_0 = 1$ est la seule valeur propre de module égal à un [45].

a) La matrice $\Pi_r$ est diagonalisable.

La matrice $\Pi_r$ étant diagonalisable, elle possède $2^r$ vecteurs propres linéairement indépendants. Si ces vecteurs propres sont les colonnes d'une matrice S, alors:

$$\Pi_r = S \cdot \Lambda_r \cdot S^{-1} \tag{4.3}$$

où $\Lambda_r = \text{diag}\{\lambda_0\ \lambda_1\ \text{---}\ \lambda_{2^r-1}\}$; $\lambda_l, 0 \leq l \leq 2^r-1$, sont les valeurs propres de $\Pi_r$.

Il devient ainsi facile de calculer $\Pi_r^\nu$:

$$\Pi_r^\nu = S \cdot \Lambda_r^\nu \cdot S^{-1}. \tag{4.4}$$

Nous avons vu que le vecteur propre $u_0$ associé à la valeur propre $\lambda_0$ est égal à $e_r$. Cela signifie que:

$$S = \begin{bmatrix} 1 & & \\ 1 & & \\ 1 & * & \\ 1 & & \\ 1 & & \end{bmatrix}.$$

Admettons que la première ligne de la matrice $S^{-1}$ soit égale à un vecteur ligne quelconque $[y_{00}\ y_{01}\ ---\ y_{02^r-1}]$:

$$S^{-1} = \begin{bmatrix} y_{00} & y_{01} & --- & y_{02^r-1} \\ & & * & \\ & & & \end{bmatrix}.$$

En prenant la limite de la relation (4.4), nous trouvons:

$$\lim_{\nu \to \infty} \Pi_r^{\nu} = \lim_{\nu \to \infty} S \cdot \Lambda_r^{\nu} \cdot S^{-1} = \begin{bmatrix} y_{00} & y_{01} & --- & y_{02^r-1} \\ & & \vdots & \\ y_{00} & y_{01} & --- & y_{02^r-1} \end{bmatrix},$$

car: $\lim_{\nu \to \infty} \operatorname{diag}\{1\ \lambda_1^{\nu}\ ---\ \lambda_{2^r-1}^{\nu}\} = \operatorname{diag}\{1\ 0\ ---\ 0\}$.

La matrice $\lim_{\nu \to \infty} \Pi_r^{\nu}$ est donc de rang 1 et s'obtient en répétant $2^r$ fois la première ligne de la matrice $S^{-1}$.

La relation (4.1) est vraie pour tout $\nu \in N$. Donc:

$$\hat{p}_r = \lim_{\nu \to \infty} \hat{p}_r \cdot \Pi_r^{\nu} = [y_{00}\ y_{01}\ ---\ y_{02^r-1}].$$

On en conclut que la première ligne de la matrice $S^{-1}$ est égale au vecteur des probabilités des états.

Si la matrice $\Pi_r$ est en plus doublement stochastique, nous obtenons:

$$\sum_{j=0}^{2^r-1} y_{0l} = \sum_{j=0}^{2^r-1} p_l = 1 \Longrightarrow p_l = \frac{1}{2^r},\ 0 \le l \le 2^r-1.$$

Le vecteur des probabilités des états est ici r-équiprobable (définition 3.5).

b) La matrice $\Pi_r$ est défective.

La matrice $\Pi_r$ ne possède plus $2^r$ vecteurs propres linéairement indépendants. Dans ce contexte, la relation (4.3) n'est pas applicable.

Supposons que $\Pi_r$ possède s vecteurs propres linéairement indépendants. Alors, $\Pi_r$ est semblable à une matrice de Jordan $H_r$ [56]:

$$\Pi_r = G \cdot H_r \cdot G^{-1}, \tag{4.5}$$

où: $H_r = \text{diag}\{J_0\ J_1\ \text{---}\ J_{s-1}\}$ et

$$J_l = \begin{bmatrix} \lambda_l & 1 & & \\ & \lambda_l & 1 & \\ & & \ddots & \ddots \\ & & & \lambda_l \end{bmatrix},$$

$J_l$ étant une matrice $n_\ell \times n_\ell$ appelée cellule de Jordan, alors que $\lambda_l$ (multiplicité $n_l$), $0 \leq l \leq s-1$, sont les valeurs propres de $\Pi_r$.

Dans notre cas, $J_0 = \lambda_0 = 1$ et la première colonne de la matrice G est égale au vecteur propre $u_0 = e_r$. Donc:

$$G = \begin{bmatrix} 1 & & \\ 1 & & \\ \vdots & * & \\ 1 & & \end{bmatrix}.$$

Ici, la matrice $\Pi_r^\nu$ devient:

$$\Pi^\nu = G \cdot H_r^\nu \cdot G^{-1}, \tag{4.6}$$

où (on admet $\nu > n_l$) [45]:

$$J_l^\nu = \begin{bmatrix} \lambda_l^\nu & \binom{\nu}{1}\lambda_l^{\nu-1} & \binom{\nu}{2}\lambda_l^{\nu-2} & \text{---} & \binom{\nu}{n_l-1}\lambda^{\nu-n_l+1} \\ & \lambda_l^\nu & \binom{\nu}{1}\lambda_l^{\nu-1} & \text{---} & \binom{\nu}{n_l-2}\lambda^{\nu-n_l+2} \\ & & \ddots & \ddots & \vdots \\ & & & & \binom{\nu}{1}\lambda_l^{\nu-1} \\ & & & & \lambda_l^\nu \end{bmatrix}. \tag{4.7}$$

Que devient la limite: $\lim_{\nu \to \infty} \Pi_r^\nu$ ? Considérons, dans la cellule de Jordan $J_1^\nu$, l'élément $\binom{\nu}{n_1-1}\lambda_1^{\nu-n_1+1}$, $1 \neq 0$:

$$\binom{\nu}{n_1-1}\lambda_1^{\nu-n_1+1} = \frac{\nu!}{(n_1-1)!\ (\nu-n_1+1)!}\lambda_1^{\nu-n_1+1} \leq \nu^{n_1-1}|\lambda_1|^{\nu-n_1+1}$$

$$= \nu^{n_1-1} e^{(\nu-n_1+1)\ln|\lambda_1|}.$$

Nous savons que $|\lambda_1| < 1$. Donc

$$\nu^{n_1-1} e^{(\nu-n_1+1)\ln|\lambda_1|} \xrightarrow[\nu \to \infty]{} 0.$$

Finalement, si la première ligne de la matrice $G^{-1}$ est posée égale à un vecteur ligne quelconque $[y_{00}\ y_{01}\ \cdots\ y_{02^r-1}]$:

$$G^{-1} = \begin{bmatrix} y_{00} & y_{01} & \cdots & y_{02^r-1} \\ & & * & \\ & & & \end{bmatrix},$$

alors,

$$\lim_{\nu \to \infty} \Pi_r^\nu = \begin{bmatrix} y_{00} & y_{01} & \cdots & y_{02^r-1} \\ & & \vdots & \\ y_{00} & y_{01} & \cdots & y_{02^r-1} \end{bmatrix}.$$

Nous nous retrouvons dans la situation déjà rencontrée au point a. Aussi, la première ligne de la matrice $G^{-1}$ est égale au vecteur des probabilités des états.

Chaînes de Markov binaires réductibles.

Bien que le contenu de ce paragraphe soit applicable à toute chaîne de Markov, nous allons intentionnellement nous restreindre au cas binaire qui est le sujet de cette étude.

Si une chaîne de Markov binaire $\Xi$ d'ordre r n'est pas irréductible, il est toujours possible de récrire sa matrice des probabilités de transition $\Pi_r$ sous une forme semblable $\Pi_r^*$ [45]:

$$\Pi_r^* = \begin{bmatrix} W_1 & & & \\ & W_2 & & \\ & & \ddots & \\ & & & W_k \\ U_1 & U_2 & \cdots & U_k & V \end{bmatrix}$$

où:

- $W_1$, $W_2$, ---, $W_k$ sont k matrices stochastiques des probabilités de transition représentant k sous-chaînes de Markov binaires $\Xi_1$, $\Xi_2$, ---, $\Xi_k$ irréductibles respectivement d'ordre $r_1$, $r_2$, ---, $r_k$.

- V est une matrice contenant les probabilités de transition entre états transitoires. V n'est pas une matrice stochastique. Elle n'a pas $\lambda_0 = 1$ comme valeur propre, donc: $\lim_{\nu \to \infty} V^\nu = 0$.

- $U_1$, $U_2$, ---, $U_k$ sont k matrices contenant les probabilités de transition entre les états transitoires et les k sous-chaînes de Markov binaires $\Xi_1$, $\Xi_2$, ---, $\Xi_k$. Ces matrices ne sont pas stochastiques et $\lim_{\nu \to \infty} U_1^\nu = 0$, $0 \leq 1 \leq k$.

En examinant $\Pi_r^*$, on constate qu'après un nombre fini de transitions, le système équivaudra forcément à l'une des k sous-chaînes de Markov binaires $\Xi_1$, $\Xi_2$, ---, $\Xi_k$, chacune d'elles étant pondérées par une probabilité $w_1$, $1 \leq 1 \leq k$, de représenter effectivement le système.

L'étude de la chaîne de Markov binaire $\Xi$ se réduit donc à l'étude de k sous-chaînes de Markov binaires $\Xi_1$, $\Xi_2$, ---, $\Xi_k$ irréductibles (pondérées par les probabilités $w_l$, $1 \leq l \leq k$) représentées respectivement par les matrices des probabilités de transition $W_1$, $W_2$, ---, $W_k$.

Théorème 4.1 [29]:

Soit $\Pi_r$ la matrice des probabilités de transition de la chaîne de Markov binaire $\Xi$ d'ordre r. Alors, la multiplicité de la valeur propre 1 est égale au nombre de sous-chaînes irréductibles.

Exemple 4.2:

Voyons la chaîne de Markov binaire d'ordre 2 représentée par la matrice des probabilités de transition $\Pi_2$:

$$\Pi_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0.8 & 0.2 \\ 0.4 & 0.6 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Les valeurs propres de cette matrice sont les suivantes:

$$\lambda_0 = 1,$$

$$\lambda_1 = 1,$$

$$\lambda_2 = 0.693,$$

$$\lambda_3 = -0.693.$$

La valeur propre 1 est de multiplicité deux. Il y a donc deux chaînes de Markov binaires irréductibles comme nous pouvons le constater en examinant la matrice $\Pi_2^*$.

$$\Pi_2^* = \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0.4 & 0 & 0 & 0.6 \\ 0 & 0.2 & 0.8 & 0 \end{array}\right] = \left[\begin{array}{cc|c} W_1 & 0 & 0 \\ 0 & W_2 & 0 \\ \hline U_1 & U_2 & V \end{array}\right].$$

Si $\overset{\sim}{P}_2 = [p_0\ p_1\ p_2\ p_3]$, alors, les probabilités $w_1$ et $w_2$ sont données par:

$$w_1 = p_0 + \frac{0.4 \cdot 0.8}{1-0.6 \cdot 0.8} p_1 + \frac{0.4}{1-0.6 \cdot 0.8} p_2,$$

$$w_2 = p_3 + \frac{0.2}{1-0.6 \cdot 0.8} p_1 + \frac{0.2 \cdot 0.6}{1-0.6 \cdot 0.8} p_2.$$

Les chaînes de Markov auxquelles nous avons affaire sont stationnaires. En résolvant l'équation (4.1), nous trouvons facilement que:

$$\overset{\sim}{P}_2 = [p_0\ 0\ 0\ p_3] \text{ et } w_1 = p_0,\ w_2 = p_3.$$

## IV.3. Moments conjoints.

Nous allons dériver une formule générale nous permettant de calculer le moment conjoint d'ordre k de k variables aléatoires binaires, à valeurs dans l'ensemble $E_\xi$, appartenant à une chaîne de Markov binaire d'ordre r.

Nous avons défini, relation (2.1), un tel moment conjoint:

$$m_{\xi\xi \cdots \xi}(\nu_1, \cdots, \nu_{k-1}) = E\{\xi(n)\xi(n+\nu_1) \cdots \xi(n+\nu_1+ \cdots + \nu_{k-1})\}.$$

*Notation:*

Pour ne pas alourdir la notation, nous écrirons le moment conjoint défini ci-dessus $\underline{m}_k(\nu_1, \cdots, \nu_{k-1})$, il correspond à la dernière composante du vecteur des moments conjoints $M_k$ de k variables aléatoires binaires, et $\tilde{\nu}_k = \nu_1+ \cdots +\nu_{k-1}$.

Théorème 4.2:

Soit une chaîne de Markov binaire $\Xi = \{\xi(n)\}$ d'ordre r, $\xi(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$, avec matrice des probabilités de transition $\Pi_r = \{\pi_{00}\ \pi_{12} \cdots \pi_{i2i\bmod 2^r} \cdots \pi_{2^r-1\,2^r-2}\}$, $\Pi_r^\nu = [\pi_{ij}(\nu)]$, $0 \le i,j \le 2^r-1$, et vecteur des probabilités des états $\overset{\gamma}{P}_r = [p_0\ p_1 \cdots p_{2^r-1}]$.

Alors, le moment conjoint d'ordre k d'une telle chaîne $\Xi$ est donné par:

$$\underline{m}_k(\nu_1, \cdots, \nu_{k-1}) = v^T \cdot P_r(\nu_{k-2}) \cdot \Pi_r^{\nu_{k-1}} \cdot v \ , \quad k = 2, 3, \cdots,$$

où: $v = [+1\ -1 \cdots (-1)^l \cdots +1\ -1]^T$ , $0 \le l \le 2^r-1$,

$$P_r(\nu_{k-2}) = \text{diag}\ \{Q_0(\nu_{k-2})\ Q_1(\nu_{k-2}) \cdots Q_{2^r-1}(\nu_{k-2})\},$$

$$P_r(\nu_0) = \text{diag}\ \{p_0\ p_1 \cdots p_{2^r-1}\} \ , \ k = 2 \quad (\nu_0 = 0),$$

$$Q_l(\nu_{k-2}) = v^T \cdot P_l(\nu_{k-3}) \cdot C_l(\nu_{k-2}) \ , \ 0 \le l \le 2^r-1,$$

$$C_l(\nu_{k-2}) = [\pi_{0l}(\nu_{k-2})\ \pi_{1l}(\nu_{k-2}) \cdots \pi_{2^r-1\,l}(\nu_{k-2})]^T.$$

Démonstration:

L'expression à dériver découle directement de la structure même des chaînes de Markov binaires.

$$\underline{m}_k(\nu_1, \text{---}, \nu_{k-1}) = (+1)(+1) \sum_{i \text{ pairs}} Q_i(\nu_{k-2}) \sum_{j \text{ pairs}} \pi_{ij}(\nu_{k-1}) +$$

$$+ (+1)(-1) \sum_{i \text{ pairs}} Q_i(\nu_{k-2}) \sum_{j \text{ impairs}} \pi_{ij}(\nu_{k-1}) +$$

$$+ (-1)(+1) \sum_{i \text{ impairs}} Q_i(\nu_{k-2}) \sum_{j \text{ pairs}} \pi_{ij}(\nu_{k-1}) +$$

$$+ (-1)(-1) \sum_{i \text{ impairs}} Q_i(\nu_{k-2}) \sum_{j \text{ impairs}} \pi_{ij}(\nu_{k-1}),$$

où le facteur $x_{n+\tilde{\nu}_{k-2}} x_{n+\tilde{\nu}_{k-1}} = (+1)(+1)$ ou $(+1)(-1)$ ou $(-1)(+1)$ ou $(-1)(-1)$ est le produit des réalisations possibles des variables aléatoires binaires $\xi(n+\tilde{\nu}_{k-2})$ et $\xi(n+\tilde{\nu}_{k-1})$ alors que $Q_i(\nu_{k-2})$, $0 \leq i \leq 2^r-1$, représente la contribution, au moment conjoint, des transitions antérieures au temps $n+\tilde{\nu}_{k-2}$.

Cette relation s'écrit sous la forme condensée:

$$\underline{m}_k(\nu_1, \text{---}, \nu_{k-1}) = v^T \cdot P_r(\nu_{k-2}) \cdot \Pi_r^{\nu_{k-1}} \cdot v,$$

avec: $v = [+1 \ -1 \ \text{---} \ (-1)^l \ \text{---} \ +1 \ -1]^T$, $0 \leq l \leq 2^r-1$,

$$P_r(\nu_{k-2}) = \text{diag}\{Q_0(\nu_{k-2}) \ Q_1(\nu_{k-2}) \ \text{---} \ Q_{2^r-1}(\nu_{k-2})\}.$$

La réalisation de la variable aléatoire binaire $\xi(n+\tilde{\nu}_{k-2})$ correspond à la terminaison d'une suite de r symboles binaires consécutifs: un état de la chaîne au temps $n+\tilde{\nu}_{k-2}$. Il y a $2^r$ états possibles pour une chaîne de Markov binaire d'ordre r. La contribution au moment conjoint de chacune des $2^r$ terminaisons vaut, pour l'état l, $0 \leq l \leq 2^r-1$:

$$Q_l(\nu_{k-2}) = v^T \cdot P_r(\nu_{k-3}) \cdot C_l(\nu_{k-2}).$$

Le vecteur $C_1(\nu_{k-2}) = [\pi_{01}(\nu_{k-2})\ \pi_{11}(\nu_{k-2})\ \text{---}\ \pi_{2^r-11}(\nu_{k-2})]^T$ correspond au vecteur contenant les probabilités de transition d'un état quelconque i, $0 \le i \le 2^r-1$, présent au temps $n+\tilde{\nu}_{k-3}$ à l'état 1 présent au temps $n+\tilde{\nu}_{k-2}$.

COFD.

Il est évident que: $\underline{m}_1 = m_\xi = \hat{P}_r \cdot v$.

Nous constatons que grâce au théorème 4.2, nous pouvons calculer récursivement la matrice $P(\nu_{k-2})$. On passe ensuite facilement, pour tout k, des matrices $P(\nu_{k-2})$ aux moments conjoints $\underline{m}_k(\nu_1, \text{---}, \nu_{k-1})$.

Exemple 4.3:

Prenons le cas d'une chaîne de Markov binaire d'ordre un avec matrice des probabilités de transition $\Pi_1$ doublement stochastique:

$$\Pi_1 = \begin{bmatrix} \pi & 1-\pi \\ 1-\pi & \pi \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix} \cdot \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & -0.5 \end{bmatrix},$$

où $\lambda = 2\pi-1$.

La première ligne de la matrice $S^{-1}$ est égale au vecteur des probabilités des états. Donc: $\hat{P}_1 = [0.5\ 0.5]$.

On trouve facilement que:

$$\Pi_1^\nu = 0.5 \begin{bmatrix} 1+\lambda^\nu & 1-\lambda^\nu \\ 1-\lambda^\nu & 1+\lambda^\nu \end{bmatrix}.$$

Calculons, par récurrence, $Q_l(\nu_k)$, l = 0, 1:

$$Q_0(0) = 0.5 \qquad Q_1(0) = 0.5$$

$$Q_0(\nu_1) = 0.5\,\lambda^{\nu_1} \qquad Q_1(\nu_1) = -0.5\,\lambda^{\nu_1}$$

$$Q_0(\nu_2) = 0.5\,\lambda^{\nu_1} \qquad Q_1(\nu_2) = 0.5\,\lambda^{\nu_1}$$

$$Q_0(\nu_3) = 0.5\,\lambda^{\nu_1}\lambda^{\nu_3} \qquad Q_1(\nu_3) = -0.5\,\lambda^{\nu_1}\lambda^{\nu_3}$$

$$Q_0(\nu_4) = 0.5\,\lambda^{\nu_1\,\nu_3} \qquad Q_1(\nu_4) = 0.5\,\lambda^{\nu_1}\lambda^{\nu_3}$$

Supposons que les relations (k impair)

$$Q_0(\nu_{k-2}) = 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} \qquad Q_1(\nu_{k-2}) = -0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}}$$

soient vraies. Alors:

$$Q_0(\nu_{k-1}) = [+1\ -1]\cdot\begin{bmatrix} 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} & 0 \\ 0 & -0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} \end{bmatrix}\cdot\begin{bmatrix} 0.5+0.5\ \lambda^{\nu_{k-1}} \\ 0.5-0.5\ \lambda^{\nu_{k-1}} \end{bmatrix} =$$

$$= 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}},$$

$$Q_1(\nu_{k-1}) = [+1\ -1]\cdot\begin{bmatrix} 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} & 0 \\ 0 & -0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} \end{bmatrix}\cdot\begin{bmatrix} 0.5-0.5\ \lambda^{\nu_{k-1}} \\ 0.5+0.5\ \lambda^{\nu_{k-1}} \end{bmatrix} =$$

$$= 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}},$$

et:

$$Q_0(\nu_k) = [+1\ -1]\cdot\begin{bmatrix} 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} & 0 \\ 0 & 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} \end{bmatrix}\cdot\begin{bmatrix} 0.5+0.5\ \lambda^{\nu_k} \\ 0.5-0.5\ \lambda^{\nu_k} \end{bmatrix} =$$

$$= 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}}\lambda^{\nu_k},$$

$$Q_1(\nu_k) = [+1\ -1]\cdot\begin{bmatrix} 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} & 0 \\ 0 & 0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}} \end{bmatrix}\cdot\begin{bmatrix} 0.5-0.5\ \lambda^{\nu_k} \\ 0.5+0.5\ \lambda^{\nu_k} \end{bmatrix} =$$

$$= -0.5\ \lambda^{\nu_1}\lambda^{\nu_3}\ \text{---}\ \lambda^{\nu_{k-2}}\lambda^{\nu_k}.$$

Par le théorème 4.2, nous trouvons:

$$\underline{m}_k(\nu_1, \text{---}, \nu_{k-1}) = \begin{cases} \lambda^{\nu_1}\lambda^{\nu_3} \text{ --- } \lambda^{\nu_{k-1}} & , \text{ k pair} \\ 0 & , \text{ k impair.} \end{cases}$$

Remarquons que toute chaîne de Markov binaire d'ordre un avec matrice des probabilités de transition doublement stochastique possède les propriétés suivantes:

- Tout vecteur des probabilités conjointes de k variables aléatoires binaires (à valeurs dans l'ensemble $E_\xi$), k entier, lui appartenant est symétrique (corollaire 3.2).

- Elle appartient à la sous-classe PP des suites aléatoires binaires (voir III.7).

Exemple 4.4:

Calculons les moments conjoints d'ordre deux, trois et quatre de la chaîne de Markov binaire d'ordre deux avec matrice des probabilités de transition doublement stochastique particulière:

$$\Pi_2 = \begin{bmatrix} \pi & 1-\pi & 0 & 0 \\ 0 & 0 & \pi & 1-\pi \\ 1-\pi & \pi & 0 & 0 \\ 0 & 0 & 1-\pi & \pi \end{bmatrix} = S \cdot \Lambda_2 \cdot S^{-1},$$

avec: $\Lambda_2 = \text{diag}\{1\ \lambda_1\ \lambda_2\ \lambda_3\} = \text{diag}\{1\ 2\pi-1\ \sqrt{2\pi-1}\ -\sqrt{2\pi-1}\}.$

$$S = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & \frac{\lambda_2-\pi}{1-\pi} & \frac{\lambda_3-\pi}{1-\pi} \\ 1 & -1 & -\frac{\lambda_2-\pi}{1-\pi} & -\frac{\lambda_3-\pi}{1-\pi} \\ 1 & 1 & -1 & -1 \end{bmatrix},$$

$$S^{-1} = 0.5 \begin{bmatrix} 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ \frac{\lambda_3-\pi}{\lambda_2-\lambda_3} & \frac{1-\pi}{\lambda_2-\lambda_3} & -\frac{1-\pi}{\lambda_2-\lambda_3} & \frac{\lambda_3-\pi}{\lambda_2-\lambda_3} \\ \frac{\lambda_2-\pi}{\lambda_2-\lambda_3} & -\frac{1-\pi}{\lambda_2-\lambda_3} & \frac{1-\pi}{\lambda_2-\lambda_3} & -\frac{\lambda_2-\pi}{\lambda_2-\lambda_3} \end{bmatrix}.$$

Par le théorème 4.2, nous trouvons:

$$m_2(\nu_1) = 0.5\ (\lambda_2^{\nu_1}+\lambda_3^{\nu_1}),$$

$$m_3(\nu_1,\nu_2) = 0,$$

$$m_4(\nu_1,\nu_2,\nu_3) = 0.25\ (\lambda_2^{\nu_1}+\lambda_3^{\nu_1})(\lambda_2^{\nu_3}+\lambda_2^{\nu_3}) + 0.25\ \lambda_1^{\nu_2}(\lambda_2^{\nu_1}-\lambda_3^{\nu_1})(\lambda_2^{\nu_3}-\lambda_2^{\nu_3}).$$

Remarquons que ce type de chaîne de Markov binaire n'appartient pas à la sous-classe PP des suites aléatoires binaires (voir III.7).

Fonction d'autocorrélation.

Concentrons-nous sur le moment conjoint d'ordre deux $\underline{m}_2(\nu)$ ou fonction d'autocorrélation $R_{\xi\xi}(\nu)$ (définition 2.11).

Théorème 4.3:

Soit une chaîne de Markov binaire $\Xi = \{\xi(n)\}$ d'ordre r, $\xi(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$, avec matrice des probabilités de transition $\Pi_r$. $\Pi_r$ possède s vecteurs propres linéairement indépendants.
Alors, la fonction d'autocorrélation $R_{\xi\xi}(\nu)$ de la chaîne $\Xi$ est donnée par:

$$R_{\xi\xi}(\nu) = m_\xi^2 + \sum_{l=1}^{s-1} c_l(\nu)\lambda_l^\nu ,$$

où: $m_\xi$ dénote la moyenne de la chaîne $\Xi$,

$\lambda_l$, $1 \leq l \leq s-1$, sont les valeurs propres (de multiplicité $n_l$) de la matrice $\Pi_r$ (on exclut $\lambda_0 = 1$), $\lambda_l \neq 0$,

s correspond au nombre de cellules dans la représentation de Jordan de $\Pi_r$,

$n_l$ est l'ordre de la cellule de Jordan l,

$c_l(\nu)$ est une fonction polynômiale en $\nu$.

Démonstration:

Reprenons la relation (4.5):

$$\Pi_r = G \cdot H_r \cdot G^{-1}.$$

Ainsi,

$$\Pi_r^\nu = G \cdot H_r^\nu \cdot G^{-1}.$$

Posons:

$$\Pi_r^{\nu} = [X_0\ X_1\ \text{---}\ X_{s-1}] \cdot \begin{bmatrix} J_0^{\nu} & & \\ & J_1^{\nu} & \\ & & J_{s-1}^{\nu} \end{bmatrix} \cdot \begin{bmatrix} Y_0 \\ Y_1 \\ \vdots \\ Y_{s-1} \end{bmatrix},$$

où $X_l$ et $Y_l$, $0 \leq l \leq s-1$, sont respectivement deux matrices de dimension $2^r \times n_\ell$ et $n_\ell \times 2^r$. Développons:

$$\Pi_r^{\nu} = \sum_{l=0}^{s-1} X_l \cdot J_l^{\nu} \cdot Y_l .$$

En examinant la relation (4.7), nous constatons qu'il est possible, pour toute cellule de Jordan $J_l^{\nu}$, $0 \leq l \leq s-1$, de mettre en évidence le facteur $\lambda_l^{\nu}$, $\lambda_l \neq 0$.

Ainsi:

$$J_l^{\nu} = \lambda_l^{\nu}\, \mathcal{J}_l^{\nu}.$$

Par le théorème 4.1, nous obtenons:

$$\underline{m}_2(\nu) = R_{\xi\xi}(\nu) = v^T \cdot P_r(0) \cdot \Pi_r^{\nu} \cdot v = \sum_{l=0}^{s-1} v^T \cdot P_r(0) \cdot X_l \cdot J_l^{\nu} \cdot Y_l \cdot v,$$

$$R_{\xi\xi}(\nu) = \sum_{l=0}^{s-1} [v^T \cdot P_r(0) \cdot X_l \cdot \mathcal{J}_l^{\nu} \cdot Y_l \cdot v]\, \lambda_l^{\nu}. \tag{4.8}$$

Nous savons que: $X_0 = e_r$, $Y_0 = \hat{P}_r$ et $J_0 = 1$. Donc:

$$c_0(\nu) = v^T \cdot P_r(0) \cdot e_r \cdot \hat{P}_r \cdot v = v^T \cdot \hat{P}_r^T \cdot \hat{P}_r \cdot v = m_\xi^2,$$

$m_\xi$ étant la moyenne (indépendante de $\nu$) de la chaîne de Markov binaire $\Xi$.

En reprenant (4.8), nous trouvons:

$$R_{\xi\xi}(\nu) = m_\xi^2 + \sum_{l=1}^{s-1} c_l(\nu)\, \lambda_l^{\nu}, \tag{4.9}$$

où $c_l(\nu) = v^T \cdot P_r(0) \cdot X_l \cdot \mathcal{J}_l \cdot X_l \cdot v$, $1 \leq l \leq s-1$, est une fonction polynômiale en $\nu$.

CQFD.

*Remarques:*

a) Une des valeurs propres est nulle.

Si une des valeurs propres de la matrice $\Pi_r$ est nulle, disons $\lambda_{s-1} = 0$, alors, la relation (4.8) devient:

$$R_{\xi\xi}(\nu) = m_\xi^2 + \sum_{l=1}^{s-2} c_l(\nu)\,\lambda_l^\nu + v^T \cdot P_r(0) \cdot X_{s-1} \cdot J_{s-1}^\nu \cdot Y_{s-1} \cdot v =$$

$$= m_\xi^2 + \sum_{l=1}^{s-2} c_l(\nu)\,\lambda_l^\nu + K_{s-1}(\nu).$$

Mais, $J_{s-1}^\nu = 0$, donc $K_{s-1}(\nu) = 0$, pour tout $\nu \geq n_{s-1}-1$.

b) La matrice $\Pi_r$ est diagonalisable.

Si la matrice $\Pi_r$ est diagonalisable, elle possède $s = 2^r-1$ vecteurs propres linéairement indépendants et la relation (4.9) se simplifie pour devenir:

$$R_{\xi\xi}(\nu) = m_\xi^2 + \sum_{l=1}^{2^r-1} c_l\,\lambda_l^\nu\,, \qquad (4.10$$

où: $c_l = v^T \cdot P_r(0) \cdot X_l \cdot Y_l \cdot v$, $0 \leq l \leq 2^r-1$, est une constante indépendante de $\nu$,

$X_l$ est le vecteur propre associé à la valeur propre $\lambda_l$,

$Y_l$ est le vecteur ligne correspondant à la ligne l de la matrice inverse des vecteurs propres.

*Remarque:*

La fonction d'autocorrélation d'un processus de Markov stationnaire (d'ordre un) continu dans le temps avec un nombre fini d'états est la suivante [55]:

$$R_{\xi\xi}(\tau) = m_\xi^2 + \sum_{l=1}^{s-1} b_l(\tau)\, e^{\lambda_l \tau}\,,$$

où $\tau$ est une différence temporelle continue alors que $b_l(\tau)$ est un polynôme en $\tau$ d'ordre n'excédent pas $n_l-1$ ($m_\xi$, s et $n_l$ sont ici les mêmes grandeurs que celles définies précédemment).

On constate la similitude entre cette expression et la relation (4.9) qui se rapporte à une chaîne de Markov binaire d'ordre r.

Exemple 4.5:

Soit la chaîne de Markov binaire d'ordre deux avec matrice des probabilités de transition donnée par:

$$\Pi_2 = \begin{bmatrix} 0.7 & 0.3 & 0 & 0 \\ 0 & 0 & 0.4 & 0.6 \\ 0.9 & 0.1 & 0 & 0 \\ 0 & 0 & 0.8 & 0.2 \end{bmatrix}.$$

$\Pi_2$ est diagonalisable ce qui fait que l'on peut utiliser la relation (4.10). La fonction d'autocorrélation de cette chaîne est alors donnée par (Fig. 4.2):

$$R_{\xi\xi}(\nu) = 0.15 - 0.013(-0.305)^{\nu} + 0.868(.512)^{\nu}\cos(-0.136+\nu 1.37).$$

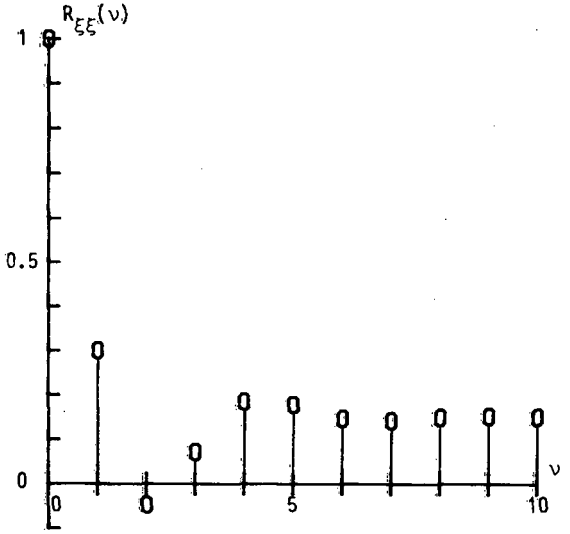



*Fig. 4.2: Fonction d'autocorrélation de la chaîne de de Markov binaire d'ordre deux avec matrice des probabilités de transition:*
*$\Pi_2$ = {0.7 0.4 0.9 0.8}.*

Corollaire 4.2:

Soit $R_{\xi\xi}(\nu) = \sum_{l=1}^{s-1} c_l(\nu)\,\lambda_l^{\nu}$ la fonction d'autocorrélation d'une chaîne de Markov binaire $\Xi = \{\xi(n)\}$, $\xi(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$. Alors:

$$\lim_{\nu \to 0} R_{\xi\xi}(\nu) = m_\xi^2 + \sum_{l=1}^{s-1} c_l(0) = 1 \text{ et}$$

$$\lim_{\nu \to \infty} R_{\xi\xi}(\nu) = m_\xi^2.$$

Démonstration:

Par définition, $R_{\xi\xi}(0) = E\{\xi^2(n)\}$. Donc:

$$R_{\xi\xi}(0) = (+1)^2 P\{\xi(n) = +1\} + (-1)^2 P\{\xi(n) = -1\} = 1.$$

Nous avons vu que pour toute cellule de Jordan (relation (4.7)), $\lim_{\nu \to \infty} J_l^{\nu} = 0$, $1 \le l \le s-1$, $\lambda_0 = 1$ étant de multiplicité un. Alors:

$$\lim_{\nu \to \infty} c_l(\nu)\,\lambda_l^{\nu} = 0\,, \quad 1 \le l \le s-1.$$

Donc:

$$\lim_{\nu \to \infty} R_{\xi\xi}(\nu) = m_\xi^2.$$

CQFD.

## IV.4. Produit ou somme modulo 2 de chaînes de Markov binaires indépendantes.

Soient $\Xi_1 = \{\xi_1(n)\}$ et $\Xi_2 = \{\xi_2(n)\}$ deux chaînes de Markov binaires indépendantes, $\xi_1(n)$ et $\xi_2(n)$ étant deux variables aléatoires binaires à valeurs dans l'ensemble $E_\xi$. Nous dirons que la suite aléatoire binaire $z = \{\zeta(n)\}$ est le produit de $\Xi_1$ et $\Xi_2$ si: $\zeta(n) = \xi_1(n)\cdot\xi_2(n)$ pour tout $n \in N$, $\zeta(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\xi$.

De la même manière, si $B_1 = \{\beta_1(n)\}$ et $B_2 = \{\beta_2(n)\}$ sont deux chaînes de Markov binaires indépendantes, $\beta_1(n)$ et $\beta_2(n)$ étant deux variables aléatoires binaires à valeurs dans l'ensemble $E_\beta$, nous dirons que la suite aléatoire binaire $H = \{\eta(n)\}$ est la somme modulo 2 de $B_1$ et $B_2$ lorsque: $\eta(n) = \beta_1(n)\oplus\beta_2(n)$ pour tout $n \in N$, $\eta(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\beta$.

Nous avons vu qu'il existe un isomorphisme L entre les deux ensembles $E_\xi$ et $E_\beta$ (définition 2.2). Si $\xi$ et $\beta$ sont deux variables aléatoires binaires à valeurs respectivement dans les ensembles $E_\xi$ et $E_\beta$, alors $\xi = L(\beta)$. Cela signifie que: $\xi(n) = L(\beta(n))$ et (Table 2.1) $\xi_1(n)\cdot\xi_1(n) = L(\beta_1(n)\oplus\beta_2(n))$.

C'est dans ce sens que l'opération produit (de deux chaînes de Markov) correspond à l'opération somme modulo 2 (de deux chaînes de Markov) justifiant ainsi la conjonction "ou" présente dans le titre de ce sous-chapitre.

Considérons la suite aléatoire binaire $H$ résultant de la somme modulo 2 des chaînes de Markov binaires $B_1$ et $B_2$ respectivement d'ordre $r_1$ et $r_2$, $r_1 \geq r_2$ (Fig. 4.3).

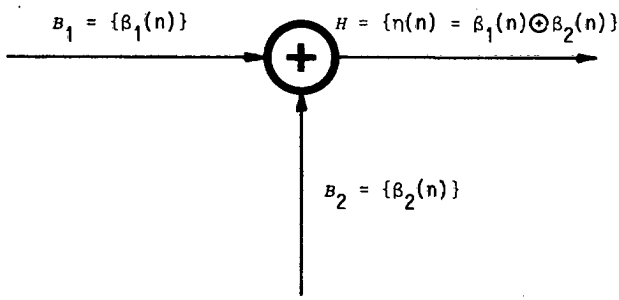



*Fig. 4.3: Suite aléatoire binaire $H$ résultant de la somme modulo 2 de deux chaînes de Markov binaires $B_1$ et $B_2$.*

Sous quelles conditions la suite aléatoire binaire $H$ est-elle aussi une chaîne de Markov binaire d'ordre r ?

Algorithme.

Supposons que $B$ soit une chaîne de Markov binaire d'ordre s avec matrice des probabilités de transition $\Pi_s = \{\pi_0\ \pi_1\ \cdots\ \pi_{2^s-1}\}$. Nous savons que le vecteur des probabilités conjointes $P_s$ de s variables aléatoires binaires successives (à valeurs dans l'ensemble $E_B$) est égal au vecteur transposé $\tilde{p}_s^T$ des probabilités des états de la chaîne. Grâce à la matrice $\Pi_s$, nous pouvons facilement construire le vecteur des probabilités conjointes $P_{s+1}$ de s+1 variables aléatoires binaires successives:

$$P_s = \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{2^s-1} \end{bmatrix} \xrightarrow{\Pi_s} P_{s+1} = \begin{bmatrix} p_0\pi_0 \\ p_0(1-\pi_0) \\ p_1\pi_1 \\ p_1(1-\pi_1) \\ \vdots \\ p_{2^s-1}\pi_{2^s-1} \\ p_{2^s-1}(1-\pi_{2^s-1}) \end{bmatrix} = \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ \vdots \\ q_{2^{s+1}-2} \\ q_{2^{s+1}-1} \end{bmatrix}.$$

De la même manière, en partant de $P_{s+1}$, il nous est facile de construire le vecteur des probabilités conjointes $P_{s+2}$ de s+2 variables aléatoires binaires successives:

$$P_{s+1} = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{2^{s+1}-1} \end{bmatrix} \xrightarrow{\Pi_s} P_{s+2} = \begin{bmatrix} q_0\pi_0 \\ q_0(1-\pi_0) \\ \vdots \\ q_{2^s-1}(1-\pi_{2^s-1}) \\ q_{2^s}\pi_0 \\ q_{2^s}(1-\pi_0) \\ \vdots \\ q_{2^{s+1}-1}(1-\pi_{2^s-1}) \end{bmatrix} = \begin{bmatrix} \tilde{q}_0 \\ \tilde{q}_1 \\ \vdots \\ \tilde{q}_{2^{s+2}-1} \end{bmatrix}.$$

Soit k un nombre pair, $0 \leq k < 2^{s+2}-1$. Posons:

$$a_k = \frac{\tilde{q}_k}{\tilde{q}_{k+1}}.$$

Or, par construction, ce rapport vaut:

$$a_k = \frac{\pi_{k/2}}{1-\pi_{k/2}}, \quad \tilde{q}_{k+1} = 0 \text{ alors } \pi_{k/2} = 1.$$

On peut retrouver la probabilité de transition $\pi_{k/2}$:

$$\pi_{k/2} = \frac{a_k}{1+a_k}.$$

Définissons un vecteur $V_{s+2}$ contenant les probabilités de transition $\pi_{k/2}$:

$$V_{s+2} = [\pi_0 \ \pi_1 \ \text{---} \ \pi_{2^{s+1}-1}]^T.$$

Mais, pour toute chaîne de Markov binaire $B$ d'ordre s, le vecteur $V_{s+2}$ est tel que:

$$V_{s+2} = [\pi_0 \ \pi_1 \ \text{---} \ \pi_{2^s-1} \ \pi_0 \ \pi_1 \ \text{---} \ \pi_{2^s-1}]^T. \tag{4.11}$$

Appliquons cet algorithme à la suite aléatoire binaire $H$ (Fig. 4.3). Heureusement, si $H$ est une chaîne de Markov binaire, son ordre r est borné par: $r \leq 2r_1+r_2$ ($r_1$ et $r_2$ étant l'ordre respectivement des chaînes $B_1$ et $B_2$ produisant $H$) [19].

En utilisant le théorème 3.4, il nous est facile de construire le vecteur des probabilités conjointes $P_{2r_1+r_2+2}(H)$ de $2r_1+r_2+2$ variables aléatoires binaires successives (la statistique des chaînes de Markov binaires $B_1$ et $B_2$ est évidemment connue).

De là, nous pouvons trouver le vecteur correspondant $V_{2r_1+r_2+2}(H)$. Si celui-ci est de la même forme que le vecteur donné en (4.11), alors $H$ est une chaîne de Markov binaire d'ordre égal ou inférieur à $2r_1+r_2$. Sinon, $H$ n'est pas une chaîne de Markov binaire (voir appendice B).

N.B.

Dans le but d'alléger la notation de ce paragraphe, nous avons utilisé le symbole $\pi_i$ pour désigner une probabilité de transition au lieu de $\pi_{i2i \bmod 2^r}$.

Exemple 4.6:

Soient deux chaînes de Markov binaires du premier ordre $B_1$ et $B_2$ avec respectivement matrices des probabilités de transition:

1) $\Pi_{1_1} = \{0.8\ 0.2\}$ et $\Pi_{2_1} = \{0.9\ 0.1\}$, alors:

$H = B_1 \oplus B_2$ est une chaîne de Markov binaire d'ordre égal ou inférieur à trois.

2) $\Pi_{1_1} = \{0.8\ 0.2\}$ et $\Pi_{2_1} = \{0.1\ 0.7\}$, alors:

$H = B_1 \oplus B_2$ n'est pas une chaîne de Markov.

Somme modulo 2 de deux chaînes de Markov binaires indépendantes du même ordre.

Etudions le cas intéressant dans lequel les deux chaînes de Markov binaires (indépendantes) $B_1$ et $B_2$ sont du même ordre, disons r. On se demande alors si la suite aléatoire binaire $H = B_1 \oplus B_2$ (Fig. 4.3) peut aussi être une chaîne de Markov binaire du même ordre, c'est-à-dire d'ordre r.

Fire [19] en examinant cette question trouve que:

> Si $B_1$ et $B_2$ sont deux chaînes de Markov binaires indépendantes d'ordre r avec respectivement matrices des probabilités de transition doublement stochastiques (définition 4.6) $\Pi_{1_r}$ et $\Pi_{2_r}$ dont les éléments non nuls ne peuvent prendre que l'une des deux valeurs disons $\pi_1$ ou $1-\pi_1$ pour $\Pi_{1_r}$ et $\pi_2$ ou $1-\pi_2$ pour $\Pi_{2_r}$, alors:
> $H = B_1 \oplus B_2$ est aussi une chaîne de Markov binaire d'ordre r avec matrice des probabilités de transition doublement stochastique dont les éléments non nuls ne peuvent prendre que l'une des deux valeurs:
>
> $$\pi = \pi_1\pi_2 + (1-\pi_1)(1-\pi_2),$$
> $$1-\pi = \pi_1(1-\pi_2) + (1-\pi_1)\pi_2.$$

Bien que les conditions énoncées ci-dessus soient nécessaires, elles ne sont (contrairement à ce qu'affirme Fire [19]) pas suffisantes comme l'illustre l'exemple suivant.

Exemple 4.7:

Soient deux chaînes de Markov binaires du second ordre $B_1$ et $B_2$ avec respectivement matrices des probabilités de transition:

$$\Pi_{1_r} = \{0.8\ 0.2\ 0.2\ 0.8\},$$

$$\Pi_{2_r} = \{0.8\ 0.8\ 0.2\ 0.2\}.$$

Ces deux matrices des probabilités de transition satisfont bien aux conditions énoncées précédemment [19]. Pourtant, en utilisant l'algorithme développé auparavant, nous trouvons que $H = B_1 \oplus B_2$ n'est pas une chaîne de Markov binaire.

Théorème 4.3:

Soient $B_1 = \{\beta_1(n)\}$ et $B_2 = \{\beta_2(n)\}$, $\beta_1(n)$ et $\beta_2(n)$ sont deux variables aléatoires binaires à valeurs dans l'ensemble $E_\beta$, deux chaînes de Markov binaires indépendantes d'ordre r avec respectivement matrices des probabilités de transition

$$\Pi_{1_r} = \{\pi_{1_{00}}\ \pi_{1_{12}}\ \text{---}\ \pi_{1_{2^r-1 2^r-2}}\} \text{ et}$$

$$\Pi_{2_r} = \{\pi_{2_{00}}\ \pi_{2_{12}}\ \text{---}\ \pi_{2_{2^r-1 2^r-2}}\}.$$

Soit la suite aléatoire binaire $H = \{\eta(n)\} = B_1 \oplus B_2$, $\eta(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\beta$.
Alors, pour que $H$ soit une chaîne de Markov binaire d'ordre r, il faut que les éléments non nuls des matrices $\Pi_{1_r}$ et $\Pi_{2_r}$ ne prennent que l'une des deux valeurs disons $\pi_1$ ou $1-\pi_1$ pour $\Pi_{1_r}$ et $\pi_2$ ou $1-\pi_2$ pour $\Pi_{2_r}$.

Démonstration:

Considérons la probabilité $\pi_{00}$ de la transition de $\{\eta(n) = 0, \text{---}, \eta(n-r) = 0\}$ à $\{\eta(n+1) = 0, \text{---}, \eta(n-r+1) = 0\}$. Par construction, cette probabilité s'obtient à partir de $\Pi_{1_r}$ et $\Pi_{2_r}$:

$$\pi_{00} = \pi_{1_{00}}\pi_{2_{00}} + (1-\pi_{1_{00}})(1-\pi_{2_{00}}) \text{ ou } \pi_{1_{12}}\pi_{2_{12}} + (1-\pi_{1_{12}})(1-\pi_{2_{12}}) \text{ ou}$$

$$\text{ou } \text{---} \text{ ou } \pi_{1_{2^r-1 2^r-2}}\pi_{2_{2^r-1 2^r-2}} + (1-\pi_{1_{2^r-1 2^r-2}})(1-\pi_{2_{2^r-1 2^r-2}}).$$

Examinons la relation:

$$\pi_{00} = \pi_{1_{ij}}\pi_{2_{ij}} + (1-\pi_{1_{ij}})(1-\pi_{2_{ij}}) \ , \ j = 2i \bmod 2^r, \ 0 \leq i \leq 2^r-1. \quad (4.12$$

Si nous considérons, par exemple, $\pi_{2_{ij}}$ comme un paramètre, l'expression (4.12) se réduit à un faisceau de droites (Fig. 4.4).

Pour que $H = B_1 \odot B_2$ soit une chaîne de Markov binaire d'ordre r, il faut évidemment que $\pi_{00}$ soit constante (droite horizontale dans la figure 4.4). Ceci implique, par exemple:

$$\pi_{00} = \pi_{1_{00}}\pi_{2_{00}} + (1-\pi_{1_{00}})(1-\pi_{2_{00}}) = \pi_{1_{12}}\pi_{2_{12}} + (1-\pi_{1_{12}})(1-\pi_{2_{12}}).$$

Ces deux égalités sont représentées, dans la figure 4.4, respectivement par les intersections a et b.

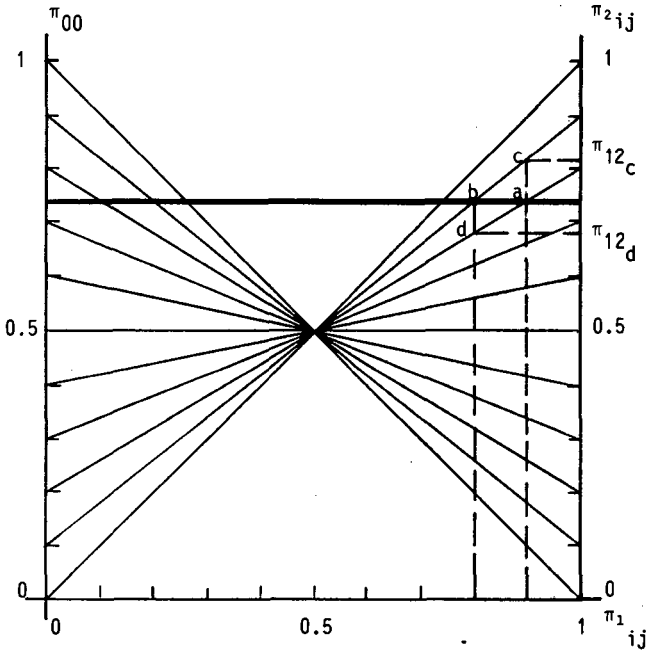



*Fig. 4.4: Graphe de la relation:* $\pi_{00} = \pi_{1_{ij}}\pi_{2_{ij}} + (1-\pi_{1_{ij}})(1-\pi_{2_{ij}})$.

Considérons maintenant la probabilité $\pi_{12}$ de la transition de $\{\eta(n) = 1, \eta(n-1) = 0, ---, \eta(n-r) = 0\}$ à $\{\eta(n+1) = 0, \eta(n) = 1, \eta(n-1) = 0, ---, \eta(n-r+1) = 0\}$. Ici aussi, pour que $H = B_1 \oplus B_2$ soit une chaîne de Markov binaire d'ordre r, il faut que $\pi_{12}$ soit constante. Mais, par exemple, cette probabilité vaut (par construction)

$$\pi_{1_{00}}\pi_{2_{12}} + (1-\pi_{1_{00}})(1-\pi_{2_{12}}) \text{ ou } \pi_{1_{12}}\pi_{2_{00}} + (1-\pi_{1_{12}})(1-\pi_{2_{00}}).$$

Ces deux grandeurs sont respectivement représentées, dans le figure 4.4, par les intersections c et d. Or, nous constatons que les valeurs résultantes $\pi_{12_c}$ et $\pi_{12_d}$ ne sont plus égales comme elles devraient l'être. Il y a donc contradiction. De la même manière, on peut facilement se convaincre que cette conclusion s'impose pour toute autre transition possible.

Ainsi, pour lever ladite contradiction, il faut que les éléments non nuls des matrices $\Pi_{1_r}$ et $\Pi_{2_r}$ ne prennent que l'une des deux valeurs disons $\pi_1$ ou $1-\pi_1$ pour $\Pi_{1_r}$ et $\pi_2$ ou $1-\pi_2$ pour $\Pi_{2_r}$.

*CQFD.*

Toute chaîne de Markov binaire $B = \{\beta(n)\}$ d'ordre r, $\beta(n)$ étant une variable aléatoire binaire à valeurs dans l'ensemble $E_\beta$, avec matrice des probabilités de transition $\Pi_r$ dont les éléments non nuls ne peuvent valoir que l'une des deux valeurs disons $\pi$ ou $1-\pi$, peut être générée à partir d'un filtre numérique récursif couplé à une source binaire sans mémoire pour laquelle $P\{\alpha(n) = 0\} = \pi$, abrégée SBSM $\pi$, $\alpha(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\beta$, (Fig. 4.5).

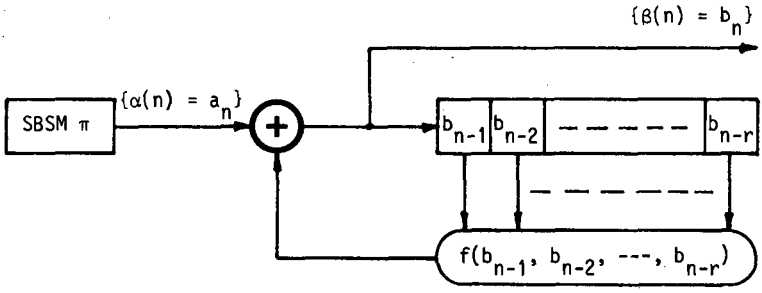



*Fig. 4.5: Filtre numérique récursif couplé à une source binaire sans mémoire générant une chaîne de Markov binaire d'ordre r.*

Ce type de représentation nous a été suggéré par Mr. le Professeur Massey.

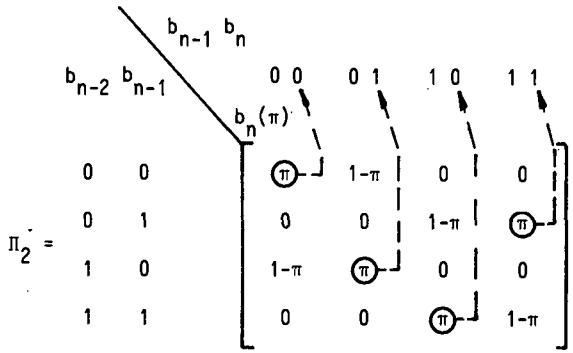
En effet, par définition $P\{\alpha(n) = 0\} = \pi$. Donc, avec probabilité $\pi$, la variable aléatoire binaire $\beta(n)$ vaut $f(b_{n-1}, b_{n-2}, ---, b_{n-r})$. Notons cette valeur $b_n(\pi)$:

$$b_n(\pi) = f(b_{n-1}, b_{n-2}, ---, b_{n-r}).$$

Ainsi, $b_n(\pi)$ représente la fonction de sortie d'un système logique combinatoire dont les entrées sont les $2^r$ états possibles de la chaîne. La matrice des probabilités de transition $\Pi_r$ est alors liée de manière unique à la fonction booléenne $f(b_{n-1}, b_{n-2}, ---, b_{n-r})$.

Exemple 4.8:

Considérons une des chaînes de Markov binaires du second ordre générée à partir d'un filtre numérique récursif couplé à une SBSM $\pi$.




| $b_{n-2}$ | $b_{n-1}$ | $b_n(\pi)$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

$$b_n(\pi) = b_{n-1} \oplus b_{n-2} = f(b_{n-1}, b_{n-2}).$$

Théorème 4.4:

Soient $B_1 = \{\beta_1(n)\}$ et $B_2 = \{\beta_2(n)\}$ deux chaînes de Markov binaires indépendantes d'ordre r, $\beta_1(n)$ et $\beta_2(n)$ deux variables aléatoires binaires à valeurs dans l'ensemble $E_\beta$, générées par deux filtres numériques récursifs, caractérisés respectivement par les fonctions booléennes $f_1(b'_{n-1}, b'_{n-2}, ---, b'_{n-r})$ et $f_2(b''_{n-1}, b''_{n-2}, ---, b''_{n-r})$, couplés respectivement aux SBSM $\pi_1$ et $\pi_2$.
$H = \{\eta(n)\} = B_1 \odot B_2$ est aussi une chaîne de Markov binaire d'ordre r, $\eta(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\beta$, générée par un filtre numérique récursif caractérisé par la fonction booléenne $f(h_{n-1}, h_{n-2}, ---, h_{n-r})$ couplé à la SBSM $\pi$, si et seulement si:

- $f_1 = f_2 = f$ et

- f est une fonction booléenne linéaire.

Démonstration:

a) *Implication dans le sens* $\Longrightarrow$ :

Soient $a'_n$ et $a''_n$ les réalisations des variables aléatoires binaires $\alpha_1(n)$ et $\alpha_2(n)$ (à valeurs dans l'ensemble $E_\beta$) avec $P\{\alpha_1(n) = 0\} = \pi_1$ et $P\{\alpha_2(n) = 0\} = \pi_2$ (Fig. 4.5).

Pour simplifier la notation, nous n'écrirons, dans cette preuve, que les réalisations des variables aléatoires binaires considérées, à valeurs dans l'ensemble $E_\beta$.

Ainsi, nous avons (Fig. 4.5):

$$b'_n = a'_n \odot f_1(b'_{n-1}, b'_{n-2}, ---, b'_{n-r}),$$
$$b''_n = a''_n \odot f_2(b''_{n-1}, b''_{n-2}, ---, b''_{n-r}).$$

Mais:

$$h_n = b'_n \odot b''_n = a'_n \odot a''_n \odot f_1(b'_{n-1}, ---, b'_{n-r}) \odot f_2(b''_{n-1}, ---, b''_{n-r}). \quad (4.13)$$

Nous pouvons récrire (4.13) comme suit:

$$h_n = a_n \odot f(b'_{n-1}, ---, b'_{n-r}; b''_{n-1}, ---, b''_{n-r}). \quad (4.14)$$

Si nous voulons que la suite aléatoire binaire $H$ soit aussi une chaîne de Markov binaire d'ordre r, la relation (4.14) doit s'identifier à:

$$h_n = a_n \oplus f(h_{n-1}, h_{n-2}, \text{---}, h_{n-r}). \qquad (4.15$$

Or, toute fonction booléenne $g(y_{n-1}, y_{n-2}, \text{---}, y_{n-r})$ peut s'écrire sous la forme [3]:

$$g(y_{n-1}, \text{---}, y_{n-r}) = d_0 \oplus d_1 y_{n-1} \oplus \text{---} \oplus d_r y_{n-r} \oplus d_{12} y_{n-1} y_{n-2} \oplus \text{--}$$
$$\text{-- } \oplus d_{12 \text{ --- } r} y_{n-1} y_{n-2} \text{ --- } y_{n-r}. \qquad (4.16$$

Développons selon (4.16) les fonctions booléennes $f_1$ et $f_2$:

$$f_1(b'_{n-1}, \text{---}, b'_{n-r}) = d'_0 \oplus d'_1 b'_{n-1} \oplus \text{---} \oplus d'_r b'_{n-r} \oplus d'_{12} b'_{n-1} b'_{n-2} \oplus \text{--}$$
$$\text{-- } \oplus d'_{12 \text{ --- } r} b'_{n-1} b'_{n-2} \text{ --- } b'_{n-r}.$$

$$f_2(b''_{n-1}, \text{---}, b''_{n-r}) = d''_0 \oplus d''_1 b''_{n-1} \oplus \text{---} \oplus d''_r b''_{n-r} \oplus d''_{12} b''_{n-1} b''_{n-2} \oplus \text{--}$$
$$\text{-- } \oplus d''_{12 \text{ --- } r} b''_{n-1} b''_{n-2} \text{ --- } b''_{n-r}.$$

Ainsi:

$$f_1(b'_{n-1}, \text{--- } b'_{n-r}) \oplus f_2(b''_{n-1}, \text{---}, b''_{n-r}) =$$
$$= d'_0 \oplus d''_0 \oplus (d'_1 b'_{n-1} \oplus d''_1 b''_{n-1}) \oplus \text{---} \oplus (d'_r b'_{n-r} \oplus d''_r b''_{n-r}) \oplus$$
$$\oplus (d'_{12} b'_{n-1} b'_{n-2} \oplus d''_{12} b''_{n-1} b''_{n-2}) \oplus \text{---} \oplus (d'_{12 \text{ --- } r} b'_{n-1} \text{ --- } b'_{n-r} \oplus$$
$$\oplus d''_{12 \text{ --- } r} b''_{n-1} \text{ --- } b''_{n-r}),$$

et:

$$f(h_{n-1}, \text{---}, h_{n-r}) = d_0 \oplus d_1 h_{n-1} \oplus \text{---} \oplus d_r h_{n-r} \oplus d_{12} h_{n-1} h_{n-2} \oplus \text{--}$$
$$\text{-- } \oplus d_{12 \text{ --- } r} h_{n-1} \text{ --- } h_{n-r} =$$
$$= d_0 \oplus d_1 (b'_{n-1} \oplus b''_{n-1}) \oplus \text{---} \oplus d_r (b'_{n-r} \oplus b''_{n-r}) \oplus$$
$$\oplus d_{12} (b'_{n-1} \oplus b''_{n-1})(b'_{n-2} \oplus b''_{n-2}) \oplus \text{--}$$
$$\text{-- } \oplus d_{12 \text{ --- } r} (b'_{n-1} \oplus b''_{n-1}) \text{ --- } (b'_{n-r} \oplus b''_{n-r}).$$

Donc, pour que les relations (4.13) et (4.15) soient identiques, il faut que:

- Tous les coefficients des développements des fonctions booléennes $f_1$, $f_2$ et f soient identiques, d'où la condition: $f_1 = f_2 = f$.

- Tous les coefficients liés aux termes non linéaires doivent être nuls, d'où la condition: f est une fonction booléenne linéaire.

On constate que, dans l'expression (4.14), $a_n$ est la réalisation d'une variable aléatoire binaire $\alpha(n)$, à valeurs dans l'ensemble $E_\beta$, avec:

$$\{\alpha(n) = a_n\} = \{\alpha_1(n) = a'_n\} \oplus \{\alpha_2(n) = a''_n\}.$$

Ainsi:

$$P\{\alpha(n) = 0\} = \pi = \pi_1\pi_2 + (1-\pi_1)(1-\pi_2).$$

*b)* *Implication dans le sens* $\Longleftarrow$ *:*

Trivial.

CQFD.

Remarquons que le théorème 4.4 implique l'équivalence statistique entre les systèmes donnés dans la figure 4.6.

Pour terminer, démontrons un petit théorème qui nous sera utile dans le prochain chapitre.

Théorème 4.5:

Toute fonction booléenne f caractérisant un filtre numérique récursif, couplé à une SBSM $\pi$, permet de générer une chaîne de Markov binaire d'ordre r avec matrice des probabilités de transition doublement stochastique $\Pi_r$, dont les éléments non nuls ne peuvent prendre que l'une des deux valeurs disons $\pi$ et $1-\pi$, si et seulement si:

$$f(b_{n-1}, b_{n-2}, \text{---}, b_{n-r}) = b_{n-r} \oplus f^*(b_{n-1}, b_{n-2}, \text{---}, b_{n-r+1}).$$

Démonstration:

Pour simplifier la notation, nous n'écrirons, dans cette preuve, que les réalisations des variables aléatoires binaires considérées, à valeurs dans l'ensemble $E_\beta$.

*a)* *Implication dans le sens* $\Longrightarrow$ *:*

Par hypothèse, $\Pi_r$ est doublement stochastique. Donc, la SBSM $\pi$ générant un zéro logique avec probabilité $\pi$ implique:

$$b_n = f(b_{n-1}, ---, b_{n-r+1}, 0) \qquad \text{avec probabilité } \pi$$

$$b_n = 1 \oplus f(b_{n-1}, ---, b_{n-r+1}, 0) \qquad \text{avec probabilité } \pi.$$

Nous avons donc, $f(b_{n-1}, ---, b_{n-r+1}, 0) = f^*(b_{n-1}, ---, b_{n-r+1})$:

| $b_{n-r}$ | $b_n$ |
|---|---|
| 0 | $f^*(b_{n-1}, ---, b_{n-r+1})$ |
| 1 | $1 \oplus f^*(b_{n-1}, ---, b_{n-r+1})$ |

ce qui implique:

$$b_n = b_{n-r} \oplus f^*(b_{n-1}, ---, b_{n-r+1})$$

pour toute fonction booléenne f*.

*b)* *Implication dans le sens* $\Longleftarrow$ *:*

Pour toute fonction booléenne f* donnée:

$$b_{n_1} = 0 \oplus f^*(b_{n-1}, ---, b_{n-r+1}) \qquad \text{avec probabilité } \pi$$

$$b_{n_2} = 1 \oplus f^*(b_{n-1}, ---, b_{n-r+1}) = 1 \oplus b_{n_1} \qquad \text{avec probabilité } \pi.$$

Dès lors, il est évident que la matrice des probabilités de transition $\Pi_r$ associée à ce filtre est doublement stochastique (ses éléments non nuls ne valant que $\pi$ ou $1-\pi$).

*CQFD.*

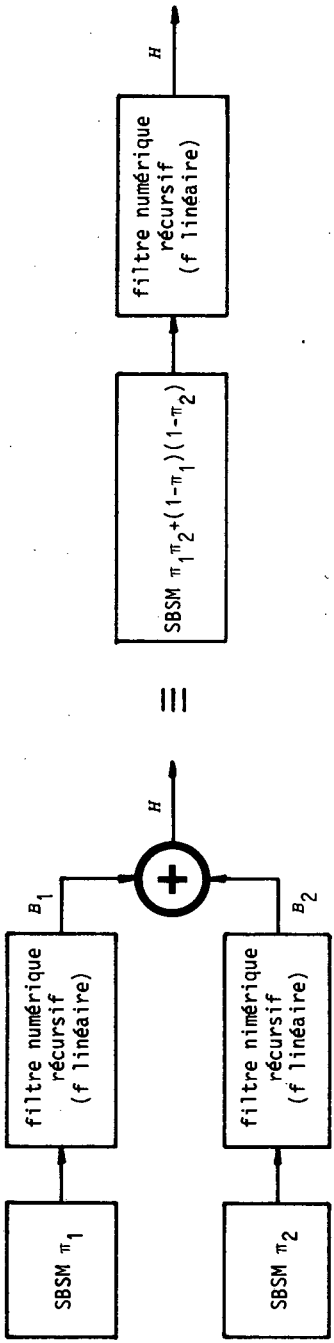



*Fig. 4.6: Equivalence statistique entre systèmes générant la chaîne de Markov binaire H.*

# V. APPLICATION: SUITES PSEUDO-ALEATOIRES BINAIRES.

Nous allons étudier dans ce chapitre, quelques aspects des suites pseudo-aléatoires binaires, générées par filtres numériques récursifs, en utilisant la théorie relative aux chaînes de Markov binaires. Une telle possibilité a été évoquée par Golomb [23], mais il nous semble que personne, depuis, n'y a donné suite (en tout cas dans la littérature consultée).

## V.1. Introduction.

Nous avons vu dans le chapitre IV qu'un filtre numérique récursif (caractérisé par une fonction booléenne $f(b_{n-1}, b_{n-2}, ---, b_{n-r})$) couplé à une SBSM $\pi$ (Fig. 4.5) produit une chaîne de Markov binaire d'ordre r. Si maintenant nous imposons à la SBSM de ne générer que des zéros logiques, $\pi = 1$, nous obtenons une chaîne de Markov binaire dégénérée d'ordre r (Fig. 5.1).

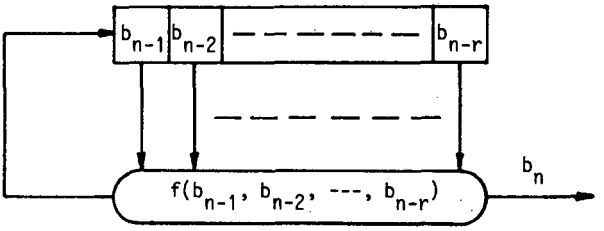



*Fig. 5.1: Filtre numérique récursif générant une suite pseudo-aléatoire binaire.*

Ici, la matrice des probabilités de transition ne contient que des zéros et des uns: la suite binaire ainsi produite n'est plus aléatoire mais déterministe.

Cependant, toutes les applications pratiques (mesures, simulations, etc ...) sont limitées dans le temps. Ainsi, celles nécessitant l'utilisation de suites de nombres aléatoires et plus particulièrement de suites de nombres aléatoires binaires n'impliquent qu'une portion finie de telles suites. Or, il faut bien se rendre compte qu'une suite finie de nombres n'est jamais vraiment aléatoire [23]. La définition de critères permettant de quantifier son degré "d'aléatoirité" s'impose alors. Ils doivent être suffisamment raisonnables pour ne pas contredire le concept intuitif de suite aléatoire, c'est-à-dire de suite "dépourvue de structure interne" [10,32].

Dans ce sens, les suites binaires générées par un filtre numérique récursif (Fig. 5.1) sont "assez aléatoires" pour de nombreuses applications. Aussi, nous les appellerons suites pseudo-aléatoires binaires, abrégées SPAB [23]. Une SBPA représente ici, une chaîne de Markov binaire dégénérée dont tous les états ont même probabilité.

L'ensemble des SPAB peut se diviser en deux classes:

- La classe $C_L$ des SPAB générées par les filtres numériques récursifs linéaires.

- La classe $C_{NL}$ des SPAB générées par les filtres numériques récursifs non linéaires.

On constate que toute SPAB est périodique (excepté peut-être pour un segment initial fini) [23].

Nous nous concentrerons sur les SPAB de période maximale appelées suites PN si elles appartiennent à $C_L$ [23] et suites de de Bruijn si elles appartiennent à $C_{NL}$ [21].

Les fonctions booléennees linéaires $f_L(b_{n-1}, b_{n-2}, ---, b_{n-r})$ liées aux suites PN sont bien définies. Elles correspondent aux polynômes primitifs modulo 2 de degré r [52]. Pour chaque entier r, il y en a $\phi(2^r-1)/r$ [23] où $\phi(1)$ dénote la fonction d'Euler [1].

Par contre, dans la littérature consultée, il n'est pas fait explicitement mention des caractéristiques nécessaires liées aux fonctions booléennes non linéaires $f_{NL}(b_{n-1}, b_{n-2}, ---, b_{n-r})$ permettant de générer les suites de de Bruijn. On sait que pour chaque entier r, il y en a $2^{2^{r-1}-r}$ [20]. Il existe cependant de nombreux algorithmes construits dans le but de produire de telles suites [3,17,20,21].

Finalement, notons que le domaine d'application des SPAB est vaste. Citons par exemple: la cryptographie [15,42,53], le test de circuits numériques [9,13,14], la théorie du codage [41] et enfin les communications utilisant la technique dite "spread-spectrum" [11].

*Rappel:*

Nous avons vu (voir IV.4) que tout filtre numérique récursif est lié de manière unique à la matrice des probabilités de transition d'une chaîne de Markov binaire. En effet, l'état de la chaîne contenu dans la mémoire (registre à décalage) du filtre représente les entrées codées d'une table de vérité alors que la sortie $b_n$ (Fig. 5.1) de ce filtre correspond à la fonction de sortie de ladite table de vérité (voir exemple 4.8 en posant ici $\pi = 1$).

## V.2. Quelques propriétés des filtres numériques récursifs générateurs de suites de de Bruijn.

Nous avons constaté précédemment qu'une suite de de Bruijn correspond à une chaîne de Markov binaire dégénérée, c'est-à-dire une chaîne de Markov binaire avec matrice des probabilités de transition $\Pi_r$ ne contenant que des zéros et des uns (Fig. 5.1). Etant donné la structure particulière de $\Pi_r$ (voir relation (4.2)), elle s'identifie à une matrice de permutations.

Théorème 5.1:

Une chaîne de Markov binaire dégénérée d'ordre r avec matrice des probabilités de transition $\Pi_r$ est une suite de de Bruijn si et seulement si $\Pi_r$ est irréductible.

Démonstration:

a) *Implication dans le sens* $\Longrightarrow$ :

Puisque toute suite de de Bruijn est par définition une SPSB de période maximale, la chaîne de Markov binaire dégénérée correspondante, se trouvant dans un état initial $i_0$, passe successivement par tous ses autres états avant de se retrouver dans l'état de départ $i_0$.

Par définition, cette chaîne de Markov binaire dégénérée est irréductible (voir IV.1).

b) *Implication dans le sens* $\Longleftarrow$ :

Si $\Pi_r$ est irréductible, la chaîne de Markov binaire dégénérée d'ordre r correspondante est par définition équivalente à une suite de de Bruijn.

*CQFD.*

Le théorème 5.1 ainsi que la définition de la périodicité d'une chaîne de Markov (voir IV.1) nous permettent de trouver qu'une suite de de Bruijn est de période $2^r$. Par conséquent, puisqu'une suite PN est de période $2^r-1$ [23], il est impossible de générer une suite de de Bruijn avec un filtre numérique récursif linéaire (sauf, nous le verrons plus loin, pour $r \leq 2$).

Théorème 5.2:

Toute suite de de Bruijn ne peut être générée que par un filtre numérique récursif ayant la propriété suivante:

$$f(b_{n-1}, ---, b_{n-r}) = b_{n-r} \oplus f(b_{n-1}, ---, b_{n-r+1}).$$

Démonstration:

Par le théorème 5.1, nous avons vu que toute suite de de Bruijn correspond à une chaîne de Markov binaire dégénérée avec matrice des probabilités de transition irréductible. Cela implique évidemment que cette matrice soit doublement stochastique.

Si ce n'est pas le cas, au moins deux lignes de la matrice des probabilités de transition sont identiques, disons la ligne i, $0 \leq i \leq 2^{r-1}-1$, et la ligne correspondante $i+2^{r-1}$. Ceci signifie que les états i et $i+2^{r-1}$ transitent sur, disons, $2i \bmod 2^r$. Ainsi, l'état $2i \bmod 2^r + 1$ n'est jamais atteint (sauf peut-être sur un segment initial fini). Cette matrice des probabilités de transition n'est donc pas irréductible.

En conclusion, la matrice des probabilités de transition étant doublement stochastique, nous obtenons (théorème 4.5):

$$f(b_{n-1}, \text{---}, b_{n-r}) = b_{n-r} \oplus g(b_{n-1}, \text{---}, b_{n-r+1}).$$

CQFD.

Pour que la matrice des probabilités de transition d'une chaîne de Markov binaire dégénérée soit irréductible, il faut que:

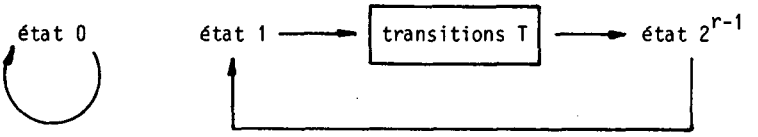
$$\Pi_r = \begin{bmatrix} 0 & 1 & & & & 0 & 0 \\ 0 & 0 & & & & \vdots & \vdots \\ \vdots & \vdots & & & & \vdots & \vdots \\ \vdots & \vdots & & & & 0 & 0 \\ 0 & 0 & & & & 0 & 1 \\ 1 & 0 & & * & & 0 & 0 \\ 0 & 0 & & & & \vdots & \vdots \\ \vdots & \vdots & & & & \vdots & \vdots \\ \vdots & \vdots & & & & 0 & 0 \\ 0 & 0 & & & & 1 & 0 \end{bmatrix}.$$

En effet, si $\pi_{00} = 1$ et/ou $\pi_{2^r-1 2^r-1} = 1$, les états correspondants sont absorbants (points fixes) et la matrice $\Pi_r$ n'est plus irréductible [18].

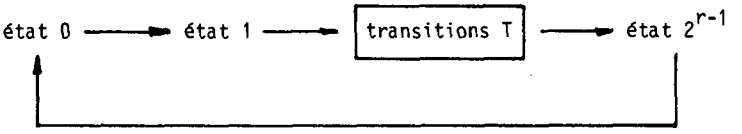
Définition 5.1:

*L'ensemble* S *[24] est l'ensemble des SPAB de période* $2^r-1$. *Chacune d'elles est une chaîne de Markov binaire dégénérée avec matrice des probabilités de transition* $\hat{\Pi}_r$ *appartenant à l'ensemble* $S_\Pi$ *des matrices* diag {1 $\Pi_r^*$}, $\Pi_r^*$ *irréductible.*

Toute SPAB, élément de S, possède la structure suivante:




En permutant les deux premières colonnes de la matrice $\hat{\Pi}_r$ qui lui est associée, nous modifions cette SPAB pour obtenir:




Nous avons maintenant affaire à une suite de de Bruijn. En fait, toute suite de de Bruijn peut être construite de cette manière. Nous en concluons que l'ensemble S contient aussi $2^{2^{r-1}-r}$ SPAB, dont $\phi(2^r-1)/r$ d'entre elles sont PN [24].

Remarquons que pour r = 1 et r = 2, les ensembles S respectifs ne contiennent qu'un seul élément. Dorénavant, nous ne considérerons que les chaînes de Markov binaires dégénérées d'ordre r > 2.

Il est évident qu'en permutant judicieusement les colonnes d'une matrice $\hat{\Pi}_{1_r}$ appartenant à $S_\Pi$, nous pouvons en obtenir une nouvelle, disons $\hat{\Pi}_{2_r}$, appartenant elle aussi à $S_\Pi$. Ainsi:

$$\hat{\Pi}_{1_r} = \hat{\Pi}_{2_r} \cdot C_{12_r},$$

où $C_{12_r}$ est une matrice de permutations.

Mais, nous avons vu que la position des éléments non nuls $\pi_{ij}$ de toute matrice des probabilités de transition $\Pi_r$ n'est pas arbitraire (voir (4.2)). Il n'y en a que deux dans chaque ligne i, $0 \leq i \leq 2^r-1$, placés dans les colonnes $2i \bmod 2^r$ et $2i \bmod 2^r + $ Donc, les seules permutations permises sont celles qui échangent deux colonnes j et j+1, j = 0, 2, ---, $2^r-2$.

Exemple 5.1:

Considérons le cas r = 3. L'ensemble $S_\Pi$ ne contient ici que deux éléments, à savoir:

$$\hat{\Pi}_{1_3} = \begin{bmatrix} 1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & & & 1 & 0 & & \\ 0 & 1 & & & & & 0 & 1 \\ & & 1 & 0 & & & & \\ & & & & 0 & 1 & & \\ & & & & & & 1 & 0 \end{bmatrix} \quad \text{et} \quad \hat{\Pi}_{2_3} = \begin{bmatrix} 1 & 0 & & & & & & \\ & & 1 & 0 & & & & \\ & & & & 0 & 1 & & \\ 0 & 1 & & & & & 0 & 1 \\ & & 0 & 1 & & & & \\ & & & & 1 & 0 & & \\ & & & & & & 1 & 0 \end{bmatrix}.$$

On constate qu'on obtient $\hat{\Pi}_{2_3}$ en échangeant les colonnes 2 et 3 puis 4 et 5 de la matrice $\hat{\Pi}_{1_3}$. Donc, la matrice de permutations $C_{1_2 3}$ est la suivante:

$$C_{1_2 3} = \begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix}.$$

Théorème 5.3:

Si $\hat{\Pi}_{1_r}$ et $\hat{\Pi}_{2_r}$ sont deux matrices des probabilités de transition appartenant à l'ensemble $S_\Pi$ avec: $\hat{\Pi}_{2_r} = \hat{\Pi}_{1_r} \cdot C_{1_2 r}$, $C_{1_2 r}$ est une matrice permutant les colonnes de $\hat{\Pi}_{1_r}$, alors la signature de la permutation correspondant à $C_{1_2 r}$ est paire.

Démonstration:

Par la périodicité des éléments de l'ensemble S, toute matrice correspondante $\hat{\Pi}_r$ est telle que:

$$\hat{\Pi}_r^{2^r-1} = I_r.$$

Ainsi:

$$\det \hat{\Pi}_r = 1.$$

Nous avons:

$$\det \hat{\Pi}_{2_r} = \det(\hat{\Pi}_{1_r} \cdot C_{12_r}) = \det \hat{\Pi}_{1_r} \det C_{12_r} = 1.$$

Ainsi, $\det C_{12_r} = 1$ et la signature de la permutation associée à $C_{12_r}$ est paire [28].

*CQFD.*

Définition 5.2:

*Nous dénoterons par* $\hat{f}(b_{n-1}, ---, b_{n-r}) = b_{n-r} \oplus \hat{g}(b_{n-1}, ---, b_{n-r+1})$ *la fonction booléenne caractérisant tout filtre numérique récursif générant une SPAB appartenant à l'ensemble* S. *Si cette dernière est une suite* PN, *alors nous le spécifierons en posant* $\hat{f}_L(b_{n-1}, ---, b_{n-r}) = b_{n-r} \oplus \hat{g}_L(b_{n-1}, ---, b_{n-r+1})$.

Définition 5.3:

*Le poids de Hamming* W(f) *d'une fonction booléenne* $f(_{b-1}, ---, b_{n-r})$ *est défini comme étant la somme:*

$$W(f) = \sum_{(b_{n-1}, ---, b_{n-r}) \in E_\beta^r} f(b_{n-1}, ---, b_{n-r}).$$

Corollaire 5.1:

Le poids de Hamming $W(\hat{g})$ de toute fonction booléenne $\hat{g}(b_{n-1}, ---, b_{n-r+1})$ (liée à une SBPA $\in$ S) est un nombre entier pair.

Démonstration:

Pour chaque entier r, il existe au moins une fonction booléenne linéaire $\hat{f}_L(b_{n-1}, ---, b_{n-r}) = b_{n-r} \oplus \hat{g}_L(b_{n-1}, ---, b_{n-r+1})$ [23]. En permutant judicieusement les colonnes de la matrice des probabilités de transition qui lui est associée, on peut obtenir tout autre matrice $\hat{\Pi}_r$ appartenant à $S_\Pi$. Or le nombre de ces permutations doit être pair (théorème 5.3). Mais $W(\hat{g}_L)$ est un nombre entier pair (propriété des fonctions booléennes linéaires). On en conclut que le poids de Hamming $W(\hat{g})$ de toute fonction booléenne $\hat{g}(b_{n-1}, ---, b_{n-r+1})$ est aussi un nombre entier pair.

*CQFD.*

Théorème 5.4:

Soit $\hat{f}(b_{n-1}, ---, b_{n-r}) = b_{n-r} \oplus \hat{g}(b_{n-1}, ---, b_{n-r+1})$ la fonction booléenne linéaire caractérisant un filtre numérique récursif générant une SPAB appartenant à l'ensemble S, avec:

$$\hat{g}(b_{n-1}, ---, b_{n-r+1}) = a_0 \oplus a_1 b_{n-1} \oplus --- \oplus a_{r-1} b_{n-r+1} \oplus$$
$$\oplus a_{12} b_{n-1} b_{n-2} \oplus --- \oplus a_{1\ ---\ r-1} b_{n-1} --- b_{n-r+1}.$$

Alors:

a) $a_0 = 0$.

b) Le nombre total de coefficients non nuls $a_{l_1 l_2 --- l_m}$, $1 \leq l_1 < l_2 < --- < l_m \leq r-1$, est impair.

c) $a_{1\ ---\ r-1} = 0$.

Démonstration:

A toute SPAB appartenant à l'ensemble S, il correspond une chaîne de Markov binaire d'ordre r avec matrice des probabilités de transition $\hat{\Pi}_r$ appartenant à l'ensemble $S_\Pi$.

Celle-ci est telle que: $\pi_{00} = 1$ et $\pi_{2^{r-1}-12^r-1} = 1$. Donc:

a) $\pi_{00} = 1$, d'où $\hat{g}(0, ---, 0) = 0$, ainsi $a_0 = 0$.

b) $\pi_{2^{r-1}-12^r-1} = 1$, d'où $\hat{g}(1, ---, 1) = 1$, ainsi:

$$a_1 \oplus a_2 \oplus --- \oplus a_{r-1} \oplus a_{12} \oplus --- \oplus a_{12 \; --- \; r-1} = 1.$$

Ceci implique que le nombre total de coefficients non nuls $a_{l_1 l_2 \; --- \; l_m}$, $1 \leq l_1 < l_2 < --- < l_m \leq r-1$, est impair.

c) $a_1 \oplus a_2 \oplus --- \oplus a_{r-1} \oplus a_{12} \oplus --- \oplus a_{2 \; --- \; r-1} = 1 \oplus a_{1 \; --- \; r-1}$.

On constate facilement que:

$$\sum_{(b_{n-1}, ---, b_{n-r+1}) \in E_\beta^{r-1} - \{1, ---, 1\}} \hat{g}(b_{n-1}, ---, b_{n-r+1}) =$$

$$= a_1 \oplus a_2 \oplus --- \oplus a_{r-1} \oplus a_{12} \oplus --- \oplus a_{2 \; --- \; r-1},$$

où: $\sum_{i=1}^{n} d_i = d_1 \oplus d_2 \oplus --- \oplus d_n$.

Puisque $W(\hat{g})$ est un nombre pair et que $\hat{g}(1, ---, 1) = 1$, nous obtenons:

$$\sum_{(b_{n-1}, ---, b_{n-r+1}) \in E_\beta^{r-1} - \{1, ---, 1\}} \hat{g}(b_{n-1}, ---, b_{n-r+1}) = 1 \oplus a_{12 \; --- \; r-1} = 1.$$

Ainsi: $a_{12 \; --- \; r-1} = 0$.

*CQFD.*

Nous avons vu que toute suite de de Bruijn ne peut être génerée que par un filtre numérique récursif ayant la propriété suivante:

$$f(b_{n-1}, ---, b_{n-r}) = b_{n-r} \oplus g(b_{n-1}, ---, b_{n-r+1}). \qquad (5.1)$$

Il existe $N = 2^{2^{r-1}}$ tels filtres. Evidemment, cette propriété est aussi partagée par tout filtre générant une SPAB appartenant à l'ensemble S. En plus, toute fonction booléenne $\hat{g}(b_{n-1}, ---, b_{n-r+1})$ doit satisfaire les conditions nécessaires du théorème 5.4, ce qui implique:

- a et b $\Longrightarrow$ le nombre total k de coefficient non nuls dans le développement (4.16 de $\hat{g}(b_{n-1}, ---, b_{n-r+1})$ vaut au plus $2^{r-1} - 2$.

- c $\Longrightarrow$ k est impair.

Le nombre N* des fonctions booléennes possédant les propriétés combinées décrites par les théorèmes 5.2 et 5.4 vaut:

$$N^* = \sum_{l = 1, 3, ---}^{2^{r-1}-3} \binom{2^{r-1}-2}{l} = 2^{2^{r-1}-3} = \frac{N}{8}.$$

Dénotons par A, l'ensemble des SPAB générées par tout filtre numérique récursif satisfaisant la condition du théorème 5.2. Représentons dans un diagramme de Venn, A et ses différents sous-ensembles (Fig. 5.2).

Notons qu'à chaque SPAB appartenant à l'ensemble S, il correspond une et une seule suite de de Bruijn.

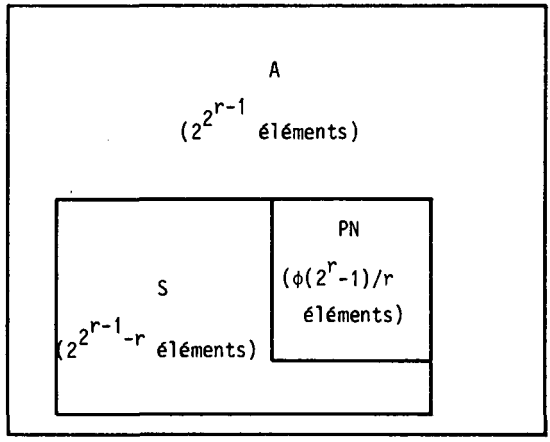



*Fig. 5.2: Diagramme de Venn représentant A et ses sous-ensembles.*

Exemple 5.3:

Examinons une SPAB de période 31 (on représente chaque état successif de la chaîne de Markov binaire dégénérée correspondante d'ordre 5) [20]:

1 3 7 14 29 27 23 15 31 30 28 25 19 6 13 26 21 11 22 12 24 17 2 4 9 18 5 10 20 8 6.

On montre facilement que le filtre numérique récursif générant cette SPAB est caractérisé par la fonction booléenne suivante:

$$\hat{f}(b_{n-1}, b_{n-2}, b_{n-3}, b_{n-4}, b_{n-5}) =$$
$$= b_{n-5} \oplus b_{n-1} \oplus b_{n-3} \oplus b_{n-1} b_{n-4} \oplus b_{n-3} b_{n-4} \oplus b_{n-2} b_{n-3} b_{n-4}.$$

Comment faut-il modifier $\hat{g}(b_{n-1}, ---, b_{n-r+1})$ pour que le filtre numérique récursif caractérisé par la fonction booléenne résultante génère une suite de de Bruijn

Définition 5.4:

*Nous dénoterons par* $f_B(b_{n-1}, ---, b_{n-r}) = b_{n-r} \oplus g_B(b_{n-1}, ---, b_{n-r+1})$ *la fonction booléenne caractérisant tout filtre numérique récursif générant une suite de de Bruijn alors que* $\Pi_{r_B}$ *sera la matrice des probabilités de transition de la chaîne de Markov binaire dégénérée d'ordre r correspondante.*

Auparavant, nous avons constaté que:

$$\Pi_r \xleftrightarrow[\text{permutation des colonnes 0 et 1}]{} \Pi_{r_B}. \qquad (5.2)$$

Corollaire 5.2:

Toute fonction booléenne $g_B(b_{n-1}, ---, b_{n-r+1})$ est de la forme:

$$g_B(b_{n-1}, ---, b_{n-r+1}) = \hat{g}(b_{n-1}, ---, b_{n-r+1}) \oplus \prod_{1=1}^{r-1} (1 \oplus b_{n-1}).$$

Démonstration:

La condition (5.2) nous impose l'adjonction de l'impliquant $\prod_{l=1}^{r-1} (1 \oplus b_{n-l})$ à la fonction booléenne $\hat{g}(b_{n-1}, ---, b_{n-r+1})$ (car $g_B(0, ---, 0) = 1$). Or, dans le développement (4.16) de $\hat{g}(b_{n-1}, ---, b_{n-r+1})$, $a_0 = 0$ et au moins un des coefficients $a_{l_1 l_2 --- l_m}$, $1 \leq l_1 < l_2 < --- < l_m \leq r-1$, est non nul (théorème 5.4). Ainsi, $g_B(b_{n-1}, ---, b_{n-r+1})$ devient:

$$g_B(b_{n-1}, ---, b_{n-r+1}) = \hat{g}(b_{n-1}, ---, b_{n-r+1}) \oplus \prod_{l=1}^{r-1} (1 \oplus b_{n-l}).$$

CQFD.

Exemple 5.4:

a) Voyons d'abord le cas $r = 2$. Ici, $\hat{g}(b_{n-1}) = b_{n-1}$ est unique. Nous obtenons alors $g_B(b_{n-1}) = b_{n-1} \oplus (1 \oplus b_{n-1}) = 1$. Le filtre numérique récursif générant la suite de de Bruijn de période 4 est donc caractérisé par la fonction booléenne $f_B(b_{n-1}, b_{n-2}) = 1 \oplus b_{n-2}$.

b) Ensuite, concentrons-nous sur le cas $r = 3$. D'après le théorème 5.4, $\hat{g}_1(b_{n-1}, b_{n-2}) = b_{n-1}$ et $\hat{g}_2(b_{n-1}, b_{n-2}) = b_{n-2}$. En appliquant le corollaire 5.2, nous obtenons:

$$g_{B_1}(b_{n-1}, b_{n-2}) = 1 \oplus b_{n-2} \oplus b_{n-1} b_{n-2} \text{ et}$$

$$g_{B_2}(b_{n-1}, b_{n-2}) = 1 \oplus b_{n-1} \oplus b_{n-1} b_{n-2}.$$

Les deux filtres numériques récursifs générant les suites de de Bruijn de période 8 sont donc caractérisés respectivement par les fonctions booléennes:

$$f_{B_1}(b_{n-1}, b_{n-2}, b_{n-3}) = 1 \oplus b_{n-2} \oplus b_{n-3} \oplus b_{n-1} b_{n-2} \text{ et}$$

$$f_{B_2}(b_{n-1}, b_{n-2}, b_{n-3}) = 1 \oplus b_{n-1} \oplus b_{n-3} \oplus b_{n-1} b_{n-2}.$$

*Remarques:*

1) Dans le développement (4.16) de la fonction booléenne $f_B(b_{n-1}, ---, b_{n-r})$, les coefficients associés aux termes $b_{n-r}$ et $b_{n-1}b_{n-2}$ --- $b_{n-r+1}$ valent un. Cela implique que chaque cellule du registre à décalage composant le filtre numérique récursif correspondant (Fig. 5.1) devra être connectée (ce qui n'est pas le cas pour les filtres numériques linéaires générant toute suite PN).

2) Si nous avons affaire à une suite PN de période $2^r-1$, seuls 2r-1 éléments de celle-ci sont suffisants pour reconstruire la fonction booléenne linéaire $\hat{f}_L(b_{n-1}, --- b_{n-r})$ [25].

Pour une suite de de Bruijn de période $2^r$, il faut au plus $2^{r-1}-2$ éléments de celle-ci pour reconstituer la fonction booléenne $f_B(b_{n-1}, ---, b_{n-r})$. On peut facilement s'en convaincre en notant que la matrice des probabilités de transition qui lui est associée est doublement stochastique et que $\pi_{00} = 0$ et $\pi_{2^{r-1}-1 2^r-1} = 1$.

## V.3. Fonction d'autocorrélation.

Il nous semble plus facile de déterminer les caractéristiques statistiques d'une SPAB dont les éléments appartiennent à l'ensemble $E_\xi$ plutôt qu'à l'ensemble $E_\beta$. Remarquons que grâce à l'application L (définition 2.2), tout élément $b_n \in E_\beta$ se transforme de manière unique en un élément $x_n \in E_\xi$. Aussi, nous employerons ici les mêmes notations et définitions que celles déjà spécifiées.

Mentionnons un théorème, valable pour toute matrice cyclique [49] mais que nous adaptons au cas particulier qui nous intéresse, liant périodicité et valeurs propres de la matrice des probabilités de transition d'une chaîne de Markov binaire d'ordre r.

**Théorème 5.5:**

Si $\Pi_r$ est la matrice des probabilités de transition d'une chaîne de Markov binaire d'ordre r irréductible de période d, alors $\lambda_l = e^{i2\pi l/d}$, $0 \leq l \leq d-1$, sont d valeurs propres distinctes de $\Pi_r$.

### Suites de de Bruijn.

Toute matrice $\Pi_{r_B}$ est irréductible de période $2^r$. Ainsi, par le théorème 5.5, ses valeurs propres sont telles que:

$$\lambda_l = e^{i2\pi l/2^r} \quad , \; 0 \leq l \leq 2^r-1.$$

Donc, la fonction d'autocorrélation d'une suite de de Bruijn est donnée par (relation (4.10)):

$$R_{\xi\xi}(\nu) = m_\xi^2 + \sum_{l=1}^{2^r-1} c_l \lambda_l^\nu = m_\xi^2 + \sum_{l=1}^{2^r-1} c_l e^{i\pi l\nu/2^{r-1}}.$$

Mais, pour toute suite de de Bruijn, $m_\xi = 0$ (il y a autant de +1 que de -1). Notons aussi que $R_{\xi\xi}(\nu)$ est une fonction réelle. Ceci implique que les constantes $c_l$ et $c_{2^r-l}$, $0 \leq l \leq 2^{r-1}$, sont complexes conjuguées et $c_{2^{r-1}}$ est réelle. Après quelques calculs, nous obtenons:

$$R_{\xi\xi}(\nu) = c_{2^{r-1}}(-1)^\nu + \sum_{l=1}^{2^{r-1}-1} 2|c_l|\cos(\psi_l + \nu l\pi/2^{r-1}) \quad , \quad c_l = |c_l|e^{i\psi_l}.$$

Exemple 5.5:

Voyons la suite de de Bruijn de période 4. Alors:

$$\Pi_{2_B} = \{0\ 0\ 1\ 1\} \text{ et } R_{\xi\xi}(\nu) = \cos\nu\pi/2.$$

*Remarque:*

La probabilité de chacun des $2^r$ états de la chaîne de Markov binaire dégénérée d'ordre r correspondante vaut $2^{-r}$. Donc, par le corollaire 3.1, tous les moments conjoints de r "variables pseudo-aléatoires binaires" successives sont nuls. En particulier:

$$R_{\xi\xi}(0) = 1,$$
$$R_{\xi\xi}(1) = R_{\xi\xi}(2) = \text{---} = R_{\xi\xi}(r-1) = 0.$$

SPAB appartenant à l'ensemble S.

Ici, la matrice des probabilités de transition $\hat{\Pi}_r$ est réductible, car:

$$\hat{\Pi}_r = \text{diag}\{1 \quad \Pi_r^*\}.$$

Concentrons-nous sur la SPAB liée à la matrice $\Pi_r^*$. Cette dernière est irréductible de période $2^r-1$. Ainsi, par le théorème 5.5, ses valeurs propres sont telles que:

$$\lambda_l = e^{i2\pi l/(2^r-1)} \quad , \quad 0 \leq l \leq 2^r-2.$$

La fonction d'autocorrélation de la SPAB considérée se calcule comme suit (théorème 4.3):

$$\underline{m}_2(\nu) = R_{\xi\xi}(\nu) = v^T \cdot P_r(0) \cdot \hat{\Pi}_r^\nu \cdot v. \qquad (5.3)$$

La probabilité de chacun des $2^r-1$ états de la chaîne de Markov binaire dégénérée d'ordre correspondante vaut $\frac{1}{2^r-1}$. Donc, la matrice $P_r(0)$ devient:

$$P_r(0) = \text{diag } \{0 \ \frac{1}{2^r-1} \ \text{---} \ \frac{1}{2^r-1}\}. \qquad (5.4$$

En utilisant les relations (5.3) et (5.4), nous trouvons:

$$R_{\xi\xi}(\nu) = m_\xi^2 + \sum_{l=1}^{2^r-2} c_l \lambda_l^\nu = m_\xi^2 + \sum_{l=1}^{2^r-2} c_l \, e^{i2\pi l\nu/(2^r-1)}.$$

Mais:

$$m_\xi = P\{\xi(n) = +1\} - P\{\xi(n) = -1\} = \frac{2^{r-1}-1}{2^r-1} - \frac{2^{r-1}}{2^r-1} = -\frac{1}{2^r-1}.$$

En plus, $R_{\xi\xi}(\nu)$ est une fonction réelle. Ceci implique que les constantes $c_l$ et $c_{2^r-1-l}$ sont complexes conjugées. Après quelques calculs, nous obtenons:

$$R_{\xi\xi}(\nu) = (\frac{1}{2^r-1})^2 + \sum_{l=1}^{2^{r-1}-1} 2|c_l|\cos(\psi_l + \frac{\nu 2l\pi}{2^r-1}) \ , \ c_l = |c_l|e^{i\psi_l}.$$

Exemple 5.6:

Voyons la SPAB de période 3. Alors:

$$\hat{\Pi}_2 = \{1\ 0\ 1\ 0\} \text{ et } \Pi_2^* = \{0\ 1\ 0\}.$$

Ignorons la suite binaire n'étant formée que de +1 (elle correspond à $\pi_{00} = 1$). La fonction d'autocorrélation cherchée vaut:

$$R_{\xi\xi}(\nu) = \frac{1}{9} + \frac{8}{9}\cos 2\pi\nu/3.$$

*Remarque:*

Le vecteur des probabilités des états de la chaîne de Markov binaire dégénérée d'ordre r avec matrice des probabilités de transition $\hat{\Pi}_r$ est du type:

$$\hat{p}_r = [\ 0 \ \frac{1}{2^r-1} \ \text{---} \ \frac{1}{2^r-1}].$$

Par le théorème 3.1, nous trouvons que tous les moments conjoints de r "variables pseudo-aléatoires binaires" successives valent $\frac{1}{2^r-1}$. En particulier:

$$R_{\xi\xi}(0) = 1,$$
$$R_{\xi\xi}(1) = R_{\xi\xi}(2) = \text{---} = R_{\xi\xi}(r-1) = -\frac{1}{2^r-1}.$$

Finalement, notons que pour toute suite PN [23]:

$$R_{\xi\xi}(\nu) = \begin{cases} 1 & \nu = k\,2^r,\ k \text{ entier} \\ -\frac{1}{2^r-1} & \nu \neq k\,2^r. \end{cases}$$

## VI. CONCLUSIONS.

Dans cette étude sur les suites aléatoires binaires, nous avons développé de nouveaux outils qui, nous semble-t-il, pourraient être appliqués dans de nombreux cas pratiques.

En particulier, le théorème reliant probabilités conjointes et moments conjoints par une transformation de Walsh ainsi que celui relatif à l'indépendance de variables aléatoires binaires devraient permettre de résoudre un certain nombre de problèmes, notamment dans le domaine de la cryptographie, domaine qui est en pleine expansion actuellement.

Il est intéressant de constater que si toute composante du vecteur des moments conjoints de m variables aléatoires binaires s'exprime comme le produit de moments du premier ordre (elles ont été définies par le terme: m-non corrélées), ces dernières sont indépendantes. Ce fait est important et n'a d'équivalent, à notre connaissance, que dans le cadre des variables aléatoires gaussiennes.

Les chaînes de Markov binaires forment une sous-classe importante des suites aléatoires binaires. Nous avons examiné leurs moments conjoints et plus particulièrement leur fonction d'autocorrélation. Pour une chaîne de Markov binaire avec matrice des probabilités de transition diagonalisable, nous avons montré que sa fonction d'autocorrélation est donnée par une combinaison linéaire des valeurs propres de ladite matrice.

Nous nous sommes aussi intéressés au produit de deux chaînes de Markov binaires indépendantes. Nous avons décrit un algorithme (facilement exécuté par un ordinateur) nous permettant de déterminer si le résultat d'un tel produit est une chaîne de Markov binaire (ce qui n'est, en général, pas le cas).

En particulier, si les deux chaînes de Markov binaires indépendantes en question sont du même ordre, disons r, et, en plus, les éléments non nuls de leurs matrices des probabilités de transition respectives ne prennent qu'une parmi deux valeurs de somme un, alors la suite aléatoire binaire, produit de ces deux chaînes, peut aussi être une chaîne de Markov binaire d'ordre r (avec matrice des probabilités de transition possèdant la propriété décrite ci-dessus).

Toute chaîne de Markov ayant cette caractéristique peut être générée par un filtre numérique récursif (par filtre numérique récursif, on entend ici un filtre séquentiel binaire traitant des variables binaires) couplé à une source binaire sans mémoire.

Dans ce contexte, il faut noter que la multiplication de deux chaînes de Markov binaires indépendantes d'ordre r est aussi une chaîne de Markov binaire d'ordre r si et seulement si toutes trois peuvent être générées à partir d'un même filtre numérique récursif linéaire. Remarquons que cette condition est très restrictive.

En guise d'application, nous nous sommes penchés sur l'étude des suites pseudo-aléatoires binaires comme cas limite de chaînes de Markov binaires (ces dernières étant produites par des filtres numériques récursifs). Cette approche nous semble nouvelle puisqu'il n'en est pas fait mention dans la littérature consultée. Par cette technique, nous avons été en mesure de définir quelques propriétés encore inconnues concernant la classe des filtres numériques récursifs générant toute suite dite de de Bruijn.

Nous espérons que ce travail représentera une ouverture pour des travaux ultérieurs. Le domaine traité est vaste et il reste encore passablement de problèmes à résoudre. Mentionnons, par exemple:

- L'étude approfondie du produit de deux chaînes de Markov binaires indépendantes d'ordre quelconque.

- Le traitement de suites aléatoires binaires par des filtres numériques récursifs ou non récursifs.

- Description générale des filtres numériques récursifs produisant toute suite de de Bruijn.

REMERCIEMENTS.

Je tiens a remercier Mr. le Professeur A. Shah, directeur de cette thèse, pour m'avoir permis d'effectuer ce travail et pour les nombreuses discussions qu'il m'a accordées.

Je remercie également Mrs. les Professeurs J. L. Massey, H. Mey et U. Suter pour les suggestions particulièrement intéressantes qu'ils m'ont faites et pour l'intérêt qu'ils ont porté à ce travail.

Ce travail a été financé par le Fonds National Suisse pour la Recherche Scientifique dans le cadre du projet No. 2.762-0.82.

APPENDICE A. SOLUTIONS DE L'EQUATION FONCTIONNELLE:

$$f(x_1y_1, x_2y_2, ---, x_ny_n) = f(x_1, x_2, ---, x_n)\cdot f(y_1, y_2, ---, y_n).$$

La solution de l'équation fonctionnelle proposée nous été fournie par Mr. le Professeur Suter.

On part du lemme [2]:

Soit $f: R \longrightarrow R$ une fonction continue satisfaisant l'équation fonctionnelle:

$$f(xy) = f(x)\cdot f(y).$$

Alors, la fonction f est du type:

$$\left.\begin{array}{l} f(x) = |x|^c,\ c \geq 0, \\ f(x) = |x|^c \cdot \text{signe}(x),\ c > 0\ (\text{signe}(0) = 0), \\ f(x) = 0, \\ \text{où c est une constante réelle.} \end{array}\right\} \quad (A.1)$$

*Remarque:*

Il est possible de supprimer les conditions sur la constante c si l'on n'admet que des valeurs de x différentes de zéro.

Soit $f(x_1, x_2, ---, x_n)$ une fonction réelle continue, définie pour tout $x_1, x_2, ---, x_n \in R$ et satisfaisant l'équation fonctionnelle:

$$f(x_1y_1, x_2y_2, ---, x_ny_n) = f(x_1, x_2, ---, x_n)\cdot f(y_1, y_2, ---, y_n).$$

On a:

$$f(x_1, x_2, ---, x_n) = \prod_{1=1}^{n} f(1, ---, 1, x_1, 1, ---, 1).$$

Posons:

$$f_l(x) = f(1, \text{---}, 1, \underset{\uparrow}{x}, 1, \text{---}, 1) \quad , \quad l = 1, 2, \text{---}, n.$$
$$l$$

Les fonctions $f_1, f_2, \text{---}, f_n$ satisfont aux conditions:

1) $f_l(xy) = f_l(x) \cdot f_l(y) \quad , \quad l = 1, 2, \text{---}, n,$

2) $f(x_1, x_2, \text{---}, x_n) = \prod_{l=1}^{n} f_l(x_l),$

3) f continue $\Longleftrightarrow$ $f_1, f_2, \text{---}, f_n$ continues.

La fonction f est donc produit de fonctions du type (A.1).

## APPENDICE B. APPLICATION DE L'ALGORITHME DEVELOPPE AU CHAPITRE IV.

Examinons la situation suivante:

- $B_1 = \{\beta_1(n)\}$, $\beta_1(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\beta$, une suite de Bernoulli avec: $P\{\beta_1(n) = 0\} = p$.

- $B_2 = \{\beta_2(n)\}$, $\beta_2(n)$ variable aléatoire binaire à valeurs dans l'ensemble $E_\beta$, une chaîne de Markov binaire du premier ordre avec matrice des probabilités de transition $\Pi_2 = \{\pi\ 1\text{-}\pi\}$.

- Formons la suite aléatoire biniare $H = \{n(n)\} = B_1 \oplus B_2$, $B_1$ et $B_2$ indépendantes.

Est-ce-que $H$ est aussi une chaîne de Markov binaire ? Pour répondre à cette question, utilisons l'algorithme développé au chapitre IV.

Il est facile de construire les deux vecteurs des probabilités conjointes $P_4(B_1)$ et $P_4(B_2)$ associés respectivement à $B_1$ et $B_2$.

$$P_4(B_1) = \begin{bmatrix} p^4 \\ p^3(1-p) \\ p^3(1-p) \\ p^2(1-p)^2 \\ p^3(1-p) \\ p^2(1-p)^2 \\ p^2(1-p)^2 \\ p(1-p)^3 \\ p^3(1-p) \\ p^2(1-p)^2 \\ p^2(1-p)^2 \\ p(1-p)^3 \\ p^2(1-p)^2 \\ p(1-p)^3 \\ p(1-p)^3 \\ (1-p)^4 \end{bmatrix} \quad \text{et} \quad P_4(B_2) = 0.5 \begin{bmatrix} \pi^3 \\ \pi^2(1-\pi) \\ \pi(1-\pi)^2 \\ \pi^2(1-\pi) \\ \pi(1-\pi)^2 \\ (1-\pi)^3 \\ \pi(1-\pi)^2 \\ \pi^2(1-\pi) \\ \pi^2(1-\pi) \\ \pi(1-\pi)^2 \\ (1-\pi)^3 \\ \pi(1-\pi)^2 \\ \pi^2(1-\pi) \\ \pi(1-\pi)^2 \\ \pi^2(1-\pi) \\ \pi^3 \end{bmatrix}.$$

Remarquons que le vecteur $P_4(B_2)$ est symétrique.

En utilisant le théorème 3.4, nous trouvons que le vecteur des probabilités conjointes $P_4(H)$ associé à $H$ (qui est aussi symétrique en vertu du corollaire 3.5) est du type:

$$P_4(H) = \frac{1}{16}\begin{bmatrix}
1 + 3\lambda m^2 + 2\lambda^2 m^2 + \lambda^3 m^2 + \lambda^2 m^4 \\
1 + \lambda m^2 - \lambda^3 m^2 - \lambda^2 m^4 \\
1 - \lambda m^2 + \lambda^3 m^2 - \lambda^2 m^4 \\
1 + \lambda m^2 - 2\lambda^2 m^2 - \lambda^3 m^2 + \lambda^2 m^4 \\
1 - \lambda m^2 + \lambda^3 m^2 - \lambda^2 m^4 \\
1 - 3\lambda m^2 + 2\lambda^2 m^2 - \lambda^3 m^2 + \lambda^2 m^4 \\
1 - \lambda m^2 - 2\lambda^2 m^2 + \lambda^3 m^2 + \lambda^2 m^4 \\
1 + \lambda m^2 - \lambda^3 m^2 - \lambda^2 m^4 \\
1 + \lambda m^2 - \lambda^3 m^2 - \lambda^2 m^4 \\
1 - \lambda m^2 - 2\lambda^2 m^2 + \lambda^3 m^2 + \lambda^2 m^4 \\
1 - 3\lambda m^2 + 2\lambda^2 m^2 - \lambda^3 m^2 + \lambda^2 m^4 \\
1 - \lambda m^2 + \lambda^3 m^2 - \lambda^2 m^4 \\
1 + \lambda m^2 - 2\lambda^2 m^2 + \lambda^3 m^2 + \lambda^2 m^4 \\
1 - \lambda m^2 + \lambda^3 m^2 - \lambda^2 m^4 \\
1 + \lambda m^2 - \lambda^3 m^2 - \lambda^2 m^4 \\
1 + 3\lambda m^2 + 2\lambda^2 m^2 + \lambda^3 m^2 + \lambda^2 m^4
\end{bmatrix}$$

où: $\lambda = 2\pi - 1$ et $m = 2p - 1$.

On en déduit, après quelques calculs, le vecteur $V_4(H)$:

$$V_4 = [\pi_0\ \pi_1\ \pi_2\ \pi_3\ \pi_4\ \pi_5\ \pi_6\ \pi_7]^T$$

avec:

$$\pi_0 = \frac{1 + 3\lambda m^2 + 2\lambda^2 m^2 + \lambda^3 m^2 + \lambda^2 m^4}{2 + 4\lambda m^2 + 2\lambda^2 m^2},$$

$$\pi_1 = \frac{1 - \lambda m^2 + \lambda^3 m^2 - \lambda^2 m^4}{2 - 2\lambda^2 m^2},$$

$$\pi_2 = \frac{1 - \lambda m^2 + \lambda^3 m^2 - \lambda^2 m^4}{2 - 4\lambda m^2 + 2\lambda^2 m^2},$$

$$\pi_3 = \frac{1 - \lambda m^2 - 2\lambda^2 m^2 + \lambda^3 m^2 + \lambda^2 m^4}{2 - 2\lambda^2 m^2},$$

$$\pi_4 = \frac{1 + \lambda m^2 - \lambda^3 m^2 - \lambda^2 m^4}{2 - 2\lambda^2 m^2},$$

$$\pi_5 = \frac{1 - 3\lambda m^2 + 2\lambda^2 m^2 - \lambda^3 m^2 + \lambda^2 m^4}{2 - 4\lambda m^2 - 2\lambda^2 m^2},$$

$$\pi_6 = \frac{1 + \lambda m^2 - 2\lambda^2 m^2 - \lambda^3 m^2 + \lambda^2 m^4}{2 - 2\lambda^2 m^2},$$

$$\pi_7 = \frac{1 - \lambda^3 m^2 - \lambda^2 m^4}{2 + 4\lambda m^2 + 2\lambda^2 m^2}.$$

On constate donc, qu'en général, la suite aléatoire binaire $H$ n'est pas une chaîne de Markov binaire, car:

$$\pi_0 \neq \pi_4,$$

$$\pi_1 \neq \pi_5,$$

$$\pi_2 \neq \pi_6,$$

$$\pi_3 \neq \pi_7.$$

BIBLIOGRAPHIE.

1. M. Abramowitz, I. Stegun (éditeurs): *"Handbook of Mathematical Functions"* National Bureau of Standards (1972).

2. J. Aczél: *"Lectures on Functional Equations and Their Applications"*, Academic Press, New York (1966).

3. A. R. Agul'nik, S. S. Musaelyan: *"Construction of Nonlinear Binary Sequences"*, I. VUZ. Radioelektronika, Vol. 26, No. 4, pp. 19-27 (1983).

4. B. D. O. Anderson, J. B. Moore: *"Optimal Filtering"*, Prentice-Hall, Englewood-Cliffs (1979).

5. R. Bellman: *"Introduction to Matrix Analysis"*, McGraw-Hill, New York (19

6. J. S. Bendat: *"Principles and Applications of Random Noise Theory"*, R. E. Krieger Publishing Co., Huntington (1977).

7. T. L. Booth: *"Sequential Machines and Automata Theory"*, Wiley, New york (1967).

8. J. W. Brewer: *"Kronecker Products and Matrix Calculus in System Theory"*, IEEE Trans. Circuits and Systems, Vol. CAS-25, No. 9, pp. 772-781 (1978)

9. W. C. Carter: *"Using a Shift Register to Generate Verification Tests"*, IBM Tech. Disclosure Bull., Vol. 26, No. 12, pp. 6510-6513 (1984).

10. G. Chaitin: *"Les suites aléatoires et les démonstrations mathématiques"*, Les progrès des mathématiques, Bibliothèque pour la science, Diffusion Belin, pp. 68-73.

11. C. E. Cook, F. W. Ellersick, L. B. Milstein, D. L. Schilling: *"Spread-Spectrum Communications"*, IEEE Press, New york (1983).

12. D. R. Cox: *"The Analysis of Binary Data"*, Chapman and Hall, London (1977).

13. W. Daehn, J. Mucha: *"Hardware Test Pattern Generation for Built-In Testing"*, 1981 IEEE Test Conference, Philadelphia, USA, pp. 110-113 (October 27-29, 1981).

14. W. Daehn, J. Mucha: *"A Hardware Approach to Self-Testing of Large Programmable Logic Arrays"*, IEEE Trans. Comput., Vol. C-30, No. 11, pp. 829-833 (1981).

15. W. Diffie, M. E. Hellman: *"Privacy and Authentification: An Introduction to Cryptography"*, Proc. IEEE, Vol. 67, No. 3, pp. 397-427 (1979).

16. G. Duella, H. S. Jamadagni, K. H. S. Rao, A. V. Shah: *"Comparative Performance and Theoritical Analysis for a Generalized DPSK Demodulator"*, 1982 IEEE International Symposium on Information Theory, Les Arcs, France (June 21-25, 1982).

17. T. Etzion, A. Lempel: *"Algorithms for the Generation of Full-Length Shift-Register"*, IEEE Trans. Inform. Theory, Vol. IT-30, No. 3, pp. 480-484 (1984).

18. W. Feller: *"An Introduction to Probability Theory and Its Applications, Volume I"*, Wiley, New York (1968).

19. P. Fire: *"Boolean Opérations on Binary Markov Chains"*, Sylvania Electronic Products, Mountain View, CA, Rept. EDL-L27 (1964).

20. H. Fredricksen: *"A Survey of Full Length Nonlinear Shift Register Cycle Algorithms"*, SIAM Rev., Vol. 24, No. 2, pp. 195-221 (1982).

21. R. A. Games: *"A Generalized Recusive Contruction for de Bruijn Sequences"*, IEEE Trans. Inform. Theory, Vol. IT-29, No. 6, pp. 843-850 (1983).

22. W. A. Gardner: *Representation and Estimation of Cyclostationary Processes"*, University of California, Davis, CA, Rept. SIPL-82-1 (1982).

23. S. W. Golomb: *"Shift Register Sequences"*, Holden-Day, San Francisco (196

24. S. W. Golomb: *"On the Classification of Balanced Binary Sequences of Period $2^n-1$"*, IEEE Trans. Inform. Theory, Vol. IT-26, No. 6, pp. 730-732 (1980).

25. E. J. Groth: *"Generation of Sequences with Controllable Complexity"*, IEE Trans. Inform. Theory, Vol. IT-17, No. 3, pp. 288-296 (1971).

26. V. S. Gutin: *"Correlation Properties of Random Binary Sequences"*, Radio Eng. and Electron. Phys., Vol. 18, No. 2, pp. 296-298 (1973).

27. H. F. Harmuth: *"Transmission of Information by Orthogonal Functions"*, Springer-Verlag, Berlin (1972).

28. K. Hoffman, R. Kunze: *"Linear Algebra"*, Prentice-Hall, Englewood-Cliffs (1971).

29. D. L. Isaacson, R. W. Madsen: *"Markov Chains Theory and Applications"*, Wiley, New York (1976).

30. J. Justesen, T. Høholdt: *"Maxentropic Markov Chains"*, IEEE Trans. Inform Theory, Vol. IT-30, No. 4, pp. 665-667 (1984).

31. T. Kailath: *"Linear Systems"*, Prentice-Hall, Englewood-Cliffs (1980).

32. S. C. Kak: *"Classification of Random Binary Sequences Using Walsh-Fourie Transform"*, IEEE Trans. Electromagn. Compat., Vol. EMC-13, No. 3, pp. 74-77 (1971).

33. S. Karlin, H. M. Taylor: *"A First Course in Stochastic Processes"*, Academic Press, New York (1975).

34. M. G. Karpovsky: *"Finite Orthogonal Series in the Design of Digital Devices"*, Wiley, New York (1976).

35. E. L. Key: *"An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators"*, IEEE Trans. Inform. Theory, Vol. IT-22, No. 6, pp. 732-736 (1976).

36. H. Kunz: *"Approximation optimaler linearer Transformationen durch eine Klasse schneller, verallgemeinerter Fourier-Tranformationen"*, Diss. ETH 5832, Zürich (1977).

37. D. H. Lee: *"On the Source Matching Approach for Markov Sources"*, IEEE Trans. Inform. Theory, Vol. IT-29, No. 5, pp. 754-755 (1983).

38. J. L. Martins de Carvalho, J. M. C. Clark: *"Characterizing the Autocorrelations of Binary Sequences"*, IEEE Trans. Inform. Theory, Vol. IT-29, No. 4, pp. 502-508 (1983).

39. E. Masry: *"On Covariance Functions of Unit Processes"*, SIAM J. Appl. Math., Vol. 23, No. 1, pp. 28-33 (1972).

40. J. L. Massey: *"Feedback Shift Register Synthesis and BCH Decoding"*, IEEE Trans. Inform. Theory, Vol. IT-15, No. 1, pp. 122-127 (1969).

41. J. L. Massey: *" Handbook of Applicable Mathematics, Volume 5, Chapter 16"*, Wiley, New York (1985).

42. J. L. Massey, A. Gubser, A. Fischer, P. Hochstrasser, B. Huber, R. Sutter: *"A Self-Synchronizing Digital Scrambler for Cryptographic Protection of Data"*, 1984 International Zurich Seminar on Digital Communications, Proc., Zurich, Switzerland, pp. 163-169 (March 6-8, 1984).

43. M. Métivier: *"Notions fondamentales de la théorie des probabilités"*, Dunod Université, Paris (1979).

44. H. Mey: *"Linear-algebraische Behandlung digitaler Signale und Systeme"*, Diss. ETH 4341, Zürich (1969).

45. G. N. de Oliveira: *"Sobre Matrizes Estocásticas e Duplamente Estocásticas"*, Rev. Fac. Ci. Univ. Coimbra, Vol. 41, pp. 15-221 (1968).

46. A. Papoulis: *"Probability, Random Variables and Stochastic Processes"*, McGraw-Hill, New York (1965).

47. J. Pearl: *"Application of Walsh Transform to Statistical Analysis"*, 4th Conf. on System Science, Hawaii, USA, pp. 406-407 (1971).

48. H. F. A. Roefs, M. B. Pursley: *"Correlation Parameters of Random Binary Sequences"*, Electronics Letters, Vol. 13, No. 16, pp. 488-489 (197

49. E. Seneta: *"Non-Negative Matrices"*, George Allen and Unwin, London (1973)

50. A. V. Shah: *"A Contribution to the Theory of Random Binary Sequences"*, 1982 IEEE International Symposium on Information Theory, Les Arcs, France (June 21-25, 1982).

51. A. V. Shah: *"Ein Beitrag zur Darstellung und Theorie binärer Zufallsfolgen"*, AGEN-Mitteilungen, pp. 3-25 (Dezember 1982).

52. A. V. Shah, M. Saglini, C. Weber: *"Integrierte Schaltungen in digitalen Systemen"*, Birkhäuser Verlag, Basel (1977).

53. T. Siegenthaler: *"Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications"*, IEEE Trans. Inform. Theory, Vol. IT-30, No. 5, pp. 776-780 (1984).

54. T. Siegenthaler: *"Decrypting a Class of Stream Ciphers Using Ciphertext Only"*, IEEE Trans. Comput., Vol. C-34, No. 1, pp. 81-85 (1985).

55. S. N. Stepanov: *"Calculation of the Correlation Function of a Markov Process with Continuous Time and a Finite Number of States"*, Engrg. Cybernetics, Vol. 17, No. 2, pp. 91-98 (1980).

56. G. Strang: *"Linear Algebra and Its Applications"*, Academic Press, New York (1980).

57. H. Ventsel: *"Théorie des probabilités"*, Editions MIR, Moscou (1973).

58. H. Weinrichter: *"Beschreibung der Verwürfelung stochastisch unabhänginger Binärfolgen in rückgekoppelten Schieberegistern mit Hilfe der Walsh-Transformation"*, Frequenz, Vol. 33, pp. 207-210 (1979).

59. J. M. Wozencraft, I. M. Jacobs: *"Principles of Communication Engineering"*, Wiley, New York (1965).

60. G.-Z. Xiao, J. L. Massey: *"A Spectral Characterization of Correlation-Immune Combining Functions"*, Soumis à l'IEEE Trans. Inform. Theory.