Ecole Polytechnique 2006 - Math PC

Titre : *Polynômes à coefficients* 1 *ou* -1, *paires de Rudin-Shapiro.*

Une séquence $\underline{a}$ de longueur ℓ, $\ell \geqslant 1$, est un vecteur $(a_0, a_1, \ldots, a_{\ell-1})$ de $\mathbb{R}^\ell$ où chacune de ses ℓ coordonnées vaut 1 ou -1.

Deux séquences $\underline{a}$ et $\underline{b}$, de même longueur, forment une paire complémentaire si $\ell = 1$ ou si $\ell > 1$ avec pour tout entier j, $1 \leqslant j \leqslant \ell - 1$, la j-ième condition de corrélation

$$\sum_{i=0}^{\ell-1-j} (a_i a_{i+j} + b_i b_{i+j}) = 0.$$

On note $\mathcal{L}$ l'ensemble des longueurs des paires complémentaires.

Première partie : propriétés de $\mathcal{L}$

1. Pour $\ell = 2$, la condition de corrélation C_1 est $a_0 a_1 + b_0 b_1 = 0$. Donc $\underline{a} = (1, 1)$ et $\underline{b} = (1, -1)$ forment une paire complémentaire et $2 \in \mathcal{L}$.

Pour $\ell = 3$, les conditions de corrélation C_1 et C_2 sont respectivement

$$(a_0 + a_2)a_1 + (b_0 + b_2)b_1 = 0 \quad \text{et} \quad a_0 a_2 + b_0 b_2 = 0.$$

Si $b_0 = b_2$, C_2 donne $a_0 = -a_2$ ainsi $(a_0 + a_2)a_1 + (b_0 + b_2)b_1 = 2b_0 b_1 \neq 0$.
Si $b_0 = -b_2$, C_2 donne $a_0 = a_2$ ainsi $(a_0 + a_2)a_1 + (b_0 + b_2)b_1 = 2a_0 a_1 \neq 0$.
Il en résulte que $3 \notin \mathcal{L}$.

2.a) Pour $\underline{a} = (a_0, a_1, \ldots, a_{\ell-1})$, de longueur $\ell \geqslant 1$, on pose $P_{\underline{a}}(X) = \sum_{i=0}^{\ell-1} a_i X^i$.

On a $P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) \sim a_0 a_{\ell-1} x^{\ell-1}$ lorsque x tend vers $+\infty$.
Si $\underline{a}$ et $\underline{b}$ sont deux séquences de longueur différentes, la plus longue ayant une longueur $\ell > 1$, on obtient $\lim_{x\to+\infty} |P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) + P_{\underline{b}}(x)P_{\underline{b}}(x^{-1})| = +\infty$.
La fonction $x \mapsto P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) + P_{\underline{b}}(x)P_{\underline{b}}(x^{-1})$ n'est donc pas bornée sur $]0, +\infty[$.

En introduisant $k = |i - j|$, on obtient les calculs suivants

$$\begin{aligned} P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) &= \sum_{0\leqslant i,j\leqslant \ell-1} a_i a_j x^{i-j} \\ &= \sum_{i=0}^{\ell-1} a_i^2 + \sum_{k=1}^{\ell-1} \left(\sum_{i=1}^{\ell-1-k} a_i a_{i+j} \right) x^k + \sum_{k=1}^{\ell-1} \left(\sum_{i=1}^{\ell-1-k} a_i a_{i+j} \right) x^{-k} \end{aligned}$$

Ainsi pour deux séquences $\underline{a}$ et $\underline{b}$ de même longueur ℓ, on obtient

$$P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) + P_{\underline{b}}(x)P_{\underline{b}}(x^{-1}) = \sum_{i=0}^{\ell-1}(a_i^2 + b_i^2) + \sum_{k=1}^{\ell-1} \left(\sum_{i=1}^{\ell-1-k} a_i a_{i+j} + b_i b_{i+j} \right) (x^k + x^{-k}).$$

Si $\underline{a}$ et $\underline{b}$ forment une paire complémentaire alors, pour tout $x \neq 0$,

$$P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) + P_{\underline{b}}(x)P_{\underline{b}}(x^{-1}) = \sum_{i=0}^{\ell-1}(a_i^2 + b_i^2) = 2\ell.$$

Ainsi la fonction $x \mapsto P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) + P_{\underline{b}}(x)P_{\underline{b}}(x^{-1})$ est constante sur $\mathbb{R}\backslash\{0\}$.

Inversement supposons la fonction constante sur $\mathbb{R}\backslash\{0\}$.

Posons $y = x + x^{-1}$, alors y décrit l'ensemble infini $D =]-\infty, -2] \bigcup [2, +\infty[$.
On montre aisément par récurrence sur k, $k \geqslant 1$, que $x^k + x^{-k}$ est un polynôme F_k en y de degré k car $F_1(X) = X$, $F_2(X) = X^2 - 1$ et pour tout $k \geqslant 2$ $F_{k+1} + F_{k-1} = F_k.F_1$.
Ainsi

$$P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) + P_{\underline{b}}(x)P_{\underline{b}}(x^{-1}) = \sum_{i=0}^{\ell-1}(a_i^2 + b_i^2) + \sum_{k=0}^{\ell-1} \alpha_m y^m.$$

On obtient une fonction polynomiale constante sur D, donc $\alpha_m = 0$ pour m, $1 \leqslant m \leqslant \ell - 1$.
Chaque α_m est une combinaison des $\displaystyle\sum_{i=1}^{\ell-1-k} a_i a_{i+j} + b_i b_{i+j}$ pour k variant de m à $\ell - 1$.
En écrivant successivement que $\alpha_m = 0$ pour m variant de $\ell - 1$ à 1, on établit que $\displaystyle\sum_{i=1}^{\ell-1-k} a_i a_{i+j} + b_i b_{i+j} = 0$ pour k variant de $\ell - 1$ à 1, ainsi la paire $\underline{a}$, $\underline{b}$ est complémentaire.

2.b) Si $\underline{a}$ est de longueur ℓ, alors $P_{\underline{a}}(1) = \ell - 2k$ où k est le nombre de coefficients égaux à -1, donc $P_{\underline{a}}(1)$ a même parité que ℓ.
Il en résulte que si $\underline{a}$ et $\underline{b}$ sont de même longueur, alors $P_{\underline{a}}(1)$ et $P_{\underline{b}}(1)$ sont des entiers de même parité.
Soient $\ell \in \mathcal{L}$ et $\underline{a}$, $\underline{b}$ une paire complémentaire de longueur ℓ.
On note $I = \{i \,/\, a_i = b_i\}$, $J = \{i \,/\, a_i = -b_i\}$, $\alpha = \displaystyle\sum_{i \in I} a_i$ et $\beta = \displaystyle\sum_{i \in J} a_i$.
On a $P_{\underline{a}}(1) = \alpha + \beta$ et $P_{\underline{b}}(1) = \alpha - \beta$ donc $P_{\underline{a}}(1)^2 + P_{\underline{b}}(1)^2 = 2\alpha^2 + 2\beta^2 = 2\ell$.
Ainsi tout élément de $\mathcal{L}$ peut s'écrire comme la somme de deux carrés d'entiers.
Nota : on retrouve $3 \notin \mathcal{L}$.

2.c) Si $m = 2k$ alors $m^2 \equiv 0(4)$ et si $m = 2k + 1$ alors alors $m^2 \equiv 1(4)$, ainsi pour tout $\ell \in \mathcal{L}$, on a $\ell \equiv 0 + 0(4)$ ou $\equiv 0 + 1(4)$ ou $\equiv 1 + 0(4)$ ou $\equiv 1 + 1(4)$.
L'ensemble infini des entier congrus à 3 modulo 4 ne contient donc aucun élément de $\mathcal{L}$.
Ainsi le complémentaire de $\mathcal{L}$ dans $\mathbb{N}$ est un ensemble infini.

3.a) Soient $\underline{a}$ et $\underline{b}$ deux séquences de même longueur et $U = \frac{1}{2}(P_{\underline{a}} + P_{\underline{b}})$ et $V = \frac{1}{2}(P_{\underline{a}} - P_{\underline{b}})$.
Le calcul donne $U(x)U(x^{-1}) + V(x)V(x^{-1}) = \dfrac{1}{2}\Big(P_{\underline{a}}(x)P_{\underline{a}}(x^{-1}) + P_{\underline{b}}(x)P_{\underline{b}}(x^{-1})\Big)$.
Il résulte de **2.a)** que $\underline{a}$ et $\underline{b}$ forment une paire complémentaire si et seulement si la fonction $x \mapsto U(x)U(x^{-1}) + V(x)V(x^{-1})$ est constante sur $\mathbb{R}\backslash\{0\}$.

3.b) Pour les séquences $\underline{a} = (1, 1, -1, 1, -1, 1, -1, -1, 1, 1)$ et $\underline{b} = (1, 1, -1, 1, 1, 1, 1, 1, -1, -1)$ de longueur 10, on a

$$\begin{cases} U(x) = 1 + x - x^2 + x^3 + x^5 \\ V(x) = -x^4 - x^6 - x^7 + x^8 + x^9 = -x^4(1 + x^2 + x^3 - x^4 - x^5) \end{cases}$$

Le calcul donne

$$\begin{aligned} U(x)U(x^{-1}) + V(x)V(x^{-1}) &= (1 + x - x^2 + x^3 + x^5)(1 + \frac{1}{x} - \frac{1}{x^2} + \frac{1}{x^3} + \frac{1}{x^5}) \\ &\quad + (1 + x^2 + x^3 - x^4 - x^5)(1 + \frac{1}{x^2} + \frac{1}{x^3} - \frac{1}{x^4} - \frac{1}{x^5}) \\ &= 10. \end{aligned}$$

Ainsi $\underline{a}$ et $\underline{b}$ forment une paire complémentaire et $10 \in \mathcal{L}$.

4. Soit $\underline{v}$ une séquence de longueur paire $2m > 0$ et n le nombre de coordonnées de $\underline{v}$ égales à -1.

On a $\sum_{i=0}^{2m_1} v_i = 2m - 2n$, donc l'assertion (i) "4 divise la somme $\sum_{i=0}^{2m_1} v_i$" équivant à $m-n$ pair, c'est-à-dire l'assertion (ii) "n a la même parité que m".

On a $\prod_{i=0}^{2m_1} v_i = (-1)^n$ donc l'assertion (ii) équivant à l'assertion (iii) "$\prod_{i=0}^{2m_1} v_i = (-1)^m$".

5. Soient $\underline{a}$ et $\underline{b}$ deux séquences formant une paire complémentaire de longueur $\ell \geqslant 2$. Pour tout entier i, $1 \leqslant i \leqslant \ell - 1$, on pose $x_i = a_i b_i$.

5.a) Soit j un entier tel que $1 \leqslant j \leqslant \ell - 1$. La somme des coordonnées de la séquence $(a_0a_j, \ldots, a_{\ell-1-j}a_{\ell-1}, b_0b_j, \ldots, b_{\ell-1-j}b_{\ell-1})$ de longueur paire $2(\ell - j)$ est nulle d'après la j-ième condition de corrélation.

Elle est donc divisible par 4 et il resulte de l'assertion (iii) de **4.** que

$$\prod_{k=0}^{\ell-1-j} x_k x_{k+j} = (-1)^{\ell-j}$$

5.b) Sachant que $x_k^2 = 1$, d'après **5.a)** pour $j = 1$, on obtient $x_0 x_{\ell-1} = (-1)^{\ell-1}$.

Pour $j = \ell - 1$, on obtient $x_0 x_{\ell-1} = -1$. Il en résulte que ℓ est paire.

On pose $\ell = 2p$ avec $p \geqslant 1$.

On a successivement :

pour $j = \ell - 1$: $x_0 x_{\ell-1} = -1$;

pour $j = \ell - 2$: $x_0 x_{\ell-2} x_1 x_{\ell-1} = (-1)^2$;

pour $j = \ell - (k+1)$: $x_0 x_{\ell-1-k} x_1 x_{\ell-k} \ldots x_k x_{\ell-1} = (-1)^{k+1}$.

La première égalité et le quotient de deux égalités consécutives donnent $x_k x_{\ell-1-k} = -1$ pour k variant de 0 à $p-1$.

On a $x_j x_{\ell-1-j} = x_k x_{\ell-1-k}$ pour $j = k$ et $j = \ell - 1 - k$.

Pour k variant de 0 à $p - 1$, on a $\ell - 1 - k$ variant de $\ell - 1$ à p ainsi

$$\forall j,\ 0 \leqslant j \leqslant \ell - 1, \quad x_j x_{\ell-1-j} = -1.$$

5.c) On a établi en **5.b)**, que tout élément ℓ de $\mathcal{L}$, $\ell \geqslant 2$ est pair.

Deuxième partie : paires de Rudin-Shapiro

Deux polynômes séquentiels forment une paire complémentaire de polynômes lorsqu'ils sont associés à des séquences formant une paire complémentaire.

Soient les deux suites de polynômes $(P_n)_{n\in\mathbb{N}}$ et $(Q_n)_{n\in\mathbb{N}}$ défines par

$$P_0(X) = Q_0(X) = 1, \quad P_{n+1}(X) = P_n(X) + X^{2^n} Q_n(X), \quad Q_{n+1}(X) = P_n(X) - X^{2^n} Q_n(X).$$

6.a) Le calcul donne $P_1(X) = 1 + X$ et $Q_1(X) = 1 - X$ puis $P_2(X) = 1 + X + X^2 - X^3$ et $Q_2(X) = 1 + X - X^2 + X^3$.

6.b) Les premiers calculs donnent $P_0(1) = Q_0(1) = P_0(-1) = Q_0(-1) = 1$,

$P_1(1) = Q_1(-1) = 2$ et $Q_1(1) = P_1(-1) = 0$,

$P_2(1) = Q_2(1) = P_2(-1) = -Q_2(-1) = 2$,

$P_3(1) = Q_3(-1) = 4$ et $Q_3(1) = P_3(-1) = 0$,

$P_4(1) = Q_4(1) = P_4(-1) = -Q_4(-1) = 4$.

Montrons par récurrence sur $k \geqslant 1$ que $P_{2k}(1) = Q_{2k}(1) = P_{2k}(-1) = -Q_{2k}(-1) = 2^k$, $P_{2k-1}(1) = Q_{2k-1}(-1) = 2^k$ et $P_{2k-1}(-1) = Q_{2k-1}(1) = 0$.

le résultat est vrai pour $k = 1$ et $k = 2$.

On suppose le résultat vrai jusqu'à l'ordre $k \geqslant 2$.

On a $P_{2k+1}(1) = P_{2k}(1) + Q_{2k}(1) = 2^k + 2^k = 2^{k+1}$ et $Q_{2k+1}(1) = P_{2k}(1) - Q_{2k}(1) = 2^k - 2^k = 0$,
$P_{2k+1}(-1) = P_{2k}(-1) + Q_{2k}(-1) = 2^k - 2^k = 0$ et $Q_{2k+1}(-1) = P_{2k}(-1) - Q_{2k}(-1) = 2^k + 2^k = 2^{k+1}$
ensuite $P_{2k+2}(1) = P_{2k+1}(1) + Q_{2k+1}(1) = 2^{k+1} + 0 = 2^{k+1}$ et $Q_{2k+2}(1) = P_{2k+1}(1) - Q_{2k+1}(1) = 2^{k+1}$,
$P_{2k+2}(-1) = P_{2k+1}(-1) + Q_{2k+1}(-1) = 0 + 2^{k+1} = 2^{k+1}$ et $Q_{2k+2}(-1) = P_{2k+1}(-1) - Q_{2k+1}(-1) = -2^{k+1}$,
le résultat est donc vrai à l'ordre $k+1$.

7. Montrons par récurrence sur $n \in \mathbb{N}$ que P_n et Q_n forment une paire complémentaire de polynômes.
Par convention, c'est vrai pour $n = 0$ car $P_0 = 1$ et $Q_0 = 1$.
$P_1(x)P_1(x^{-1}) + Q_1(x)Q_1(x^{-1}) = (1+x)(1+\frac{1}{x}) + (1-x)(1-\frac{1}{x}) = 4$ et
P_1 et Q_1 ont leurs coefficients valant ± 1 donc c'est vrai pour $n = 1$.
On suppose le résultat vrai jusqu'à l'ordre $n \geqslant 1$.
La valuation de $X^{2^n}Q_n(X)$ est égale au degré de $Q_n(X)$ augmenté de 1, donc $P_{n+1}(X)$ et $Q_{n+1}(X)$ ont tous leurs coefficients valant ± 1.
On a

$$\begin{aligned} P_{n+1}(x)P_{n+1}(x^{-1}) &= (P_n(x) + x^{2^n}Q_n(x))(P_n(x^{-1}) + x^{-2^n}Q_n(x^{-1})) \\ &= P_n(x)P_n(x^{-1}) + Q_n(x)Q_n(x^{-1}) + x^{2^n}Q_n(x)P_n(x^{-1}) + x^{-2^n}P_n(x)Q_n(x^{-1}). \end{aligned}$$

et

$$\begin{aligned} Q_{n+1}(x)Q_{n+1}(x^{-1}) &= (P_n(x) - x^{2^n}Q_n(x))(P_n(x^{-1}) - x^{-2^n}Q_n(x^{-1})) \\ &= P_n(x)P_n(x^{-1}) + Q_n(x)Q_n(x^{-1}) - x^{2^n}Q_n(x)P_n(x^{-1}) - x^{-2^n}P_n(x)Q_n(x^{-1}) \end{aligned}$$

ainsi

$$P_{n+1}(x)P_{n+1}(x^{-1}) + Q_{n+1}(x)Q_{n+1}(x^{-1}) = 2P_n(x)P_n(x^{-1}) + 2Q_n(x)Q_n(x^{-1})$$

est constant. Le résultat est donc vrai à l'ordre $k+1$.
P_k et Q_k sont associés à des séquences de longueur 2^k. D'après **3.a)**, on a donc $2^k \in \mathcal{L}$ pour tout $k \in \mathbb{N}$.

8. Montrons par récurrence sur $n \geqslant 0$ que pour tout $z \in \mathbb{C}\backslash\{0\}$, on a $Q_n(z) = (-1)^n z^{2^n-1}P_n(-z^{-1})$.
Pour $n = 0$ le résultat est trivial car $P_0 = Q_0 = 1$
Pour $n = 1$, on a $-zP_1(-z^{-1}) = -z + 1 = Q_1(z)$.
On suppose l'égalité établie jusqu'à l'ordre $n \geqslant 1$.
On a $P_{n+1}(-z^{-1}) = P_n(-z^{-1}) + z^{-2^n}Q_n(-z^{-1})$ avec $Q_n(-z^{-1}) = (-1)^{n+1}z^{-2^n+1}P_n(z)$
ainsi $P_{n+1}(-z^{-1}) = P_n(-z^{-1}) + (-1)^{n+1}z^{-2^{n+1}+1}P_n(z)$
et $(-1)^{n+1}z^{2^{n+1}-1}P_{n+1}(-z^{-1}) = (-1)^{n+1}z^{2^{n+1}-1}P_n(-z^{-1}) + P_n(z)$.
Par ailleurs $Q_{n+1}(z) = P_n(z) - z^{2^n}Q_n(z) = P_n(z) + (-1)^{n+1}z^{2^{n+1}-1}P_n(-z^{-1})$.
D'où l'égalité à l'ordre $n+1$.

9.a) Soit $T(X) = t_0 + t_1X + \ldots + t_dX^d \in \mathbb{C}[x]$ de degré $d \geqslant 1$. Montrons que toute racine $z \in \mathbb{C}$ de T vérifie $|z| \leqslant 1 + M$ où $M = \sup\limits_{0 \leqslant i \leqslant d-1} |t_i/t_d|$.
Si $|z| \leqslant 1$ l'inégalité est évidente.
Si $|z| > 1$ on a $z^d = -\dfrac{t_0}{t_d} - \dfrac{t_1}{t_d}z \ldots - \dfrac{t_{d-1}}{t_d}z^{d-1}$ donc $|z|^d \leqslant M(1 + |z| + \ldots + |z|^{d-1})$.
Il vient $|z|^d(|z|-1) \leqslant M(|z|^d - 1)$, puis $|z| - 1 \leqslant M\dfrac{|z|^d - 1}{|z|^d} \leqslant M$ d'où l'inégalité $|z| \leqslant 1 + M$.

9.b) Soit z une racine (complexe) du polynôme P_nQ_n pour $n \geqslant 1$. Alors z est racine de P_n ou de Q_n et $z \neq 0$.

Comme les coefficients de P_n ou Q_n valent ± 1, on obtient, d'après **9.a)** $|z| \leqslant 2$.

D'après **8.**, on a $Q_n(z) = (-1)^n z^{2^n-1} P_n(-z^{-1})$ donc $P_n(z) = (-1)^{n+1} z^{2^n-1} Q_n(-z^{-1})$ ainsi $-z^{-1}$ est racine de P_n ou de Q_n donc d'après **9.a)** $|z^{-1}| \leqslant 2$. Finalement

$$\frac{1}{2} \leqslant |z| \leqslant 2.$$

Si $|z| = 2$, alors $|z^{2^n-1}| = |R_n(z)|$ où R_n est le polynôme P_n ou Q_n tronqué à l'ordre $2^n - 2$.
On a $|z^{2^n-1}| = 2^{2^n-1}$ et $|R_n(z)| \leqslant 2^{2^n-2} + \ldots + 2 + 1 = 2^{2^n-1} - 1$ ce qui est impossible.
Si $|z| = \dfrac{1}{2}$, on considère la racine $-z^{-1}$ pour se ramener au cas antérieur.
Il en résulte que les deux inégalités sont strictes.

10.a) P_n est la partie de P_{n+1} tronquée à l'ordre $2^n - 1$, il existe donc une série entière, $S(z) = \sum_{p=0}^{\infty} u_p z^p$, dont les P_n sont des sommes partielles.
Comme $|u_p| = 1$ pour tout p, le rayon de convergence est égal à 1.

10.b) On a $P_n(z) = \sum_{p=0}^{2^n-1} u_p z^p$ avec $u_p = \pm 1$.

Pour tout $|z| \leqslant \dfrac{1}{2}$, on a $|P_n(z)| \geqslant 1 - \left|\sum_{p=1}^{2^n-1} u_p z^p\right|$ avec $\left|\sum_{p=1}^{2^n-1} u_p z^p\right| \leqslant \sum_{p=1}^{2^n-1} \dfrac{1}{2^p} = 1 - 2^{1-2^n}$ ainsi $|P_n(z)| \geqslant 2\left(\dfrac{1}{2}\right)^{2^n}$.

Supposons que la somme de la série S ait un zéro z_0 tel que $|z_0| < \dfrac{1}{2}$.

On a $|P_n(z_0)| = |S(z_0) - P_n(z_0)| \leqslant \sum_{p=2^n}^{\infty} |z_0|^p = \dfrac{1}{1-|z_0|}|z_0|^{2^n}$.

On aboutit à une contradiction, puisque $\dfrac{1}{1-|z_0|}|z_0|^{2^n} < 2\left(\dfrac{1}{2}\right)^{2^n}$.

La somme de la série S n'a donc pas de zéros dans le disque ouvert de rayon 1/2 centré à l'origine.