Décomposants de Goldbach généralisés (pouvant être négatifs), et ondes prolate
Denise Vella-Chemla

1. Présentation

Ce texte explique comment utiliser la notion de fonction prolate pour trouver les décomposants de Goldbach d'un nombre pair. On pose $h = n/2$ et $u = x - h$. Une décomposition $n = x + y$ s'écrit alors

$$n = (h - u) + (h + u),$$

et $|u|$ est l'écart au centre. Le recentrage est un simple décalage d'origine : les solutions "dans la fenêtre autorisée" pour $n = 98$ sont $u = \pm 12, \pm 18, \pm 30$ au lieu de $x = 19, 31, 37, 61, 67, 79$) ; une *symétrie* $u \leftrightarrow -u$ permet de travailler avec des fonctions paires.

Pour un nombre pair n, on construit un ensemble $S_0 \subset \mathbb{Z}$, périodique et symétrique, défini par des conditions sur les restes modulo les petits premiers. Dans la fenêtre $[-n/2, n/2]$, il coïncide (à une réserve près, proposition **??**) avec l'ensemble des u tels que $h-u$ et $h+u$ soient tous deux premiers. On regarde S_0 comme un signal (une suite de 0 et de 1), on le "floute" par un filtre passe-bas, puis on projette ce signal flouté, restreint à la fenêtre, sur les fonctions sphéroïdales prolates (de Slepian), puis on compare aux vraies solutions.

2. Les données et les notations

2.1. Entrées du programme

n est le nombre pair étudié, h sa moitié (le centre). E dit jusqu'où l'on regarde au-delà de 0 et de n, $u \in [-E - h,\ E + h]$; il contient donc des entiers de part et d'autre de 0. W règle le "flou" (section **??**) ; plus W est petit, plus le flou est grand.

2.2. Les petits premiers et la période

Définition : soit $\mathcal{P} = \{p \text{ premier} : p \leq \sqrt{n}\}$ (`ps`).

On pose $M = \prod_{p \in \mathcal{P}} p$.

Pour $n = 98$: $h = 49$, $\mathcal{P} = \{2, 3, 5, 7\}$, $M = 210$, et $h \bmod p = (1, 1, 4, 0)$ pour $p = 2, 3, 5, 7$ (le programme affiche "restes de h : (1, 1, 4, 0)").

On ne garde que les premiers dont le carré ne dépasse pas n. Le nombre M est leur produit. On travaille dans les corps $\mathbb{Z}/p\mathbb{Z}$, un par petit premier p.
Dans la suite, on considère comme nombre premier un nombre dont la valeur absolue est un nombre premier : ainsi -11 et -103 sont premiers au même titre que 19 et 43.

3. L'ensemble S_0 des restes admis, centré en 0

3.1. Définition

Définition : pour n pair, $h = n/2$, on pose

$$\begin{aligned} S_0 &= \Big\{ u \in \mathbb{Z} \ : \ \forall p \in \mathcal{P},\ p \nmid (h+u) \ \text{ et } \ p \nmid (h-u) \Big\} \\ &= \Big\{ u \in \mathbb{Z} : \ \operatorname{pgcd}(h+u, M) = \operatorname{pgcd}(h-u, M) = 1 \Big\}. \end{aligned}$$

C'est l'ensemble S de la version non centrée, décalé de h : $u \in S_0 \iff x = h+u \in S$ (car $n - x = h - u$). La fonction `dans_S0(u, h, ps)` calcule l'indicatrice $\mathbf{1}_{S_0}(u)$; le tableau `s` est la suite

$$s_j = \mathbf{1}_{S_0}(u_j), \qquad u_j = j - (E+h), \qquad j = 0, \dots, L-1, \qquad L = n + 2E + 1,$$

valeurs de $\mathbf{1}_{S_0}$ sur tous les entiers de $[-E-h,\ E+h]$ (`us = np.arange(-E-h, E+h+1)`). Cette plage est symétrique par rapport à 0 ; son centre est l'indice $j = E + h = (L-1)/2$.

Écrire $x = h + u$ et $y = h - u$ revient à mesurer chaque décomposant par son écart u au centre. L'entier u est admis si ni $h+u$ ni $h-u$ n'est multiple d'un petit premier. Python donne un reste positif même pour un entier négatif, ce qui est exactement ce qu'il faut.

3.2. Propriétés de S_0

Proposition 1. *On a que :*

1. *S_0 est symétrique : $u \in S_0 \iff -u \in S_0$ (échanger u et $-u$ échange $h+u$ et $h-u$).*
2. *S_0 est périodique de période M (restes chinois).*
3. *Dans une période, S_0 compte exactement*

$$\prod_{p \in \mathcal{P},\ p \mid n} (p-1) \prod_{p \in \mathcal{P},\ p \nmid n} (p-2)$$

éléments, donc sa densité moyenne est ce nombre divisé par M.

Démonstration. (a) et (b) sont immédiats.

(c) Modulo p, la condition interdit les classes $u \equiv -h$ et $u \equiv h$. Ces deux classes sont distinctes sauf si $2h = n \equiv 0 \pmod p$; dans ce cas il n'y en a qu'une ($p-1$ restes permis), sinon $p-2$ restes sont permis ; le théorème chinois donne le produit. □

Pour $n = 98$: $p = 2, 3, 5, 7$ donnent respectivement $1, 1, 3, 6$ restes permis (car $2 \mid 98$ et $7 \mid 98$ donnent $p-1$, et $3, 5 \nmid 98$ donnent $p-2$), soit 18 éléments par période de 210, densité $\approx 0{,}0857$. Sur $[-147, 147]$, S_0 contient les 26 éléments (chaque signe compté)

$$\begin{aligned} S_0 \cap [-147, 147] = \{ &\pm 138, \pm 132, \pm 120, \pm 108, \pm 102, \pm 90, \pm 78, \pm 72, \pm 60, \\ &\pm 48,\ \pm 30,\ \pm 18,\ \pm 12 \}, \end{aligned}$$

soit en $x = h + u$ la liste $-89, -83, \dots, 19, 31, \dots, 187$ de la version non centrée. On remarque que les u sont tous pairs : c'est l'effet de $p = 2$ (ici $h = 49$ est impair, donc $h \pm u$ n'est impair que si u

est pair).

S_0 est un motif qui se répète tous les M entiers, et il est exactement symétrique par rapport à 0 : si u convient, $-u$ aussi. C'est la symétrie "$x \leftrightarrow n-x$" de la version non centrée, devenue un simple changement de signe.

3.3. Que représente S_0 dans la fenêtre ?

Proposition 2. *Pour $|u| \le h-3$ (c'est-à-dire $3 \le h+u \le n-3$) :*

$$u \in S_0 \iff h-u \text{ et } h+u \text{ sont premiers et tous deux } > \sqrt{n}.$$

Démonstration. ($\Rightarrow$) Si $u \in S_0$, aucun $p \le \sqrt{n}$ ne divise $h+u \ge 3$. S'il était composé, il aurait un facteur premier $\le \sqrt{h+u} \le \sqrt{n}$, donc dans $\mathcal{P}$: contradiction. Il est donc premier, et $> \sqrt{n}$. Même raisonnement pour $h-u \ge 3$. ($\Leftarrow$) Un premier $> \sqrt{n}$ n'est divisible par aucun $p \le \sqrt{n}$. □

Conséquence et réserve. Les "vraies solutions" (`vraies`) sont donc les u tels que les *deux* termes $h \pm u$ dépassent $\sqrt{n}$. Si $n = p+q$ avec $p \le \sqrt{n}$ premier et q premier, c'est une décomposition de Goldbach ; la fenêtre $[-46, 46]$ contient exactement $u \in \{\pm 12, \pm 18, \pm 30\}$, c'est-à-dire les trois décompositions $37+61$, $31+67$, $19+79$, chacune comptée deux fois (par u et par $-u$).

3.4. Les éléments de S_0 hors fenêtre (les "intrus")

Hors de la fenêtre, S_0 contient des u pour lesquels $h-u$ ou $h+u$ n'est pas premier (variable `intrus`). Pour $n = 98$:

$$u \in \{\pm 48,\ \pm 72,\ \pm 120,\ \pm 138\},$$

ce qui correspond à $x = h+u \in \{1, 97, 121, 169, -23, -71, -89, 187\}$. Raisons : $u = \pm 48$ donne $\{1, 97\}$ (1 n'est pas premier) ; $u = \pm 72$ donne $\{121, -23\}$ avec $121 = 11^2$; $u = \pm 120$ donne $\{169, -71\}$ avec $169 = 13^2$; $u = \pm 138$ donne $\{187, -89\}$ avec $187 = 11 \cdot 17$.

Dans la fenêtre, ce qui passe le filtre des restes est automatiquement premier (un nombre composé a un petit diviseur). En dehors, ce n'est plus vrai dès que le nombre atteint $11^2 = 121$ (le carré du premier suivant $\sqrt{98}$), ou vaut ± 1.

4. Les décompositions avec des premiers négatifs

Le programme parcourt tous les $u \in [-E-h,\ E+h]$ et retient ceux qui vérifient

$$u \le 0, \qquad |h+u| \text{ premier}, \qquad |h-u| \text{ premier}.$$

La condition $u \le 0$ équivaut à $x = h+u \le n-x = h-u$ (on ne compte qu'une fois chaque couple). Comme $h-u \ge h > 0$, seul $x = h+u$ peut être négatif ; on écrit alors $x = -q$ avec q premier et $n+q$ premier. Cela correspond à $u = -(h+q) < -h$: *les décompositions à premier négatif sont celles dont l'écart au centre dépasse h*, c'est-à-dire qui sortent de l'intervalle $[-h, h]$ (l'ancien $[0, n]$). Pour chaque solution, le programme affiche x, y, u, les restes $(x \bmod p)_{p \in \mathcal{P}}$ et une marque "premier négatif" si $x < 0$, "petit premier, hors de S_0" si $u \notin S_0$.

Proposition 3. *Si $x = -q < 0$ avec q et $n+q$ premiers, alors $u = -(h+q) \in S_0 \iff q > \sqrt{n}$.*

Démonstration. $h - u = n + q$ est premier et $> \sqrt{n}$: aucun $p \in \mathcal{P}$ ne le divise. Reste $p \nmid h + u = -q$ pour tout $p \in \mathcal{P}$, soit $q \notin \mathcal{P}$, soit $q > \sqrt{n}$. □

Pour $n = 98$, le programme trouve 3 décompositions positives et 8 avec un premier négatif :

$98 = 19 + 79$ $(u = -30)$, $98 = 31 + 67$ $(u = -18)$, $98 = 37 + 61$ $(u = -12)$,
$98 = -11 + 109$ $(u = -60)$, $98 = -29 + 127$ $(u = -78)$, $98 = -41 + 139$ $(u = -90)$,
$98 = -53 + 151$ $(u = -102)$, $98 = -59 + 157$ $(u = -108)$, $98 = -83 + 181$ $(u = -132)$,
$98 = -5 + 103$ $(u = -54)$, $98 = -3 + 101$ $(u = -52)$.

Tous sont dans S_0 sauf les deux dernières ($q = 5$ et $q = 3 \leq \sqrt{98}$), signalées "petit premier".

En centrant, on voit tout de suite la structure : les décompositions ordinaires ont un petit écart au centre ($|u| = 12, 18, 30 < 49$), celles à premier négatif un grand écart ($|u| > 49$). Le motif S_0 se prolonge naturellement de part et d'autre de la fenêtre par périodicité, d'où l'intérêt de le regarder sur tout $\mathbb{Z}$ et pas seulement dans $[-h, h]$.

5. Étape passe-bas : "flouter" le signal

On traite la suite $s = (s_0, \ldots, s_{L-1})$, $L = n + 2E + 1$ (pour $n = 98$, $E = 98$: $L = 295$). Sa transformée de Fourier discrète est

$$F_k = \sum_{j=0}^{L-1} s_j \, e^{-2\pi i \, jk/L}, \qquad k = 0, \ldots, L-1,$$

associée à la fréquence $f_k \in [-\frac{1}{2}, \frac{1}{2})$: $f_k = k/L$ pour $0 \leq k \leq \frac{L-1}{2}$, $f_k = (k-L)/L$ sinon (L impair). On annule les composantes de fréquence $|f_k| > W$:

$$\tilde{F}_k = F_k \cdot \mathbf{1}_{\{|f_k| \leq W\}}, \qquad s_j^{\mathrm{bl}} = \mathrm{Re}\, \frac{1}{L} \sum_{k=0}^{L-1} \tilde{F}_k \, e^{2\pi i \, jk/L} \quad (\texttt{s_bl}).$$

De façon équivalente, s^{bl} est la convolution circulaire de s par le noyau pair

$$D_W(d) = \frac{1}{L} \sum_{|f_k| \leq W} e^{2\pi i \, f_k d} \;\approx\; \frac{\sin(2\pi W d)}{\pi d} \qquad (L \text{ grand}), \qquad D_W(0) \approx 2W.$$

Une convolution circulaire ne dépend pas de l'origine choisie : décaler l'origine de x à u ne change pas s^{bl}, seulement l'étiquette de ses points. Chaque pic est remplacé par une bosse de hauteur $\approx 2W$ et de largeur $\approx 1/(2W)$ entiers (0,4 et 2,5 pour $W = 0{,}2$).

Le passe-bas ne laisse passer que les oscillations lentes : c'est un flou. Chaque 1 isolé devient une petite bosse étalée sur deux ou trois entiers, de hauteur d'environ 0,4 au lieu de 1 ; c'est pourquoi les courbes ne montent jamais jusqu'à 1.

Précautions de lecture. : la suite finie de longueur L est traitée comme circulaire : ses bords $\pm(E+h)$ sont "recollés" par la FFT. Comme $L = 295$ n'est pas un multiple de $M = 210$, cela crée de petits effets de bord, faibles au centre mais visibles aux extrémités de la courbe grise. (ii) W n'est pas un multiple exact de $1/L$: la coupure tombe entre deux fréquences discrètes.

La symétrie se conserve. : comme s est symétrique par rapport au centre $j = E + h$ de la plage et que le noyau D_W est pair, s^{bl} est encore symétrique : $s^{\mathrm{bl}}(-u) = s^{\mathrm{bl}}(u)$ (le programme le vérifie : écart $\approx 10^{-16}$).

6. La fenêtre et les fonctions prolates

6.1. La restriction à la fenêtre

On extrait la fenêtre $\{-(h-3), \dots, h-3\}$ (`fen = np.abs(us) <= h-3`), de longueur $N = 2(h-3)+1 = n-5$ ($N = 93$ pour $n = 98$, fenêtre $[-46, 46]$) : c'est exactement l'ancienne fenêtre $[3, n-3]$, maintenant symétrique autour de 0. On note $u_i = -(h-3) + i$ pour $i = 0, \dots, N-1$, et

$$r_i = s^{\mathrm{bl}}(u_i) \quad (\texttt{r}), \qquad t_i = \mathbf{1}_{S_0}(u_i) \quad (\texttt{vraies}).$$

6.2. Les fonctions prolates (découvertes par Slepian et al.)

Définition : soit $W \in (0, \frac{1}{2})$ et $N \geq 1$. La *matrice de Slepian* est la matrice symétrique réelle $A \in \mathbb{R}^{N\times N}$:

$$A_{ij} = \frac{\sin\big(2\pi W(i-j)\big)}{\pi(i-j)} \ (i \neq j), \qquad A_{ii} = 2W, \qquad \text{soit} \quad A_{ij} = \int_{-W}^{W} e^{2\pi i f(i-j)}\, df.$$

Ses valeurs propres sont $1 > \lambda_0 > \lambda_1 > \cdots > \lambda_{N-1} > 0$ (toutes simples), avec des vecteurs propres orthonormés $v_0, \dots, v_{N-1} \in \mathbb{R}^N$: les *fonctions prolates discrètes*.

Pour $v \in \mathbb{R}^N$ de norme 1 (signal nul hors fenêtre) et $V(f) = \sum_j v_j e^{-2\pi i f j}$, on a

$$\lambda(v) = v^{\top} A v = \int_{-W}^{W} |V(f)|^2\, df,$$

la *part de l'énergie de v située dans la bande* $[-W, W]$. La prolate v_0 est la suite de la fenêtre dont l'énergie est la plus concentrée dans la bande, v_1 la suivante (orthogonale à v_0), etc. Comme $\operatorname{tr} A = 2WN = \sum_k \lambda_k$ et que les λ_k valent presque 1 puis chutent brutalement, il y a environ $2NW$ valeurs propres proches de 1.

Le programme garde

$$K = \#\{k : \lambda_k > \tfrac{1}{2}\}, \qquad V = [\, v_0 \,|\, \cdots \,|\, v_{K-1} \,] \in \mathbb{R}^{N\times K}.$$

Pour $n = 98$, $W = 0{,}2$, $N = 93$: $2NW = 37{,}2$, $K = 37$, $\lambda_0 \approx 1{,}0000$ et $\lambda_{36} \approx 0{,}7264$. La fonction construit A, la diagonalise, trie par valeurs propres décroissantes et ne garde que celles $>$ seuil.

Une “fonction prolate” est une fonction signal définie sur la fenêtre, qui oscille lentement, au point que presque toute son énergie se trouve dans la bande $|f| \le W$. Il y en a environ $2NW$ de bonne qualité (ici 37) ; elles forment une base de l'espace des signaux lents que la fenêtre peut contenir.

6.3. La projection

Comme $V^\top V = I_K$, $\Pi = VV^\top$ est le projecteur orthogonal sur $E_K = \mathrm{Vect}(v_0, \dots, v_{K-1})$ et

$$p = \Pi r = \sum_{k=0}^{K-1} c_k\, v_k, \qquad c_k = \langle v_k, r \rangle.$$

On exprime le signal flouté r dans la base des prolates, on garde les K premières composantes (les “lentes”), et on recompose. Cela supprime ce qui ne peut pas être un signal lent sur la fenêtre : essentiellement les défauts créés par la coupure aux bords. Comme r était déjà lent, la courbe rouge est très proche de la courbe grise.

7. Ce que le centrage apporte : la parité

Soit J le retournement $(Jv)_i = v_{N-1-i}$, c'est-à-dire $u \mapsto -u$ dans la fenêtre centrée.

Proposition 4. *On a*

1. $JAJ = A$ *(car A_{ij} ne dépend que de $i-j$ et est pair en $i-j$), donc chaque prolate v_k est paire ($Jv_k = v_k$) ou impaire ($Jv_k = -v_k$), de parité $(-1)^k$.*
2. $Jr = r$ *(symétrie de s^{bl}, section* **??***).*
3. *Par suite $c_k = \langle v_k, r\rangle = 0$ pour k impair, Π commute avec J, et $Jp = p$: la projection est symétrique, et seules les prolates paires interviennent. Pour $K = 37$: les 19 prolates $v_0, v_2, \dots, v_{36}$ (sur 37).*

Démonstration. On a

(a) A est une matrice de Toeplitz symétrique, donc persymétrique ; ses valeurs propres étant simples, chaque vecteur propre est invariant ou changé en son opposé par J, et la parité alterne avec k (résultat classique de Slepian).

(b) s est symétrique par rapport au centre de la plage (proposition **??**(a)) et le noyau D_W est pair.

(c) Si k est impair, v_k est impaire et r paire, donc orthogonales.

□

Réserve numérique. : les premières valeurs propres sont égales à 1 à la précision machine près (les 27 premières pour $n = 98$, $W = 0{,}2$) : `eigh` ne peut alors pas les distinguer, et renvoie des combinaisons quelconques de prolates paires et impaires dans ce paquet. Les vecteurs pris individuellement n'ont donc pas toujours une parité nette dans le calcul, mais le sous-espace E_K, le projecteur Π et le résultat p ne sont pas affectés. Le programme vérifie la symétrie directement : `|r - J r|` et `|proj - J proj|` sont de l'ordre de 10^{-16} à 10^{-15}.

Comme tout est symétrique autour de 0, le signal ne contient que des “motifs pairs”. La moitié des prolates (les impaires, qui changent de signe quand on passe de u à $-u$) ne peuvent donc rien apporter : le calcul se ramène à 19 prolates sur 37. Mathématiquement, on pourrait travailler sur la demi-fenêtre $u \in [0, h-3]$ seulement.

8. La décision et la comparaison aux vraies solutions

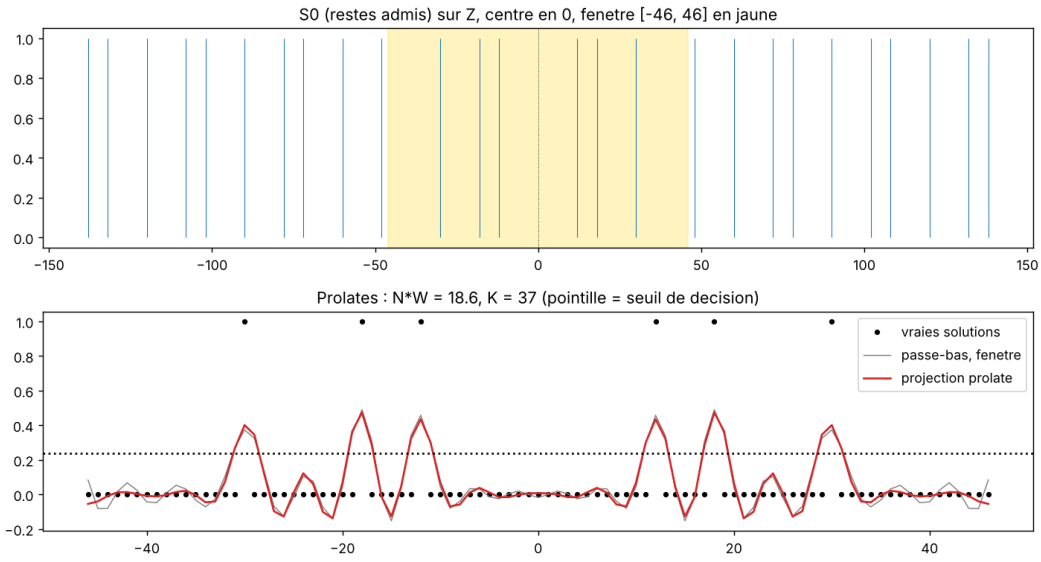
Les bosses de la projection ont une hauteur de 0,4 à 0,48, non 1 : le programme utilise un seuil *relatif*,

$$\sigma = \frac{1}{2}\max_i p_i \quad (\texttt{seuil}), \qquad d_i = \mathbf{1}_{\{p_i > \sigma\}} \quad (\texttt{decide}),$$

Pour $n = 98$: les $T = 6$ plus grandes valeurs de la projection sont en $u = -30, -18, -12, 12, 18, 30$, exactement les vraies solutions ; aucune solution ratée.

Cependant, le problème est que les entiers voisins des solutions effectives passent aussi le filtre passe-bas.
On compare ce que le programme “croit” (là où la courbe rouge dépasse la moitié de son maximum) et la réalité. Le flou étale chaque pic sur trois cases, d'où les douze fausses alarmes (6×2). Le test le plus parlant est celui des T plus grandes valeurs : les six sommets tombent exactement sur les six vraies solutions, qui sont symétriques par rapport à 0.

Lecture du dessin. Dans cette version, la ligne pointillée horizontale du graphique du bas est tracée au niveau du seuil réel σ (et non plus à 0,5 comme dans la version non centrée) ; le graphique du haut montre S_0 sur $[-E-h, E+h]$ avec la fenêtre en jaune et l'axe $u = 0$ en pointillé.



Sortie graphique pour $n = 98$, $E = 98$, $W = 0{,}2$ (centré en 0).

9. Intérêt et limites du programme

1. *L'utilisation des fonctions prolates* : le filtre passe-bas et la projection sont le pendant lisse de l'approche par filtrage de certains restes modulaires.
2. *Le filtre passe-bas doit être calibré* : les voisins immédiats des nombres impairs correspondant aux décomposants de Goldbach ne doivent pas pouvoir passer pas à travers le filtre. Une bosse a une largeur $\approx 1/(2W)$; deux solutions voisines restent séparées seulement si leur distance dépasse cette largeur.
3. *La symétrie ne diminue pas la difficulté.* On considère des fonctions paires uniqueement.
4. Cette approche *ne permet pas d'aller vers une démonstration de la conjecture de Goldbach* : elle ne permet que la visualisation des décomposants pour de petits nombres pairs.