L'application différence

Daniel PERRIN

Le problème qui suit m'a été posé[1] *par André Béthermin. C'est aussi lui qui m'a mis sur la piste du cas $n = 2^r$ et il m'a posé une multitude de questions pertinentes auxquelles j'essaie de répondre dans ce qui suit. Pour tout cela, je le remercie chaleureusement.*

1 Le problème et le résultat

1.1 La fonction F_n

Soit n un entier ≥ 2. On considère l'application $F_n : \mathbf{R}^n \to (\mathbf{R}^+)^n$ définie par :

$$F_n(x_1, \ldots, x_n) = (|x_1 - x_2|, |x_2 - x_3|, \ldots, |x_{n-1} - x_n|, |x_n - x_1|).$$

Cette fonction associe à un n-uplet de points de $\mathbf{R}$ les distances de ses points pris dans l'ordre (en regardant les indices modulo n). Lorsque l'entier n est bien identifié, on la notera simplement F.

1.2 Notations

On travaille dans $\mathbf{R}^n$ qui est muni de sa structure d'espace vectoriel naturelle et c'est en ce sens qu'on parlera d'addition et de multiplication par un scalaire. On a donc $0 = (0, 0, \ldots, 0)$. On pose $\underline{a} = (a, a, \ldots, a)$ pour $a \in \mathbf{R}$. On note $e_1, \ldots, e_n$ la base canonique de $\mathbf{R}^n$.

1.3 Le résultat principal

On se propose d'étudier les itérées de l'application F, en particulier lorsque les x_i sont entiers, voire rationnels. Voici quelques questions naturelles issues de l'expérience avec des x_i entiers : les $F^N(X)$ finissent-ils toujours par être nuls ? Ou au contraire définissent-ils des cycles ? Le théorème suivant fait le bilan des principaux résultats obtenus.

1.1 Théorème. *Soit n un entier ≥ 2.*

1. Parmi beaucoup d'autres issus de son imagination fertile !

1) On suppose que n est une puissance de 2 : $n = 2^\alpha$. Alors, pour tout $X \in \mathbf{Q}^n$, il existe N tel que $F^N(X) = 0$ (et alors $F^M(X) = 0$ pour $M \geq N$).

2) On suppose que n n'est pas une puissance de 2, $n = 2^\alpha m$ avec $\alpha \geq 0$ et m impair, $m > 1$. Alors, pour tout X dans $\mathbf{Q}^n$, on a l'alternative suivante :

- *Ou bien il existe N tel que $F^N(X) = 0$.*
- *Ou bien il existe $M, N \in \mathbf{N}$, avec $M > 0$, et $a \in \mathbf{Q}$ tels que*[2] *$Y := F^N(X) \in \{0, a\}^n$ et $F^M(Y) = Y$.*

1.2 *Exemples.* 1) Pour $n = 4$ et $X = (3, 2, 6, 1)$ les itérés successifs sont $(1, 4, 5, 2)$, $(3, 1, 3, 1)$, $(2, 2, 2, 2)$ et $(0, 0, 0, 0)$.

2) Pour $n = 3$ et $X = (3, 7, 2)$ on obtient successivement $(4, 5, 1)$, $(1, 4, 3)$, $(3, 1, 2)$, $(2, 1, 1)$, $(1, 0, 1)$, $(1, 1, 0)$, $(0, 1, 1)$, $(1, 0, 1)$, etc.

Pour une discussion sur la longueur de la période M, voir §4.17.

2 Préliminaires

2.1 Quelques remarques

2.1 *Remarques.* Soit $X \in \mathbf{R}^n$.

1) Si a est un réel positif, on a $F(aX) = aF(X)$.

2) Si a est un réel quelconque, on a $F(X + \underline{a}) = F(X)$.

3) Si γ est la permutation circulaire : $\gamma = (1, 2, \ldots, n)$, opérant sur $\mathbf{R}^n$ par $\gamma(x_1, \ldots, x_n) = (x_2, x_3, \ldots, x_n, x_1)$, on a $F \circ \gamma = \gamma \circ F$ et donc aussi $F^n \circ \gamma = \gamma \circ F^n$.

2.2 Définition. *1) Soit $X = (x_1, \ldots, x_n) \in \mathbf{R}^n$. On dit que X est* **normalisé** *si l'on a $x_i \geq 0$ pour tout i et si l'un des x_i est nul.*

2) Soit $X \in \mathbf{Z}^n$ et soit $a \in \mathbf{Z}$. On dit que a divise X si l'on a $X = aY$ avec $Y \in \mathbf{Z}^n$. On dit que X est **irréductible** *si l'on a pgcd $(x_1, \ldots, x_n) = 1$.*

2.3 *Remarque.* Pour étudier le comportement des F^n on peut se ramener à un X normalisé. En effet, il suffit de prendre le plus petit des x_i et de le retrancher aux autres (cf. 2.1.2). On peut même souvent supposer que c'est x_1 qui est nul en effectuant une permutation circulaire (cf. 2.1.3).

2.2 Injectivité, surjectivité

L'application F n'est pas injective. En effet, on a vu en 2.1.2 qu'on a $F(X + \underline{a}) = F(X)$. Notons, par exemple :

2. L'élément Y est ce que nous appellerons plus loin un soliton.

2.4 Proposition. *On a $F(X) = 0$ si et seulement si $X = \underline{a}$, avec $a \in \mathbf{R}$.*

Elle est évidemment à valeurs positives ou nulles, mais son image n'est jamais $(\mathbf{R}^+)^n$ tout entier :

2.5 Proposition. *L'application $F : \mathbf{R}^n \to (\mathbf{R}^+)^n$ n'est jamais surjective. Précisément l'image de F est contenue dans la réunion des 2^{n-1} hyperplans d'équations $\epsilon_1 y_1 + \epsilon_2 y_2 + \cdots + \epsilon_n y_n = 0$ avec $\epsilon_i = \pm 1$.*

Démonstration. Soit $X \in \mathbf{R}^n$ un élément non nul. On pose $\epsilon_i = 1$ si $x_{i+1} \geq x_i$ et $\epsilon_i = -1$ si $x_{i+1} < x_i$. On a alors :

$$F(X) = (\epsilon_1(x_2 - x_1), \epsilon_2(x_3 - x_2), \ldots, \epsilon_{n-1}(x_n - x_{n-1}), \epsilon_n(x_1 - x_n))$$

$$:= (y_1, \ldots, y_n)$$

et on a $\displaystyle\sum_{i=1}^{n} \epsilon_i y_i = (x_2 - x_1) + (x_3 - x_2) + \cdots + (x_1 - x_n) = 0$. On notera qu'on a ainsi 2^n équations $f_i = 0$ mais seulement 2^{n-1} hyperplans car f_i et $-f_i$ donnent le même hyperplan.

Comme on sait qu'une réunion finie d'hyperplans est d'intérieur vide, elle ne peut jamais être égale à $\mathbf{R}^n$.

2.6 *Remarque.* Il résulte de 2.1.2 que si Y est dans l'image de F il admet un antécédent X normalisé. Attention, ici, on ne peut pas supposer que c'est x_1 qui est nul. Par exemple $Y = (1, 3, 2)$ admet l'antécédent normalisé $X = (2, 3, 0)$ mais pas d'antécédent de la forme $(0, b, c)$ avec $b, c \geq 0$.

Du côté des entiers, on a deux résultats :

2.7 Corollaire. *Soit $Y = (y_1, \ldots, y_n) \in \mathbf{N}^n$. Si Y est dans* $\operatorname{Im} F$*, la somme des y_i est paire. En particulier, si n est impair, l'élément $\underline{a}$ avec $a \in \mathbf{N}^*$ n'est pas dans* $\operatorname{Im} F$*.*

Démonstration. En vertu de 2.5 on a $\displaystyle\sum_{i=1}^{n} \epsilon_i y_i = 0$ avec $\epsilon_i = \pm 1$. Si J est l'ensemble des i tels que $\epsilon_i = -1$, on a :

$$\sum_{i=1}^{n} y_i = \sum_{i=1}^{n} \epsilon_i y_i + 2 \sum_{i \in J} y_i = 2 \sum_{i \in J} y_i$$

d'où le résultat.

2.8 Lemme. *Soit $X \in \mathbf{N}^n$. Si X est dans l'image de F et s'il est multiple de $a \in \mathbf{N}$, il admet un antécédent normalisé et tout antécédent normalisé de X est aussi multiple de a.*

Démonstration. On pose $X = (x_1, \ldots, x_n)$. L'existence d'un antécédent normalisé Y vient de 2.3. Quitte à effectuer une même permutation circulaire sur X et Y on se ramène au cas où y_1 est nul. On a $|y_i - y_{i+1}| = x_i$. Comme les x_i sont multiples de a, une récurrence immédiate sur i montre que les y_i le sont aussi.

2.9 *Remarque.* Si n est pair, $n = 2p$, $\underline{a}$ est dans l'image grâce à la formule $\underline{a} = F(0, a, 0, a, \ldots 0, a)$. Mais il y a de nombreuses autres solutions, même en se limitant aux nombres positifs, par exemple :

$$\underline{a} = F(0, a, 2a, \ldots, pa, (p-1)a, \ldots, 2a, a).$$

La question de déterminer les X tels que $F^N(X) = \underline{a}$ (et donc $F^{N+1}(X) = 0$) n'est donc pas évidente. Voici un exemple, pour $n = 6$:

2.10 Proposition. *On suppose $n = 6$. Soit $a \in \mathbf{N}^*$. Les $X = (x_1, \ldots, x_6) \in \mathbf{N}^6$ dont l'image est $\underline{a}$ sont $(0, a, 0, a, 0, a)$, $(0, a, 0, a, 2a, a)$, $(0, a, 2a, a, 0, a)$, $(0, a, 2a, a, 2a, a)$ et $(0, a, 2a, 3a, 2a, a)$, les éléments obtenus à partir de ceux-là par permutation circulaire et les éléments obtenus à partir des précédents en leur ajoutant $\underline{b}$ avec $b \in \mathbf{N}$. Aucun de ces éléments n'est dans l'image de F.*

Démonstration. Soit X tel que $F(X) = \underline{a}$ et soit m le minimum des éléments de X. Quitte à retrancher $\underline{m}$ on peut supposer X normalisé. Si σ est une permutation circulaire qui place un zéro en tête, quitte à appliquer σ on peut supposer $x_1 = 0$. On a alors $x_2 = x_6 = a$. On en déduit que x_3 et x_5 valent 0 ou $2a$. En distinguant les quatre cas, on trouve les valeurs possibles pour x_3. La dernière assertion, après division par a, vient de 2.7.

2.3 Norme

On munit l'espace $\mathbf{R}^n$ de la norme *sup* définie par $\|X\| = \mathrm{Max}_i\, |x_i|$.
On a le lemme suivant :

2.11 Lemme. *Pour $X \in (\mathbf{R}^+)^n$, F diminue la norme : on a $\|F(X)\| \leq \|X\|$. De plus l'inégalité est stricte si tous les x_i sont > 0 et plus précisément s'il n'y a pas un terme nul et un terme maximal côte à côte.*

Démonstration. En effet, on a $|x_{i+1} - x_i| \leq \mathrm{Max}\,(|x_i|, |x_{i+1}|) \leq \|X\|$ comme on le voit en distinguant selon le signe de $x_{i+1} - x_i$.

2.12 *Remarque.* L'application F est continue sur $\mathbf{R}^n$ et plus précisément lipschitzienne de rapport 2, autrement dit $\|F(X) - F(Y)\| \leq 2\|X - Y\|$. En effet, cela résulte de l'inégalité :

$$|x_{i+1} - x_i| - |y_{i+1} - y_i| \leq |x_{i+1} - y_{i+1}| + |x_i - y_i|$$

qui résulte de l'égalité ci-dessous et de l'inégalité triangulaire :

$$x_{i+1} - x_i = x_{i+1} - y_{i+1} + y_{i+1} - y_i + y_i - x_i.$$

Ce résultat est optimal comme on le voit en prenant $X = (a, b, 0, \ldots, 0)$ et $Y = (a - \epsilon, b + \epsilon, 0, \ldots, 0)$ avec $0 < \epsilon < a < b$. En effet, on a $\|X - Y\| = \epsilon$, $F(X) = (b-a, b, 0, \ldots, 0, a)$ et $F(Y) = (b-a+2\epsilon, b+\epsilon, 0, \ldots, 0, a-\epsilon)$, donc $\|F(X) - F(Y)\| = 2\epsilon$.

2.4 Points fixes et cycles

2.13 Proposition. *L'application F n'a pas d'autre point fixe que* 0.

Démonstration. Si X est fixe, ses termes sont ≥ 0 et la remarque 2.11 montre que l'un de ses termes est nul. Quitte à faire une permutation circulaire, on peut supposer qu'on a $x_1 = 0$ et on montre par récurrence qu'on a $x_i = 0$ pour tout i.

2.14 *Remarque.* En ce qui concerne les cycles, le théorème 1.1 montre qu'il n'y a pas de cycle de longueur > 1 lorsque n est une puissance de 2. Le lecteur pourra traiter le cas $n = 4$ directement à titre d'exercice.

3 Le lemme des solitons

3.1 Le lemme

3.1 Définition. *Soit $X \in \mathbf{N}^n$ et soit a un entier positif. On dit que X est un a-soliton (ou simplement un* **soliton***) si X est dans $\{0, a\}^n$ (autrement dit, X ne comporte que des* 0 *et des a).*

On note que l'ensemble $\{0, a\}^n$ est stable par F. Le résultat est alors le suivant :

3.2 Théorème. (Lemme des solitons) *Soit $X \in \mathbf{N}^n$. Il existe $N \in \mathbf{N}^*$ tel que $F^N(X)$ soit un soliton.*

Démonstration. On raisonne par l'absurde en supposant qu'il existe $X \in \mathbf{N}^n$ tel qu'aucun $F^N(X)$ ne soit un soliton. Comme l'application F diminue la norme, on peut supposer l'entier $b := \|X\|$ minimum et on a évidemment $b > 0$. Comme l'élément X n'est pas un soliton, il contient un terme a avec $0 < a < b$. Comme il est de norme minimale, il contient un terme nul (sinon, on a $\|F(X)\| < \|X\|$ en vertu de 2.11). Parmi les termes nuls, on distingue ceux qui sont **liés**[3] c'est-à-dire tels qu'il existe un terme b avec uniquement des 0 entre[4] ce b et le zéro considéré. Soit $r(X)$ la somme du nombre de termes $b = \|X\|$ et du nombre de zéros liés. On va montrer le lemme suivant :

3.3 Lemme. *Dans la situation précédente, si X n'est pas un soliton, on a $r(F(X)) < r(X)$.*

Admettons un instant ce lemme. On prend alors, parmi les contre-exemples au théorème, un contre-exemple de norme minimale et parmi ceux-ci un X tel que $r(X)$ soit minimal. Alors, le lemme montre que c'est un soliton, ce qui est absurde.

Il reste à prouver le lemme. On a $\|F(X)\| = \|X\| = b$ et on écrit X comme réunion disjointe $X = Y \cup Z$ où Y, dite partie liée, est formée des termes $b = \|X\|$ et des zéros liés et Z, dite partie libre, des autres. Le cardinal de Y est $r(X)$. On applique F en posant $F(X) = X'$ et en écrivant $X' = Y' \cup Z'$ comme réunion de ses parties liée et libre et on cherche $r(X')$ qui est le cardinal de Y'.

Le point crucial est le suivant :

3.4 Lemme. *Soient x_i, x_{i+1} deux termes successifs de X. Si $|x_i - x_{i+1}|$ est dans Y', x_i et x_{i+1} sont tous deux dans Y.*

Démonstration. (de 3.4) On note d'abord que les seuls couples (x_i, x_{i+1}) qui donnent b dans X' sont les couples $(0, b)$ ou $(b, 0)$ dont les deux termes sont bien contenus dans Y.

On note ensuite que les couples (x_i, x_{i+1}) qui donnent 0 sont des couples (a, a). Si a est égal à b ou si c'est un zéro lié, on a gagné, et, sinon, il y a deux cas :

• Si on a $0 < a < b$, le zéro obtenu n'est pas lié. En effet, on englobe le couple (a, a) dans une suite de a maximale : $c, a, a, \ldots, a, d$, avec $c, d \neq a$ et par F on obtient $|c - a|, 0, \ldots, 0, |d - a|$ et comme $|c - a|$ et $|d - a|$ ne sont ni nuls (car $c, d \neq a$), ni égaux à b (car on a $c, d \leq b$ et $0 < a < b$), les zéros intermédiaires ne sont pas liés.

3. Sous-entendu aux b.

4. On prend cette notion modulo n, bien entendu.

• Si a est un zéro libre, on écrit une suite maximale de 0 englobant $(0,0)$: $c, 0, \ldots, 0, d$ avec c, d non nuls et $< b$. Alors, par F, on obtient $c, 0, \ldots, 0, d$ avec un 0 de moins et le zéro considéré n'est pas lié.

Revenons à 3.3. On considère un ensemble lié maximal $y_1, \ldots, y_r$ de $Y = F(X)$ et ses voisins immédiats : $u, y_1, \ldots, y_r, v$ où les y_i sont des b ou des 0 liés, mais pas u ni v. On peut écrire $u = |x_1 - x_0|$, $y_1 = |x_2 - x_1|$, ..., $y_i = |x_{i+1} - x_i|$, ..., $y_r = |x_{r+1} - x_r|$ et $v = |x_{r+2} - x_{r+1}|$ avec $x_i \in X$. Le lemme 3.4 montre que $x_1, \ldots, x_{i+1}$ sont dans Y, mais comme u, v ne sont pas dans Y', x_0 et x_{r+2} ne sont pas dans Y. On voit que tout sous-ensemble lié maximal de X' provient d'un sous-ensemble lié maximal de X comportant un élément de plus, ce qui montre que le nombre des éléments de Y' a décru par rapport à celui de Y.

Cela établit le théorème.

3.5 *Remarque.* Le lecteur qui trouverait la preuve précédente compliquée regardera les exemples suivants : $(b, b, 0)$, $(0, b, b, b, b)$, $(0, a, a, b)$, $(0, a, b)$ pour infirmer les conjectures hasardeuses suivantes : par F le nombre de b diminue, le nombre de 0 diminue, l'un ou l'autre diminue, les valeurs des termes diminuent, etc.

3.2 Conséquences

Pour étudier les $F^N(X)$ on est ramené au cas des solitons et même, vu la remarque 2.1.1 qui permet de diviser par a, aux solitons de $\{0,1\}^n$. Le point crucial est alors le suivant :

3.6 Lemme. *L'application F_n induit une application, notée encore F_n : $\{0,1\}^n \to \{0,1\}^n$. Soit $\theta_n : \{0,1\}^n \to (\mathbf{Z}/2\mathbf{Z})^n$ la bijection canonique. Alors, l'application $G_n = \theta_n F_n \theta_n^{-1} : (\mathbf{Z}/2\mathbf{Z})^n \to (\mathbf{Z}/2\mathbf{Z})^n$ est une application linéaire, donnée par la formule :*

$$G_n(x_1, \ldots, x_n) = (x_1 + x_2, x_2 + x_3, \ldots, x_{n-1} + x_n, x_n + x_1).$$

La matrice de G_n dans la base canonique de $(\mathbf{Z}/2\mathbf{Z})^n$ est :

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

Lorsque l'entier n sera bien identifié, on notera simplement G au lieu de G_n.

Démonstration. En effet, pour des x_i de $\{0,1\}$, on voit [5] que $|x_i - x_{i+1}|$ est égal au relevé canonique de $x_i + x_{i+1}$ modulo 2 par θ_n. (Modulo 2, signes et valeurs absolues disparaissent.)

3.7 *Commentaire.* On voit que l'étude des itérées de F, modulo le lemme des solitons et le lemme précédent, est essentiellement ramenée à l'étude de l'application linéaire [6] G et de ses itérées.

4 L'étude de l'application linéaire G

On pose $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$, $E = \mathbf{F}_2^n$ et on note $\overline{\mathbf{F}_2}$ une clôture algébrique de $\mathbf{F}_2$. On se souviendra qu'en caractéristique 2, l'élévation au carré est un homomorphisme (dit de Frobenius), c'est-à-dire qu'on a $(x+y)^2 = x^2 + y^2$.

4.1 Proposition. *On note γ la permutation circulaire $\gamma = (1, 2, \ldots, n)$ et Γ l'endomorphisme de E associé défini par $\Gamma(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, x_1)$, ou encore par $\Gamma(e_1) = e_n$ et $\Gamma(e_i) = e_{i-1}$ pour $i \geq 2$.*

1) On a $G = \Gamma + \mathrm{Id}$.

2) Le polynôme caractéristique $\chi_G(T)$ de l'application linéaire G est égal à $(T+1)^n + 1$. Ses racines dans $\overline{\mathbf{F}_2}$ sont les $\zeta + 1$ où les ζ sont les racines n-ièmes de l'unité dans $\overline{\mathbf{F}_2}$, comptées avec leurs multiplicités.

3) Le noyau de G est la droite $\{0, \underline{1}\}$, l'image de G est l'hyperplan défini par $\sum_{i=1}^n x_i = 0$.

Démonstration. Le point 1) est évident sur la formule donnant G. On en déduit le point 2). En effet, on a $\chi_G(T) = \det(G+T\mathrm{Id}) = \det(\Gamma+(1+T)\mathrm{Id}) = (1+T)^n+1$ (on peut aussi calculer le déterminant en développant par rapport à la première colonne). Si x en est une racine, on a $(1+x)^n = 1$, de sorte que $1 + x = \zeta$ est une racine n-ième de 1 et on a $x = 1 + \zeta$. Enfin, le point 3) est immédiat.

4.2 *Remarque.* Cette proposition ramène, pour l'essentiel, l'étude de χ_G à celle de $T^n + 1$. En effet, l'application $P(T) \mapsto P(T+1)$ est un isomorphisme involutif de l'anneau des polynômes qui transforme polynômes irréductibles en polynômes irréductibles. Si $Q_1, \ldots, Q_r$ sont les facteurs irréductibles de $T^n + 1$, ceux de χ_G sont les $Q_i(T+1)$.

4.3 *Remarque.* Le groupe cyclique $<\Gamma>$ engendré par Γ opère sur E. L'écriture $G = \Gamma + \mathrm{Id}$ montre que G et Γ commutent, ce qui implique que les orbites de E sous $<\Gamma>$ sont permutées par G.

5. Le plus simple est de distinguer les quatre cas : $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$.
6. Quel bonheur !

4.1 Factorisation de $T^n + 1$ sur $\mathbf{F}_2$

Posons $n = 2^\alpha m$ avec $\alpha \geq 0$ et m impair. L'homomorphisme de Frobenius montre qu'on a $T^n+1 = (T^m+1)^{2^\alpha}$ et on sait que, sur $\mathbf{F}_2$, T^m+1 est le produit des polynômes cyclotomiques : $T^m + 1 = \prod_{d|m} \Phi_d(T)$ où Φ_d est le polynôme unitaire dont les zéros (simples) sont les racines d-ièmes primitives de l'unité. On sait que Φ_d est la réduction modulo 2 du polynôme cyclotomique sur $\mathbf{Z}$, qui est à coefficients entiers et de degré $\varphi(d)$ (l'indicatrice d'Euler). On a en particulier $\Phi_1(T) = T + 1$ et $T + 1$ ne divise aucun autre Φ_d.

Attention, le polynôme Φ_d est irréductible sur $\mathbf{Z}$, mais pas nécessairement sur $\mathbf{F}_2$. On sait même (c'est une conséquence de [1] III 4.14), qu'il ne peut être irréductible que si $d = 1$ ou q^β où q est un nombre premier impair. De plus, même pour ces entiers, Φ_d n'est pas nécessairement irréductible sur $\mathbf{F}_2$. Précisément, on a le résultat suivant :

4.4 Lemme. *Soit d un entier impair. Les facteurs irréductibles de Φ_d sur $\mathbf{F}_2$ sont simples, ils ont tous même degré $r(d)$ et cet entier est l'ordre de 2 dans $(\mathbf{Z}/d\mathbf{Z})^*$. Il y a $\varphi(d)/r(d)$ tels facteurs.*

Démonstration. Les facteurs de Φ_d sont à l'ordre 1 car $T^d + 1$ n'a pas de racines multiples (sa dérivée dT^{d-1} n'a que la racine 0). Soit Q un facteur irréductible de degré r et soit $K = \mathbf{F}_{2^r}$ un corps de rupture de Q. Comme les racines de Q sont primitives d-ièmes de 1, K est le corps de décomposition de $X^d - 1$ et cela vaut pour tous les facteurs, qui ont donc même degré. Les racines de Q sont dans K^* qui est un groupe fini de cardinal $2^r - 1$, ce qui montre que d divise $2^r - 1$, ou encore qu'on a $2^r \equiv 1 \pmod{d}$. Inversement, si d divise $2^s - 1$, comme le groupe multiplicatif de $\mathbf{F}_{2^s}$ est cyclique, il contient les racines d-ièmes de l'unité, donc $\mathbf{F}_{2^r}$, de sorte qu'on a $r \leq s$ et r est bien l'ordre de 2 dans $(\mathbf{Z}/d\mathbf{Z})^*$.

4.5 *Exemples.* Voici quelques exemples de décompositions en facteurs irréductibles des polynômes cyclotomiques sur $\mathbf{F}_2$: $\Phi_3(T) = T^2 + T + 1$, $\Phi_5(T) = T^4 + T^3 + T^2 + T + 1$, $\Phi_7(T) = T^6 + T^5 + T^4 + T^3 + T^2 + T + 1 = (T^3+T^2+1)(T^3+T+1)$, $\Phi_9(T) = T^6+T^3+1$, $\Phi_{11}(T) = T^{10}+T^9+\cdots+T+1$, $\Phi_{13}(T) = T^{12} + \cdots + T + 1$, $\Phi_{15}(T) = T^8 + T^7 + T^5 + T^4 + T^3 + T + 1 = (T^4 + T^3 + 1)(T^4 + T + 1)$ et enfin $\Phi_{17}(T) = T^{16} + \cdots + T + 1 = (T^8 + T^7 + T^6 + T^4 + T^2 + T + 1)(T^8 + T^5 + T^4 + T^3 + 1)$.

4.6 Notations. On pose $\Phi_d(T) = \prod_{i=1}^{\varphi(d)/r(d)} \Phi_{d,i}(T)$ où les $\Phi_{d,i}$ sont les facteurs irréductibles de Φ_d (tous de degré $r(d)$). On les appelle **facteurs cycloto-**

miques. Pour d fixé, on ordonne les polynômes $\Phi_{d,i}$ par ordre lexicographique inverse des degrés des monômes. Par exemple, pour $d = 7$, on pose $\Phi_{7,1}(T) = T^3 + T^2 + 1 \prec \Phi_{7,2}(T) = T^3 + T + 1$.

4.7 Corollaire. *Soit $n = 2^\alpha m$ avec m impair. Le polynôme χ_G est produit des polynômes $(\Psi_d(T))^{2^\alpha} := (\Phi_d(T+1))^{2^\alpha}$ pour d diviseur de m. Les polynômes Ψ_d seront appelés* **polynômes pseudo-cyclotomiques**. *On pose $\Psi_{d,i}(T) = \Phi_{d,i}(T+1)$ où les $\Phi_{d,i}$ sont les facteurs irréductibles des polynômes cyclotomiques. Ces polynômes sont irréductibles et le polynôme χ_G est le produit des $(\Psi_{d,i}(T))^{2^\alpha}$. Tous les $\Psi_{d,i}(T)$ relatifs à un même d sont de degré $r(d)$ qui est l'ordre de 2 dans $(\mathbf{Z}/d\mathbf{Z})^*$ et il y en a $\varphi(d)/r(d)$. On les appelle* **facteurs pseudo-cyclotomiques.**

4.8 *Remarque.* Comme on a $\Phi_1(T) = T + 1$, on en déduit $\Psi_1(T) = T$ et le polynôme χ_G contient donc le facteur T^{2^α}, mais T ne divise aucun autre $\Psi_d(T)$.

4.2 Le cas où n est une puissance de 2 : premier cas de 1.1

La remarque précédente donne aussitôt :

4.9 Lemme. *On a $(T+1)^n + 1 = T^n$ modulo 2 si et seulement si n est une puissance de 2.*

Démonstration. En effet [7], si n a un facteur impair $m > 1$, les polynômes pseudo-cyclotomiques Ψ_d pour d diviseur de m ne sont pas multiples de T.

4.10 Corollaire. *L'application G est nilpotente si et seulement si n est une puissance de 2 et on a alors précisément $G^n = 0$.*

Démonstration. Une application linéaire est nilpotente si et seulement si elle n'a que la valeur propre 0, donc si son polynôme caractéristique est T^n.

On peut maintenant traiter le point 1) de 1.1.

4.11 Corollaire. *1) On a le premier point de 1.1 : si n est une puissance de 2, pour tout $X \in \mathbf{Q}^n$ il existe N tel que $F^N(X) = 0$.*

2) Inversement, si n n'est pas une puissance de 2, il existe des $X \in \mathbf{N}^n$ tels que $F^N(X)$ soit non nul pour tout N.

7. On peut aussi faire le calcul directement en posant $Y = T^{2^\alpha}$.

Démonstration. 1) Notons qu'il suffit de montrer le résultat pour $X \in \mathbf{N}^n$. En effet, si X est dans $\mathbf{Q}^n$, il existe $m \in \mathbf{N}^*$ tel que $mX \in \mathbf{Z}^n$, donc tel que $\Phi(mX) = m\Phi(X)$ soit dans $\mathbf{N}^n$. On conclut alors avec 2.1.1.

Le lemme des solitons 3.2 montre qu'il existe N tel que $F^N(X)$ soit un soliton et on peut même supposer qu'il s'agit d'un 1-soliton. Les images de $F^N(X)$ par F et ses itérées sont alors les mêmes que celles de G et de ses itérées. Comme G est nilpotente, on a le résultat.

2) Le corollaire 4.10 montre le point 2) : il suffit de prendre un soliton qui n'est pas transformé en 0 par les puissances de G.

4.12 *Remarque.* L'application linéaire G est aussi la réduction modulo 2 de F. Comme on a $G^n = 0$, cela montre que, pour tout $X \in \mathbf{N}^n$, $F^n(X)$ est pair (c'est-à-dire que tous ses termes sont pairs.).

4.3 L'ubiquité des facteurs cyclotomiques

Le point crucial à noter est que les valeurs propres de G, qui sont de la forme $1 + \zeta$ avec $\zeta^n = 1$, sont elles-mêmes des racines de l'unité, comme d'ailleurs tous les éléments non nuls de $\overline{\mathbf{F}}_2$. Précisément, on a le lemme suivant :

4.13 Lemme. *Soit $P \in \mathbf{F}_2[T]$ un polynôme irréductible de degré p, distinct de T. Alors P est un facteur cyclotomique, autrement dit, il existe un unique entier $k = k(P)$ tel que P divise Φ_k (donc aussi $T^k + 1$) et il existe i tel que $P = \Phi_{k,i}$. Les racines de P sont des racines primitives k-ièmes de l'unité. L'entier $k(P)$ divise $2^p - 1$ et on le nomme* **exposant** *de P.*

Si α est un entier positif, P^{2^α} divise le polynôme $(T^k + 1)^{2^\alpha}$.

Démonstration. On considère un corps de rupture K de P, c'est une extension de degré p de $\mathbf{F}_2$, c'est donc $\mathbf{F}_{2^p}$. Comme cette extension est normale (c'est le corps de décomposition de $X^{2^p} - X$), toutes les racines de P sont dans ce corps, non nulles, et vérifient donc $x^{2^p-1} = 1$. Si k est l'ordre de x dans K^* on a $x^k = 1$ pour un entier k qui divise $2^p - 1$ et x est une racine primitive k-ième de l'unité, de sorte que P divise Φ_k, donc en est un des facteurs irréductibles $\Phi_{k,i}$.

4.14 *Exemples.* On peut notamment appliquer ce lemme aux polynômes $\Psi_{d,i}$ pour d impair. Pour faire ces calculs on utilise le logiciel *xcas*. On trouvera des détails sur les algorithmes utilisés en 5.9. Voici quelques résultats :

1) On a $\Psi_3(T) = \Phi_3(T + 1) = T^2 + T + 1 = \Phi_3(T)$.

2) On a $\Psi_5(T) = \Phi_5(T + 1) = T^4 + T^3 + 1 = \Phi_{15,1}(T)$.

3) On a $\Psi_{7,1}(T) = \Phi_{7,1}(T + 1) = T^3 + T + 1 = \Phi_{7,2}(T)$ et $\Psi_{7,2}(T) = T^3 + T^2 + 1 = \Phi_{7,1}(T)$.

4) Pour $d = 11$, Ψ_{11} est irréductible de degré 10 et le lemme montre qu'il divise $T^{1023} - 1$ car $1023 = 2^{10} - 1$, mais l'entier $k(\Psi_{11})$ n'est pas $1023 = 3 \times 11 \times 31$ mais $341 = 11 \times 31$.

5) Pour $d = 15$, on a deux polynômes à considérer : $\Psi_{15,1}(T) = T^4 + T^3 + T^2 + T + 1 = \Phi_5(T)$ et $\Psi_{15,2} = T^4 + T + 1 = \Phi_{15,2}$. Autrement dit, on a $k(\Psi_{15,1}) = 5$ mais $k(\Psi_{15,2}) = 15$. On voit que deux facteurs pseudo-cyclotomiques relatifs au même entier n peuvent avoir des exposants différents.

6) On note seulement les exposants des monômes pour alléger l'écriture. On a $\Psi_{17,1} = (8, 7, 5, 4, 3, 2, 0) = \Phi_{85,3}$ et $\Psi_{17,2} = (8, 5, 3, 2, 0) = \Phi_{255,14}$. Même remarque que ci-dessus.

4.4 Sur l'exposant des $\Psi_{n,i}$

L'expérience semble indiquer que l'exposant $k(\Psi_{n,i})$ est souvent multiple de n, souvent mais pas toujours. Par exemple pour $n = 15$, l'un des facteurs de Ψ_{15} a un exposant 5, voir paragraphe 5.7. On a cependant le résultat partiel suivant :

4.15 Proposition. *Soit p un nombre premier impair. On suppose que l'ordre $r(p)$ de 2 dans $(\mathbf{Z}/p\mathbf{Z})^*$ est pair. Alors, tous les exposants $k(\Psi_{p,i})$ sont multiples de p.*

Démonstration. Supposons $r := r(p)$ pair, $r = 2s$. On a alors $2^r - 1 = (2^s + 1)(2^s - 1)$. Comme r est l'ordre de 2 modulo p, p ne divise pas $2^s - 1$, et comme p est premier, il divise $2^s + 1$, $2^s + 1 = p^e m$ où p ne divise pas m.

Les racines de $\Psi_{p,i}$ sont les $1+\zeta$ où ζ est une racine de $\Phi_{p,i}$, donc une racine primitive p-ième de 1. On calcule $(1+\zeta)^{2^s} = 1+\zeta^{2^s}$. Comme on a $2^s = -1+\lambda p$, on a $\zeta^{2^s} = \zeta^{-1}$. On en déduit $(1 + \zeta)^{2^s-1} = (1 + \zeta^{-1})/(1 + \zeta) = \zeta^{-1}$.

Soit k l'exposant de $\Psi_{p,i}$, c'est-à-dire le plus petit entier tel que $(1+\zeta)^k = 1$. Comme k divise $2^r - 1 = (2^s - 1)p^e m$, si k n'est pas multiple de p, c'est qu'il divise $(2^s - 1)m$ et on a donc $(1 + \zeta)^{m(2^s-1)} = 1$. Mais ce nombre est égal à ζ^{-m} et comme m n'est pas multiple de p, c'est impossible.

4.16 *Remarques.* 1) Attention, $r(p)$ n'est pas toujours pair. On a, par exemple, $r(7) = 3$, $r(23) = 11$, $r(31) = 5$, etc. Cette condition n'est pas nécessaire pour que $k(n)$ soit multiple de n. Par exemple, pour $n = 23$, on vérifie que l'exposant est $2^{11} - 1 = 2047 = 23 \times 89$ et non pas 89. Pour $n = 47$, on a $r = 23$ et $2^{23} - 1 = 47 \times 178481$. Là encore on vérifie que $1 + \zeta$ n'est pas d'ordre 178481 (en écrivant ce nombre en base 2). J'ignore si le résultat de 4.15 est valable pour tous les nombres premiers impairs.

2) Il est possible que l'exposant e introduit dans la preuve ci-dessus soit > 1, c'est-à-dire que, si r est l'ordre de 2 modulo p, $2^r - 1$ soit multiple de p^2. Possible, mais rarissime : les nombres vérifiant cette propriété sont tels que $2^{p-1} - 1$ soit multiple de p^2 (nombres de Wieferich, 1909). On n'en connaît que deux : $p = 1093$, avec $r = 364$ (1093^2 divise $2^{364} - 1$) et $p = 3511$ avec $r = 1755$ et il n'y en a pas d'autre pour $p < 10^{17}$. Ces nombres sont liés au grand théorème de Fermat : si un nombre p est tel que $x^p + y^p = z^p$ sans que p divise xyz c'est un nombre de Wieferich.

4.5 Décomposition de E en sous-espaces caractéristiques

On suppose que n n'est pas une puissance de 2 et on écrit $n = 2^\alpha m$ avec m impair, $m > 1$. Le corollaire 4.7 fournit la décomposition du polynôme $\chi_G(T) = (T+1)^n + 1$ en produit de polynômes primaires (i.e. puissances d'irréductibles) : $\chi_G(T) = T^{2^\alpha} \times \prod_{d|m, d>1} \prod_{i=1}^{\varphi(d)/r(d)} (\Psi_{d,i}(T))^{2^\alpha}$. On pose $V = \mathrm{Ker}\,(G^{2^\alpha})$ et $W_{d,i} = \mathrm{Ker}\,((\Psi_{d,i}(G))^{2^\alpha})$. On notera qu'on a, par Frobenius, $(\Psi_{d,i}(T))^{2^\alpha} = \Psi_{d,i}(T^{2^\alpha})$. Ces sous-espaces sont les sous-espaces caractéristiques de G et on sait qu'on a la décomposition en somme directe $E = V \oplus (\bigoplus_{d,i} W_{d,i})$. Les sous-espaces $W_{d,i}$ sont stables par G et on a le résultat suivant :

4.17 Proposition. *Soit $x \in E$. On a l'alternative suivante :*

1) Si $x \in V$ on a $G^{2^\alpha}(x) = 0$.

2) Si x est dans $W_{d,i}$ on a $G^{2^\alpha k(\Psi_{d,i})}(x) = x$ et donc aussi $G^{2^\alpha (k(\Psi_{d,i})+1)}(x) = G^{2^\alpha}(x)$.

3) Si x n'est ni dans V ni dans un $W_{d,i}$ on a $G^{2^\alpha (K+1)}(x) = G^{2^\alpha}(x)$ où K est le ppcm des $k(\Psi_{d,i})$.

Démonstration. Posons $H = G^{2^\alpha}$. On écrit $x = x_0 + \sum_{d,i} x_{d,i}$ avec $x_0 \in V$ et $x_{d,i} \in W_{d,i}$. Le premier cas correspond à $x = x_0$ et on a bien $H(x) = 0$. Si x est dans $W_{d,i}$, on a $\Psi_{d,i}(H)(x) = 0$. Mais, on a vu que $\Psi_{d,i}(T)$ divise $T^{k(\Psi_{d,i})} - 1$, de sorte que x vérifie $H^{k(\Psi_{d,i})}(x) = G^{2^\alpha k(\Psi_{d,i})}(x) = x$.

Dans le cas général, comme $G^{2^\alpha}(x_0)$ est nul, $G^{2^\alpha}(x)$ est dans la somme directe des $W_{d,i}$ et, si K est le *ppcm* des $k(\Psi_{d,i})$ on a $G^{2^\alpha K}(G^{2^\alpha}(x)) = G^{2^\alpha}(x)$ par le cas précédent, d'où le résultat.

4.6 Fin de la preuve de 1.1

On pose $n = 2^\alpha m$ avec m impair et $m > 1$. Soit $X \in \mathbf{Q}^n$. Comme dans la preuve de 4.11 on peut supposer que X est dans $\mathbf{N}^n$. Le lemme des solitons

3.2 montre alors qu'il existe N tel que $F^N(X)$ soit dans $\{0,a\}^n$ et on peut supposer $a=1$ en utilisant 2.1.1. On est ainsi ramené au cas où X est dans $\{0,1\}^n$. L'application F est alors égale à G et on peut décomposer X sur les sous-espaces caractéristiques. En vertu de 4.17, il y a deux possibilités :

- Soit $G^{2^\alpha}(X)=0$.
- Soit il existe un entier M tel que $G^{2^\alpha M}(X)=G^{2^\alpha}(X)$.

Cela achève de prouver 1.1.

5 Exemples

Voici quelques exemples des comportements des itérées de F pour n petit.

5.1 Le cas $n=2$

Ce cas est trivial, y compris sur $\mathbf{R}$: on a $F(a,b)=(|a-b|,|a-b|)$ et $F^2(X)=0$ pour tout $X=(a,b)\in\mathbf{R}^2$.

5.2 Le cas des puissances de 2

Pour $n=2^\alpha$, on a vu que, pour tout $X\in\mathbf{Q}^n$, il existe N tel que $F^N(X)=0$, mais, attention, pour $n\neq 2$, il n'existe pas de N universel, voir §7.1.

5.3 Le cas $n=3$

5.1 Proposition. *On suppose $n=3$. Le comportement des $X=(a,b,c)\in\mathbf{N}^3$ est le suivant.*

1) Si $X=(a,a,a)$ on a $F^N(X)=0$ pour tout $N\geq 1$.

2) Les éléments $(a,a,0)$, $(0,a,a)$, $(a,0,a)$ avec $a\neq 0$, forment un cycle d'ordre 3 sous l'action de F. Si a,b,c ne sont pas tous égaux, il existe N tel que $F^N(X)$ soit un élément d'un tel cycle.

Démonstration. Soit $X\in\mathbf{N}^3$. Le lemme des solitons montre qu'il existe N tel que $F^N(X)$ soit un a-soliton et on peut même supposer $a=1$. On est ramené à travailler dans $\mathbf{F}_2^3$. Le polynôme caractéristique de G est $T(T^2+T+1)$. Le noyau V de G est formé de 0 et $(1,1,1)$. Il y a un unique sous-espace W qui est le noyau de $G^2+G+\mathrm{Id}$, ou encore l'image de G. Il est formé des vecteurs $(1,1,0)$, $(0,1,0)$ et $(0,1,1)$ qui forment un cycle d'ordre 3. Les autres vecteurs de $\mathbf{F}_2^3$ sont les vecteurs de base $(1,0,0)$, $(0,1,0)$ et $(0,0,1)$ dont les images sont dans W. On a vu en 2.7 que (a,a,a) n'est pas dans l'image de F, de sorte qu'un (a,b,c) distinct de (a,a,a) tombe nécessairement sur un cycle.

5.2 *Remarque.* Le N de la proposition peut être arbitrairement grand. Voici un moyen de construire des exemples. On note u_n le n-ième terme de la suite de Fibonacci : $u_{n+2} = u_{n+1} + u_n$ avec $u_0 = u_1 = 1$. On se donne a, b entiers et l'on pose $X_n(a,b) = (u_n\,a + u_{n+1}\,b, u_{n+1}\,a + u_{n+2}\,b, u_{n+2}\,a + u_{n+3}\,b)$. Alors, on a $F(X_n(a,b)) = X_{n-1}(a,b)$. Avec $a = 0$ et $b = 1$, on voit que $F^n(u_{n-1}, u_n, u_{n+1}) = (0,1,1)$.

5.4 Un cas relativement simple : n premier impair et Φ_n irréductible modulo 2

5.4.1 Généralités

On a vu que ce cas se produit si et seulement si 2 est d'ordre $n-1$ dans $(\mathbf{Z}/n\mathbf{Z})^*$, donc pour $n = 3, 5, 11, 13, 19, 29, 37, 53, 59, \ldots$ La proposition suivante est alors conséquence de 1.1 :

5.3 Proposition. *On suppose que n est premier impair et que 2 est d'ordre $n-1$ dans $(\mathbf{Z}/n\mathbf{Z})^*$. Le polynôme $\Psi_n(T) = \Phi_n(T+1)$ est irréductible. On note $k = k(n)$ l'entier $k(\Psi_n)$ tel que Ψ_n divise Φ_k (donc $X^k + 1$). Cet entier est multiple de n en vertu de 4.15 et divise $2^{n-1}-1$. On pose $2^{n-1}-1 = k(n)d(n)$. Alors, les $X \in \{0,a\}^n$ distincts de 0 et comprenant un nombre pair de termes a forment $d(n)$ cycles $C_i(a)$ d'ordre $k(n)$ sous l'action de F et on a les deux cas suivants pour $X \in \mathbf{N}^n$:*

1) Si $X = \underline{a}$ on a $F(X) = 0$.

2) Sinon, il existe N et a tels que $F^N(X)$ soit dans l'un des $d(n)$ cycles $C_i(a)$.

Voici les premières valeurs de $k(n)$: $k(3) = 3$, $k(5) = 15$, $k(11) = 341$, $k(13) = 819$, ...

5.4.2 L'exemple $n = 5$

Dans ce cas, on a $k(5) = 15 = 2^4 - 1$, donc $d(5) = 1$. On peut se contenter d'examiner G sur $\mathbf{F}_2^5$, qui est de cardinal 32. Outre le vecteur nul et l'élément $\underline{1}$ qui donne 0 par application de G, il reste 30 éléments. Les 15 éléments $(x_1, \ldots, x_5)$ non nuls pour lesquels la somme $\sum_i x_i$ est nulle[8] forment un unique cycle d'ordre 15. Les 15 autres tombent dans ce cycle par application de G.

On peut préciser que $W - \{0\}$ est découpé en trois orbites sous l'action des permutations circulaires : les cinq éléments du type $(1,1,0,0,0)$ avec

8. Ici, le sous-espace $\sum_i x_i = 0$ est à la fois l'espace W et l'image de G.

deux 1 collés, les cinq du type $(1,0,1,0,0)$ avec deux 1 séparés et les cinq comprenant quatre 1 : $(1,1,1,1,0)$. Ces orbites sont permutées par G (voir 4.3) et les orbites des éléments "impairs" s'envoient respectivement sur celles-ci, les cinq éléments du type $(1,0,0,0,0)$ sur le premier type, les cinq du type $(1,1,1,0,0)$ sur le second et les cinq $(1,1,0,1,0)$ sur le troisième.

5.5 Les cas n premier impair et Φ_n réductible

5.5.1 Le cas $n = 7$

Là encore, on se limite à l'étude sur $\mathbf{F}_2^7$. Dans ce cas, le polynôme cyclotomique Φ_7 est réductible avec deux facteurs de même degré et on en déduit que c'est aussi le cas de Ψ_7 : $\Psi_7(T) = (T^3+T+1)(T^3+T^2+1) = \Psi_{7,1}(T)\Psi_{7,2}(T)$. L'espace V est toujours formé de 0 et de $\underline{1}$. Les deux sous-espaces $W_{7,i}$ sont de dimension 3 (donc ont 7 éléments en plus de 0), l'image I de G est formée des éléments de somme paire (63 éléments non nuls) et les éléments qui ne sont pas dans l'image tombent dedans dès qu'on applique G. On va décrire en détail l'image I qui est formée de 9 cycles d'ordre 7 sous l'action de G.

Tout d'abord, pour trouver les $W_{7,i}$, on note que $\operatorname{Ker}\Psi_{7,i}$ est aussi l'image de $G \circ \Psi_{7,j}(G)$ avec $i \neq j$ et que les $W_{7,i}$ sont stables par G. On part d'un vecteur arbitraire, par exemple $e_1 := (1,0,0,0,0,0,0)$ et on applique $G \circ \Psi_{7,1}(G) = G^4 + G^2 + G$. On obtient $\epsilon_1 := (1,0,0,1,0,1,1)$ qui est dans $W_{7,2}$ et les autres vecteurs de cet espace forment avec lui un 7-cycle sous l'action de G. De même, avec $G^4 + G^3 + G$ on obtient $\epsilon'_1 := (1,0,0,1,1,1,0)$ dont les transformés par G remplissent $W_{7,1}$. Comme $G = \Gamma + \mathrm{Id}$, la permutation circulaire Γ commute à G et les sous-espaces W_i sont stables par Γ. Ainsi, $W_{7,2}$ a pour base ϵ_1, $\epsilon_2 := (1,0,1,1,1,0,0)$ et $\epsilon_3 := (1,1,0,0,1,0,1)$ et l'action de G sur $W_{7,2}$ est la suivante : $\epsilon_1 \mapsto \epsilon_2 \mapsto \epsilon_3 \mapsto \epsilon_1+\epsilon_3 \mapsto \epsilon_1+\epsilon_2+\epsilon_3 \mapsto \epsilon_1+\epsilon_2 \mapsto \epsilon_2+\epsilon_3 \mapsto \epsilon_1$, tandis que celle de Γ est donnée par $\epsilon_1 \mapsto \epsilon_1+\epsilon_2 \mapsto \epsilon_1+\epsilon_3 \mapsto \epsilon_2 \mapsto \epsilon_2+\epsilon_3 \mapsto \epsilon_1+\epsilon_2+\epsilon_3 \mapsto \epsilon_3 \mapsto \epsilon_1$.

On peut alors achever la description de l'image I. Elle est formée de 9 orbites sous l'action de G, les W_i et 7 autres obtenues en prenant des combinaisons linéaires des vecteurs des W_i. Si l'on note ϵ'_1, $\epsilon'_2 = (1,0,1,0,0,1,1)$ et $\epsilon'_3 = (1,1,1,0,1,0,0)$ une base de $W_{7,1}$, on peut par exemple calculer l'orbite de $u_1 = \epsilon_2 + \epsilon'_1 + \epsilon'_2 = (1,0,0,0,0,0,1)$ qui contient $\epsilon_3 + \epsilon'_2 + \epsilon'_3$, $\epsilon_1+\epsilon_3+\epsilon'_1+\epsilon'_2+\epsilon'_3$, $\epsilon_1+\epsilon_2+\epsilon_3+\epsilon'_1+\epsilon'_3$, $\epsilon_1+\epsilon_2+\epsilon'_1$, $\epsilon_2+\epsilon_3+\epsilon'_2$ et $\epsilon_1+\epsilon'_3$. Il y a deux différences entre ces orbites et les $W_{7,i}$:

1) Ce ne sont pas des sous-espaces vectoriels.

2) Elles sont stables par G mais pas par la permutation circulaire Γ qui permute les 7 orbites en question.

5.5.2 Le cas $n = 17$

Ce cas est particulièrement intéressant. D'abord, le polynôme cyclotomique $\Phi_{17}(T) = T^{16} + T^{15} + \cdots + T + 1$ est réductible, on a :

$$\Phi_{17}(T) = \Phi_{17,1}(T)\Phi_{17,2}(T) := (X^8+X^7+X^6+X^4+X^2+X+1)(X^8+X^5+X^4+X^3+1).$$

On en déduit que $\Psi_{17}(T) = \Phi_{17}(T+1)$ l'est aussi, précisément :

$$\Psi_{17}(T) = \Psi_{17,1}(T)\Psi_{17,2}(T) := (T^8+T^7+T^5+T^4+T^3+T^2+1)(T^8+T^5+T^3+T^2+1).$$

Si ζ est une racine primitive 17-ième de l'unité et si on pose $\xi = \zeta + 1$, le corps engendré par ζ ou ξ est $\mathbf{F}_{2^8} = \mathbf{F}_{256}$, de sorte que ξ (qu'elle soit racine de $\Psi_{17,1}$ ou $\Psi_{17,2}$) vérifie $\xi^{255} = 1$. Mais, selon que ξ est racine de l'un ou l'autre polynôme Ψ, son ordre est différent (et c'est là tout l'intérêt de cet exemple). Précisément :

5.4 Théorème. *Si ξ est racine de $\Psi_{17,2}$ il vérifie $\xi^{255} = 1$ et pas moins, si ξ est racine de $\Psi_{17,1}$ il vérifie $\xi^{85} = 1$ et pas moins. (On rappelle qu'on a $255 = 3 \times 5 \times 17$ et $85 = 5 \times 17$).*

Démonstration. On calcule avec *xcas* les factorisations de $X^{15} + 1$, $X^{17} + 1$, $X^{51} + 1$ et $X^{85} + 1$. Seule cette dernière fait apparaître $\Psi_{17,1}$.

Il est facile de trouver des cycles d'ordre 255. On écrit la décomposition en sous-espaces caractéristiques $E = \mathbf{F}_2^{17} = V \oplus W_1 \oplus W_2$. Si l'on part d'un $x \in E$ écrit selon cette décomposition $x = v + w_1 + w_2$, on a $G(x) = G(w_1) + G(w_2)$ et, sauf si w_2 est nul, cet élément définit un cycle d'ordre 255. Si on prend les termes de manière aléatoire, on est la plupart du temps dans ce cas. Il est plus difficile de trouver un cycle d'ordre 85 (i.e. un élément de W_1). On cherche un tel élément dans $\operatorname{Ker} \Psi_{17,1}(G) = \operatorname{Im} G \circ \Psi_{17,2}(G)$. On part de $e_1 = (1, 0, \ldots, 0)$ et on applique $G \circ \Psi_{17,2}(G) = G^9 + G^6 + G^4 + G^3 + G$ en tenant compte des formules $G(e_1) = e_1 + e_{17}$ et $G(e_i) = e_i + e_{i-1}$ pour $i \geq 2$. Le calcul est facile mais un peu fastidieux et on trouve :

$$w_1 = (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1).$$

On vérifie qu'il donne bien un cycle d'ordre 85.

Pour l'application F sur $\mathbf{N}^{17}$, on a les possibilités suivantes :

• Si $X = \underline{a}$ on a $F(X) = 0$.

• Sinon, il existe N tel que $F^N(X)$ soit un soliton et engendre un cycle d'ordre 255 ou 85.

5.6 Le cas $n = 9$

On aborde maintenant les n impairs non premiers. Dans le cas de $n = 9$, on a $\chi_G(T) = T(T^2+T+1)(T^6+T^4+T^3+T+1) = T\Psi_3(T)\Psi_9(T)$. On sait que l'on a $k(\Psi_3) = 3$ et on vérifie que $k(\Psi_9)$ vaut 63. Il y a donc trois cas pour les éléments de $\mathbf{N}^9$: soit on tombe sur 0, soit on tombe dans un cycle d'ordre 3, soit dans un cycle d'ordre 63. Pour trouver un cycle d'ordre 3 on prend un X de $\mathrm{Ker}\,(G^2+G+\mathrm{Id}) = \mathrm{Im}\,(G^7+G^5+G^4+G^2+G) = \mathrm{Im}\,(\Gamma^7+\Gamma^6+\Gamma^4+\Gamma^3+\Gamma+\mathrm{Id})$. Avec e_1 on trouve $e_1+e_3+e_4+e_6+e_7+e_9 = (1,0,1,1,0,1,1,0,1)$.

5.7 Le cas $n = 15$

Ce cas fournit un exemple de cycle dont l'ordre n'est pas multiple de n. En effet, voir 4.14, on a $\Psi_{15,1}(T) = T^4+T^3+T^2+T+1 = \Phi_5(T)$, donc $k(\Psi_{15,1}) = 5$ et $\Psi_{15,2}(T) = T^4+T+1 = \Phi_{15,2}(T)$, donc $k(\Psi_{15,1}) = 15$. Comme dans le cas de $n = 17$, les cycles d'ordre 5 sont plus rares que ceux d'ordre 15. Pour trouver un cycle d'ordre 5, donc un élément du noyau de $G^4+G^3+G^2+G+\mathrm{Id}$, on prend un élément de l'image de $G(G^2+G+\mathrm{Id})(G^4+G^3+\mathrm{Id})(G^4+G+\mathrm{Id}) = G^{11}+G^6+G$. Avec $G = \Gamma+\mathrm{Id}$ on calcule $G^{11}+G^6+G = \Gamma^{11}+\Gamma^{10}+\Gamma^9+\Gamma^8+\Gamma^6+\Gamma^4+\Gamma^3+\mathrm{Id}$. On applique cet élément à e_1 et on obtient $e_1+e_{13}+e_{12}+e_{10}+e_8+e_7+e_6+e_5$ soit $(1,0,0,0,1,1,1,1,0,1,0,1,1,0,0)$. On vérifie qu'on obtient bien un cycle d'ordre 5.

5.8 Le cas $n = 6$

On a $\chi_G(T) = T^2(T^2+T+1)^2$, donc $E = V \oplus W$ avec $V = \mathrm{Ker}\,G^2$ et $W = \mathrm{Ker}\,((G^2+G+\mathrm{Id})^2) = \mathrm{Ker}\,(G^4+G^2+\mathrm{Id})$. Une base de V est donnée par les vecteurs $v_1 = (1,1,1,1,1,1)$ (dans $\mathrm{Ker}\,G$) et $v_2 = (1,0,1,0,1,0)$ et V contient en plus 0 et la somme v_1+v_2. Pour calculer une base de W, on écrit $G = \Gamma+\mathrm{Id}$ et W est le noyau de $\Gamma^4+\Gamma^2+\mathrm{Id}$, engendré par les quatre vecteurs :

$$(1,0,0,0,1,0), (0,1,0,0,0,1), (0,0,1,0,1,0), (0,0,0,1,0,1).$$

Le comportement de F est décrit par la proposition suivante :

5.5 Proposition. *Soit $X \in \mathbf{N}^6$. Il y a deux cas :*

1) Ou bien il existe N tel que $F^N(X) = 0$.

2) Ou bien il existe N tel que $F^N(X)$ est un soliton et que $F^{6+N}(X) = F^N(X)$.

5.6 *Remarque.* Les $X = (x_1, \ldots, x_6) \in \mathbf{N}^6$ tels que $F^N(X) = 0$ sont donnés par 2.10, ce sont 0, $\underline{a}$, les éléments $(0, a, 0, a, 0, a)$, $(0, a, 0, a, 2a, a)$, $(0, a, 2a, a, 0, a)$, $(0, a, 2a, a, 2a, a)$ et $(0, a, 2a, 3a, 2a, a)$, leurs images par permutation circulaire et les éléments obtenus à partir des précédents en leur ajoutant $\underline{b}$ avec $b \in \mathbf{N}$.

5.9 Résumé de l'algorithme de détermination des cycles

Il n'y a pas vraiment de résultat général sur la longueur des cycles, mais l'algorithme suivant permet de faire le calcul dans chaque cas (sous réserve de la puissance de l'ordinateur bien entendu).

On part d'un $n = 2^\alpha m$ avec m impair > 1. Les longueurs des cycles sont les $2^\alpha k$ où les k sont les longueurs des cycles relatifs à m. On décompose alors $(T+1)^m + 1$ sur $\mathbf{F}_2$ en facteurs cyclotomiques $\Psi_{d,i}$, de degré $r(d)$ dont il faut calculer les k. Pour cela, on sait que $k(\Psi_{d,i})$ est diviseur de $2^{r(d)} - 1$. On fait la liste de ces diviseurs k et on cherche l'unique k tel que $\Psi_{d,i}$ divise Φ_k. C'est le $k(d)$ cherché. Une autre possibilité, pour majorer $k(d)$ par un diviseur K de $2^{r(d)} - 1$, est de vérifier qu'on a $(1+\zeta)^K = 1$ pour tout ζ vérifiant $\zeta^d = 1$. Pour cela on peut calculer la puissance à la main en écrivant K en base 2, ou diviser $(X+1)^K + 1$ par $X^d + 1$. Les logiciels font ça très bien.

Pour avoir un cycle de longueur $k(\Psi_{d,i})$, on le cherche dans le noyau de $\Psi_{d,i}(G)$ ou encore dans l'image de $(\chi_G/\Psi_{d,i})(G)$.

5.7 *Exemple.* Outre son facteur T, le polynôme $(T+1)^{105} + 1$ est produit de $T^2 + T + 1$, de deux polynômes de degré 3, trois de degré 4, deux de degré 6 et six de degré 12. Pour les facteurs de degrés < 12, les valeurs de k sont, dans l'ordre, 3, 7, 7, 5, 15, 15, 63, 63. Voici la liste des facteurs de degré 12, donnés par les degrés de leurs monômes :

$$12,6,5,4,3,2,0 \quad 12,9,5,4,3,2,0 \quad 12,11,9,5,4,1,0 \quad 12,10,9,8,7,5,3,2,0$$

$$12,11,10,7,6,5,3,2,0 \quad \text{et} \quad 12,10,9,7,6,5,4,3,2,1,0.$$

Les valeurs de k sont toutes égales à $4095 = 2^{12} - 1$, sauf pour les deux dernières où elles valent 819. (On notera que, dans ce cas, l'exposant k n'est pas multiple de $n = 105$.)

5.8 *Remarque.* Pour calculer les sommes de puissances de G, il peut être commode d'écrire $G = \Gamma + \mathrm{Id}$, mais, pour calculer G^n, il est nécessaire de savoir quels sont les coefficients binomiaux $\binom{n}{p}$ qui sont impairs. Le lecteur vérifiera que, si n est écrit en base 2 avec des chiffres $\alpha_0, \alpha_1, \ldots, \alpha_k$, ce sont les p qui, toujours en base 2, ont des chiffres β_i avec $\beta_i \leq \alpha_i$. En particulier, les n qui sont tels que tous les $\binom{n}{p}$ soient impairs sont les $2^k - 1$.

6 Quelques programmes sur *xcas*

Les programmes suivants sont implantés dans le logiciel libre *xcas* que l'on peut télécharger à l'adresse suivante :

`https://www-fourier.ujf-grenoble.fr/~parisse/install_fr`

Le lecteur pourra les améliorer sans effort.

6.1 Calculer les itérées de F

On commence par programmer la permutation circulaire. L'entrée est une liste $l := (x_1, \ldots, x_n)$, la sortie la liste $(x_2, \ldots, x_n, x_1)$:

```
circ(l):={
local a,l1;
a:=l[0];
l1:=tail(l);
l:=append(l1,a);
retourne l;
}:;
```

On programme ensuite l'itération de l'application F. L'entrée est une liste $l := (x_1, \ldots, x_n)$ et un entier N et le programme affiche les $F^s(l)$ pour $s \leq N$:

```
beth(l,N):={
local s,n,l1;
n:=size(l);
pour s de 1 jusque N faire
Disp l;
l1:=circ(l);
l:=abs(l-l1);
fpour
}:;
```

Enfin, on calcule l'ordre des cycles (à supposer qu'il en existe et qu'ils soient de longueur moindre que 10000) :

```
ordre(l):={
local s,n,m,l1;
m:=l;
s:=size(l);
l1:=circ(l);
l:=abs(l-l1);
n:=1;
tantque l!=m et n<10^4 faire
l1:=circ(l);
```

```
l:=abs(l-l1);
n:=n+1;
ftantque
return n;
}:;
```

6.2 Les calculs modulo 2

La commande pour travailler modulo 2 est `%2`. Par exemple, `factor((x^17+1)%2)` renvoie la factorisation [9] de $x^{17}+1$ modulo 2.

Pour obtenir le polynôme cyclotomique Φ_n sur $\mathbf{F}_2$ il suffit de taper : `r2e(cyclotomic(n))%2`.

7 Compléments

7.1 F nilpotente ?

On a vu, dans le cas où n est une puissance de 2, que l'on a $F^n = 0$ en réduction modulo 2 et on en a déduit que, pour tout $X \in \mathbf{N}^n$, il existe N tel que $F^N(X) = 0$. En revanche, on va voir que, sauf pour $n = 2$ où l'on a $F^2 = 0$, il n'existe pas de N universel, au sens où l'on aurait $F^N(X) = 0$ pour tout $X \in \mathbf{N}^n$.

7.1 Définition. *Soit n une puissance de 2 et soit $X = (x_1, \ldots, x_n) \in \mathbf{N}^n$. On appelle* **ordre** *de X le plus petit N tel que $F^N(X) = 0$. On le note $\omega(X)$.*

7.2 Proposition. *Il existe des $X = (a, b, c, d)$ avec $0 < a < b < c$ et $d = a + b + c$ d'ordre arbitrairement grand.*

Démonstration. On part d'un X quelconque comme ci-dessus, d'ordre N, et on construit un Z, du même type et d'ordre $N + 1$.

Pour cela on pose $y_1 = 0$, $y_2 = a$, $y_3 = a + b$, $y_4 = a + b + c$ et $Y = (y_1, y_2, y_3, y_4)$. On a $F(Y) = X$. On pose ensuite $z_1 = y_4 - y_2 - y_3 = c - a > 0$, $z_2 = 2y_2 + z_1 = a + c$, $z_3 = 2y_3 + z_1 = a + 2b + c$, $z_4 = 2y_4 + z_1 = a + 2b + 3c$. Alors, $Z = (z_1, z_2, z_3, z_4)$ vérifie les conditions de la proposition et, comme $Z = 2Y + (z_1, z_1, z_1, z_1)$, on a $F(Z) = F(2Y) = 2F(Y) = 2X$, ce qui montre que Z est d'ordre $N + 1$.

9. Je suppose que cette factorisation se fait à l'aide des algorithmes classiques : Berlekamp ou Cantor-Zassenhaus.

7.3 *Exemple.* La proposition précédente permet de construire des exemples d'ordres arbitrairement grands. Par exemple, $X = (41792, 76864, 141376, 260032)$ est d'ordre 22.

7.4 *Remarque.* La construction utilisée dans la proposition s'appuie sur trois principes :

• Les éléments $X = (a, b, c, d)$ vérifiant $d = a + b + c$ sont dans l'image de F.

• On a $F(x_1, \ldots, x_n) = F(x_1 + u, \ldots, x_n + u)$, de sorte que X et $X + (u, \ldots, u)$ sont de même ordre.

• On a $F(\lambda X) = \lambda F(X)$, de sorte que X et λX sont de même ordre.

7.5 Corollaire. *Si $n \geq 4$ est une puissance de 2, il existe des $X \in \mathbf{N}^n$ d'ordres arbitrairement grands.*

Démonstration. Il suffit de mettre bout à bout des X de longueur 4. En effet, si $X = (x_1, \ldots, x_n)$ et si l'on pose $X \vee X = (x_1, \ldots, x_n, x_1, \ldots, x_n)$, on vérifie qu'on a $F(X \vee X) = F(X) \vee F(X)$.

7.2 Ordre et permutations

Soit $X = (x_1, \ldots, x_n)$ et soit $\sigma \in \mathfrak{S}_n$ une permutation. On pose $\sigma(X) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Attention, sauf si σ est une permutation circulaire, $F(\sigma(X))$ n'est pas en général une permutation de $F(X)$. Par exemple, avec $X = (1, 2, 3, 4)$ on a $F(X) = (1, 1, 1, 3)$, mais avec $Y = (1, 3, 2, 4)$ on a $F(Y) = (2, 1, 2, 3)$. Il n'y a donc aucune raison que les ordres de X et $\sigma(X)$ soient liés. D'ailleurs, le lemme suivant doit enlever les illusions de ce côté :

7.6 Lemme. *Soit $(a, b, c, d) \in (\mathbf{R}^+)^4$. On suppose que a, c sont grands et b, d petits i.e. $a \geq b, d$ et $c \geq b, d$. Alors, on a $F^4(X) = 0$.*

Démonstration. On a $F(X) = (a - b, c - b, c - d, a - d)$, d'où $F^2(X) = (|a - c|, |b - d|, |a - c|, |b - d|)$ et $F^4(X) = 0$ (voir 8.4 ci-dessous).

Comme on a vu ci-dessus qu'il y a des X d'ordres arbitrairement grands alors qu'ils ont toujours un permuté $\sigma(X)$ d'ordre ≤ 4, la différence d'ordre entre X et $\sigma(X)$ peut donc être arbitrairement grande aussi.

Par exemple, on a vu que $X = (41792, 76864, 141376, 260032)$ est d'ordre 22, mais $Y = (141376, 41792, 260032, 76864)$ est d'ordre 4. Sur $\mathbf{R}$, on peut même avoir des X d'ordre infini dont une permutation est d'ordre 4, voir la remarque 8.2 ci-dessous.

7.3 Majoration de l'ordre

On suppose toujours que n est une puissance de 2. La proposition suivante montre que l'ordre de X, même s'il peut être arbitrairement grand, n'est pas très grand par rapport à sa norme.

7.7 Proposition. *Soit $X \in \mathbf{N}^n$ un élément non nul. On a la formule :* $\omega(X) \leq n(1 + \dfrac{\ln(\|X\|)}{\ln 2})$.

Démonstration. On raisonne par l'absurde en prenant un contre-exemple X de norme minimale. On sait que $Y := F^n(X)$ est pair (voir 4.12), et il est non nul (sinon on a $\omega(X) \leq n$ et X n'est pas un contre-exemple), de sorte que $Y/2$ est encore entier et de norme strictement plus petite que X. Ce n'est donc plus un contre-exemple et on a $\omega(Y) = \omega(Y/2) \leq n(1 + \dfrac{\ln(\|\frac{Y}{2}\|)}{\ln 2}) = n(1+\dfrac{\ln(\|Y\|)}{\ln 2}-1) = n(\dfrac{\ln(\|Y\|)}{\ln 2})$. Mais on a $\omega(X) \leq \omega(Y)+n$ et $\|Y\| \leq \|X\|$, d'où $\omega(X) \leq n(1 + \dfrac{\ln(\|X\|)}{\ln 2})$, ce qui est absurde.

7.8 *Remarque.* Cette proposition montre que l'ordre n'est pas une fonction polynomiale de $(x_1, \ldots, x_n)$ (car elle est majorée par une fonction logarithmique).

7.9 Corollaire. *Soit $X \in \mathbf{Q}^{+n}$ et soit $q(X)$ le ppcm des dénominateurs des termes de X. On a* $\omega(X) \leq \dfrac{n}{\ln 2}(\ln 2 + \ln(q(X)) + \ln(\|X\|))$.

Démonstration. On pose $q = q(X)$ et $X = (\dfrac{p_1}{q_1}, \cdots, \dfrac{p_n}{q_n})$ et $q = r_i q_i$. On a $\omega(X) = \omega(qX)$ avec $qX \in \mathbf{N}^n$ et $\|qX\| = q\|X\|$ et on en déduit le résultat.

8 Le cas irrationnel

Une question naturelle consiste à se demander si le résultat obtenu dans le cas rationnel, lorsque n est une puissance de 2, est encore valable sur $\mathbf{R}$, avec un argument de densité. On montre ci-dessous qu'il n'en est rien (cela tient au fait qu'il n'y a pas de N universel vérifiant $F^N(X) = 0$). En revanche, on a un résultat asymptotique, bien naturel, mais pas aussi évident qu'on aurait pu le croire.

8.1 Un contre-exemple pour $n = 4$

8.1 Contre-exemple. *Il existe un quadruplet X de réels tel que, pour tout $N \in \mathbf{N}$, on ait $F^N(X) \neq 0$.*

Démonstration. On note que si $X = (a, b, c, d)$ avec $0 < a < b < c$ et $d = a + b + c$, on a $F(X) = (b - a, c - b, a + b, b + c) := (A, B, C, D)$ avec $D = A + B + C$. De plus, on a $0 < A < B < C$ pourvu que X vérifie $c - a < 2b < c + a$.

Considérons alors la matrice $M := \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ qui décrit l'action de F sur les trois premières coordonnées. Son polynôme caractéristique est $T^3 + 2T^2 - 2$ qui admet une unique racine réelle $\lambda \sim 0.839287$ avec le vecteur propre $(a, b, c) \sim (0.251359, 0.462321, 0.850340)$. On note qu'on a $0 < a < b < c$ et $c - a < 2b < c + a$.

Si maintenant on part de ce vecteur (a, b, c) et qu'on pose $X = (a, b, c, a + b + c)$, on a $F(X) = \lambda X$, puis $F^N(X) = \lambda^N X$. On voit que $F^N(X)$ n'est jamais nul.

8.2 *Remarques.* 1) Si l'on fait l'expérience avec des valeurs approchées décimales de X, on tombe évidemment sur 0 au bout d'un temps relativement bref.

2) Bien entendu, avec les mêmes chiffres, mais en les mettant dans l'ordre "grand, petit, grand, petit", on obtient un élément Y tel que $F^4(Y) = 0$, voir 7.6.

8.2 Le cas très croissant

Il y a pourtant de nombreux X réels dont l'image par un F^N est nulle. Outre le cas vu en 7.6, en voici un autre :

8.3 Proposition. *Soit $X = (a, b, c, d) \in \mathbf{R}^4$ un quadruplet avec $a \ll b \ll c \ll d$ où le signe $\ll$ signifie "beaucoup plus petit que" (en pratique, suffisamment pour que les différences considérées soient toujours positives, par exemple $b > a$, $c > 2b$ et $d > 3c$ conviennent). Alors, on a $F^6(X) = 0$.*

En effet, on calcule les itérées de $F(X)$:

$$F(X) = (b-a, c-b, d-c, d-a), \quad F^2(X) = (c-2b+a, d-2c+b, c-a, d-b),$$

$$F^3(X) = (d - 3c + 3b - a, d - 3c + b + a, d - c - b + a, d - c + b - a)$$

$$F^4(X) = (2b - 2a, 2c - 2b, 2b - 2a, 2c - 2b)$$

$$F^5(X) = (2c - 4b + 2a, 2c - 4b + 2a, 2c - 4b + 2a, 2c - 4b + 2a)$$

et donc $F^6(X) = 0$.

8.3 Un résultat asymptotique pour $n = 4$

On commence par un lemme qui rassemble quelques cas particuliers :

8.4 Lemme. *Soient a, b, c, d des réels.*
1) Si $X = (a, a, a, a)$ on a $F(X) = 0$.
2) Si $X = (a, b, a, b)$ on a $F^2(X) = 0$.
3) Si $X = (a, b, b, a)$ ou $X = (a, a, b, b)$ on a $F^3(X) = 0$.
4) Si $X = (0, a, b, 0)$ on a $F^6(X) = 0$.
5) Si $X = (0, b, c, d)$ avec $0 \leq c \leq d \leq b$ on a $F^4(X) = 0$.
6) Si $X = (0, a, a, b)$ avec $0 \leq b \leq a$ on a $F^6(X) = 0$.

Démonstration. Les points 1), 2), 3) sont évidents. Pour 4) on peut supposer, par exemple, $a \geq b$, et on a $F(X) = (a, a-b, b, 0)$ puis $F^2(X) = (b, |a - 2b|, b, a)$. Il y a deux cas.

• Si $a \geq 2b$, on a $F^2(X) = (b, a - 2b, b, a)$ et $F^3(X) = (|a - 3b|, |a - 3b|, a - b, a - b)$ et on est ramené à 3).

• Si $2b \geq a$, on a $F^2(X) = (b, 2b-a, b, a)$ et $F^3(X) = (a-b, a-b, a-b, a-b)$ et on est ramené à 1).

Pour 5) on a $F(X) = (b, b - c, d - c, d)$, d'où $F^2(X) = (c, b - d, c, b - d)$ et on est ramené au cas 2).

Pour 6), on a $F(X) = (a, 0, a-b, b)$ puis $F^2(X) = (a, a-b, |a-2b|, a-b)$. On distingue deux cas :

• $2b \leq a$. On a alors $F^2(X) = (a, a-b, a-2b, a-b)$ et $F^3(X) = (b, b, b, b)$. On est ramené au cas 1).

• $2b > a$. On a $F^2(X) = (a, a - b, 2b - a, a - b)$ et $F^3(X) = (b, |2a - 3b|, |2a - 3b|, b)$ et on est ramené à 3).

Le lemme suivant complète 2.11 :

8.5 Lemme. *Soit $X \in \mathbf{N}^4$ un élément non nul. Alors, on a $\|F^4(X)\| < \|X\|$.*

Démonstration. On rappelle (voir 2.11) que l'on a, pour tout X, $\|F(X)\| \leq \|X\|$ avec inégalité stricte sauf si un terme atteignant le maximum et un terme nul sont côte à côte. On peut donc supposer qu'on est dans ce cas et, quitte à faire une permutation circulaire, qu'on a $X = (0, b, c, d)$ avec $b \geq c, d$. On a alors $F(X) = (b, b - c, |c - d|, d)$.

Traitons d'abord quelques cas particuliers.

1) $c = b$. Dans ce cas on a $F(X) = (b, 0, b - d, d)$ et $F^2(X) = (b, b - d, |b - 2d|, b - d)$. Si l'on a $0 < d < b$, la norme diminue strictement au pas suivant car les voisins de b sont non nuls. Si $d = 0$ on a $F(X) = (b, 0, b, 0)$, donc $F^3(X) = 0$ par 8.4. Si $d = b$, on a $F(X) = (b, 0, 0, b)$, donc $F^4(X) = 0$ par 8.4.

2) $c = 0$. Dans ce cas, on a $F(X) = (b, b, d, d)$ et $F^4(X) = 0$, encore par 8.4.

3) $d = 0$. Dans ce cas, on a $F(X) = (b, b - c, c, 0)$ puis $F^2(X) = (c, |b - 2c|, c, b)$ et $F^3(X)$ est de norme strictement plus petite que X, sauf si $c = 0$ ou $c = b$, cas déjà envisagés.

4) $d = b$. Dans ce cas on a $F(X) = (b, b - c, b - c, b)$ et $F^4(X) = 0$, toujours par 8.4.

On peut donc supposer $0 < c < b$ et $0 < d < b$. Mais alors, la norme de $F^2(X)$ est $< b$ car, dans $F(X)$, le terme b est le seul à atteindre le maximum et ses voisins sont non nuls.

8.6 Théorème. *On suppose $n = 4$. Soit $X \in \mathbf{R}^n$. Alors $F^N(X)$ tend vers 0 quand N tend vers l'infini.*

Démonstration. On raisonne par l'absurde en supposant qu'il existe $X \in \mathbf{R}^4$ tel que $F^N(X)$ ne tende pas vers 0. Comme la norme décroît en appliquant F, la suite $\|F^N(X)\|$ a une limite quand N tend vers l'infini, et cette limite est non nulle par hypothèse. En appliquant 2.1.1, on peut supposer que cette limite est 1. Vu le lemme 8.5, les normes des $F^N(X)$ sont strictement plus grandes que 1. La contradiction cherchée vient du lemme suivant :

8.7 Lemme. *Soit $X \in (\mathbf{R}^+)^4$ de norme $1 + \epsilon$. Si ϵ est assez petit, il existe N tel que $\|F^N(X)\| < 1$.*

Démonstration. Supposons $\epsilon < 1/2^6$. En retranchant le plus petit terme de X aux autres et en permutant circulairement au besoin, on se ramène au cas $X = (0, b, c, d)$ avec $b = \|X\| = 1 + \epsilon$. On a $F(X) = (b, b - c, |c - d|, d)$.

Supposons d'abord $c \leq d$. On a alors $F^4(X) = 0$ en vertu de 8.4.

Supposons maintenant $c > d$, de sorte que $F(X) = (b, b - c, c - d, d)$ et $F^2(X) = (c, |b - 2c + d|, |c - 2d|, b - d)$.

8.8 Lemme. *Si on a $c \leq 1$ et $d \geq \epsilon$, alors on a $\|F^2(X)\| \leq 1$.*

Démonstration. Il s'agit de montrer que les quatre termes de $F^2(X)$ sont ≤ 1. C'est évident pour c et pour $b - d$. On a $|c - 2d| = c - 2d$ ou $2d - c$. Dans le premier cas on a $|c-2d| \leq c \leq 1$, dans l'autre $|c-2d| = d-(c-d) \leq d \leq c \leq 1$. Pour l'autre terme, il y a deux cas : $|b-2c+d| = b-2c+d = b-c-(c-d) \leq b - c \leq b - d \leq 1$ ou $|b - 2c + d| = 2c - b - d = c - d - (b - c) \leq c \leq 1$.

En vertu de ce lemme on peut supposer que X vérifie $c > 1$ ou $d < \epsilon$.

• On suppose $c > 1$. Posons $Y = (0, 1, 1, d')$ où $d' = \mathrm{Min}\,(d, 1)$. On a $\|X-Y\| \leq \epsilon$. En vertu de 8.4.6 on a $F^6(Y) = 0$. Comme F est 2-lipschitzienne (voir 2.12) on a $\|F^6(X) - F^6(Y)\| = \|F^6(X)\| \leq 2^6\|X - Y\| \leq 2^6\epsilon \leq 1$.

• On suppose $d < \epsilon$. On peut approcher X à ϵ près par $Y = (0, 1, c, 0)$. Là encore on a $F^6(Y) = 0$ par 8.4.4 et on conclut de la même manière.

8.9 *Remarque.* J'imagine que ce résultat vaut pour $n = 2^r$ quelconque, mais j'ai eu assez de mal avec $n = 4$ pour ne pas m'aventurer sur le cas général.

Références

[1] Perrin Daniel, *Cours d'algèbre*, Ellipses, 1996.