Théorèmes de Chevalley-Warning et d'Erdös-Ginzburg-Ziv

Leçons : 120 [1], 123, 142, 144, *121, 126, 190*

[Ser], paragraphe 1.2
[Zav], problème 7.II

Théorème (*Chevalley-Warning*)

Soient p un nombre premier, $r \in \mathbb{N}^*$; on note $q = p^r$.
Soient $f_1, \dots, f_s \in \mathbb{F}_q[X_1, \dots, X_n]$, tels que $\sum_{i=1}^{s} \deg f_i < n$.
On note $V = \left\{ (x_1, \dots, x_n) \in \mathbb{F}_q^n \middle| \forall i \in [\![1, s]\!], f_i(x_1, \dots, x_n) = 0 \right\}$.
Alors on a : $\#V \equiv 0\,[p]$.

Démonstration :

Posons $P = \prod_{i=1}^{s} \left(1 - f_i^{q-1}\right)$ et soit $\underline{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$.

- Si $\underline{x} \in V$, alors $\forall i \in [\![1, s]\!], f_i(\underline{x}) = 0$ et donc $P(\underline{x}) = 1$.
- Si $\underline{x} \notin V$, alors $\exists i_0 \in [\![1, s]\!], f_{i_0}(\underline{x}) \neq 0$ puis $f_{i_0}(\underline{x})^{q-1} = 1$ d'où $P(\underline{x}) = 0$.

Ainsi, en posant $S(f) = \sum_{\underline{x} \in \mathbb{F}_q^n} f(\underline{x})$ pour $f \in \mathbb{F}_q[X_1, \dots, X_n]$, on a : $S(P) = \sum_{\underline{x} \in V} 1 + 0 \equiv \#V\,[p]$.

On veut désormais montrer que $S(P) = 0$.

Lemme

Soit $u \in \mathbb{N}$, vérifiant $u = 0$ ou $(q-1) \nmid u$.
On pose $s(X^u) = \sum_{x \in \mathbb{F}_q} x^u$, et on a alors $s(X^u) = 0$, avec la convention $0^0 = 1$. [2]

Démonstration :

Si $u = 0$, alors $\forall x \in \mathbb{F}_q, x^u = 1$ et $s(X^u) = 0$.
Si $(q-1) \nmid u$, on écrit la division euclidienne $u = (q-1)k + r$, où $k \in \mathbb{N}$ et $0 < r < q-1$.
Soit y un générateur de $\mathbb{F}_q^\times$, qui est cyclique [3].

On a donc $y^u = \left(y^{q-1}\right)^k y^r = y^r \neq 1$ car y est d'ordre $(q-1)$ et $0 < r < q-1$.
Ainsi on a :

$$s(X^u) = \sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q^\times} x^u = \sum_{x \in \mathbb{F}_q^\times} (xy)^u = y^u \sum_{x \in \mathbb{F}_q^\times} x^u = y^u s(X^u)$$

Donc $(1 - y^u)\, s(X^u) = 0$, puis par intégrité de $\mathbb{F}_q$, $s(X^u) = 0$ car $1 - y^u \neq 0$. ■

On a $\deg P = \sum_{i=1}^{s} (q-1) \deg f_i < n(q-1)$ et donc $P = \sum_{|\underline{u}| < n(q-1)} \alpha_{\underline{u}} \underline{X}^{\underline{u}}$ où $|\underline{u}| = \sum_{j=1}^{n} u_j$ et $\alpha_{\underline{u}} \in \mathbb{F}_q$.

D'où $S(P) = \sum_{\underline{x} \in \mathbb{F}_q^n} \sum_{|\underline{u}| < n(q-1)} \alpha_{\underline{u}} \underline{x}^{\underline{u}} = \sum_{|\underline{u}| < n(q-1)} \alpha_{\underline{u}} S(\underline{X}^{\underline{u}})$.

Or, pour $|\underline{u}| < n(q-1)$, $S(\underline{X}^{\underline{u}}) = \sum_{(x_1, \dots, x_n) \in \mathbb{F}_q^n} x_1^{u_1} \dots x_n^{u_n} = \sum_{x_1 \in \mathbb{F}_q} x_1^{u_1} \dots \sum_{x_n \in \mathbb{F}_q} x_n^{u_n} = \prod_{j=1}^{n} s(X^{u_j})$.

Mais $\sum_{j=1}^{n} u_j < n(q-1)$ impose $\exists j_0 \in [\![1, n]\!], u_{j_0} < q-1$ donc $(q-1) \nmid u_{j_0}$ ou $u_{j_0} = 0$.

Donc $s\left(X^{u_{j_0}}\right) = 0$, d'où $S(P) = 0$ puis $\#V \equiv 0\,[p]$. ■

1. On passera le lemme permettant de démontrer le théorème de Chevalley-Warning et on détaillera le cas non-premier du théorème d'Erdös-Ginzburg-Ziv.
2. On peut montrer que si $u \geqslant 1$ et $(q-1) | u$, alors $s(X^u) = -1$.
En effet, $\exists k \in \mathbb{N}^*, u = (q-1)k$ et pour $x \in \mathbb{F}_q^\times$, $x^u = \left(x^{q-1}\right)^k = 1^k = 1$.
En outre $0^u = 0$, donc $s(X^u) = (q-1) \times 1 + 0 = -1$ dans $\mathbb{F}_q$.
3. Pour la cyclicité de $\mathbb{F}_q^\times$, on renvoie à la page **??**.

Diffusion à titre gratuit uniquement.

Théorème (*Erdös-Ginzburg-Ziv*)

Soit p un nombre premier, et soient $a_1, \dots, a_{2p-1} \in \mathbb{Z}$.[4]
Parmi ces $(2p-1)$ nombres entiers, on peut en trouver p dont la somme est divisible par p.

Démonstration :

Pour $a \in \mathbb{Z}$, on note $\overline{a}$ sa classe modulo p.

On considère les polynômes $P_1 = \sum_{k=1}^{2p-1} X_k^{p-1}, P_2 = \sum_{k=1}^{2p-1} \overline{a_k} X_k^{p-1} \in \mathbb{F}_p\left[X_1, \dots, X_{2p-1}\right]$.

On a : $\deg P_1 + \deg P_2 = 2p-2 < 2p-1$, et $(0, \dots, 0)$ est une racine commune à ces deux polynômes ; donc, par le théorème de Chevalley-Warning, ils admettent une autre racine commune $\left(x_1, \dots, x_{2p-1}\right) \in \mathbb{F}_p^{2p-1}$.

De $P_1\left(x_1, \dots, x_{2p-1}\right) = 0$, il vient que parmi $x_1, \dots, x_{2p-1}$, exactement p d'entre eux sont non-nuls, et on les note $x_{n_1}, \dots, x_{n_p}$.

De $P_2\left(x_1, \dots, x_{2p-1}\right) = 0$, il vient ensuite que $\sum_{i=1}^{p} \overline{a_{n_i}} = 0$.

On a donc trouvé p éléments $a_{n_1}, \dots, a_{n_p}$ dont la somme est divisible par p. ■

Références

[Ser] J.-P. SERRE – *Cours d'arithmétique*, 1^e^ éd., Presses Universitaires de France, 1970.
[Zav] M. ZAVIDOVIQUE – *Un max de maths*, Calvage & Mounet, 2013.

4. Ce résultat reste vrai pour n'importe quel $n \in \mathbb{N}^*$. On opère par récurrence forte.
 - Si $n = 1$, le résultat est trivial.
 - Soit $n > 1$, on suppose le résultat jusqu'au rang $(n-1)$. Soient $a_1, \dots, a_{2n-1} \in \mathbb{Z}$.
   - Si n est premier, c'est l'objet du développement.
   - Sinon, on écrit $n = pn'$, avec p premier et $n' \in \mathbb{N}^*$.
   On a alors : $2n-1 = 2n'p-1 = (2n'-1)p + p - 1$.
   Pour i allant de 1 à $2n'-1$, on construit par récurrence les ensembles suivants appelés E_i :
   E_i est un ensemble de p éléments parmi $\left\{a_j \middle| j \in [\![1, (i+1)p-1]\!]\right\} \setminus \bigcup_{k=1}^{i-1} E_k$, dont la somme est divisible par p.
   La construction de ces ensembles utilise le résultat démontré dans le développement, car $\# \left\{a_j \middle| j \in [\![1, (i+1)p-1]\!]\right\} \setminus \bigcup_{k=1}^{i-1} E_k = 2p-1$.
   Puis, pour $i \in [\![1, 2n'-1]\!]$, S_i désigne la somme des éléments de E_i et $S_i' = \frac{S_i}{p} \in \mathbb{Z}$.
   Par hypothèse de récurrence, parmi les $(2n'-1)$ entiers S_i', il en existe n' dont la somme est divisible par n', et on les note $S_{k_1}', \dots, S_{k_n'}'$.
   On pose alors $E = \bigsqcup_{i=1}^{n'} E_{k_i}$, et $\#E = n'p = n$ et $\sum_{x \in E} x = \sum_{i=1}^{n'} S_{k_i} = p \sum_{i=1}^{n'} S_{k_i}'$.
   Or $n' \left| \sum_{i=1}^{n'} S_{k_i}' \right.$ donc $n = pn' \left| \sum_{x \in E} x \right.$.

On peut même montrer un résultat d'optimalité : prenons un ensemble de $(2n-2)$ entiers composé de $(n-1)$ fois 0, et de $(n-1)$ fois 1. Un sous-ensemble de n entiers parmi ceux-ci sera de somme comprise entre 1 et $n-1$, donc non-divisible par n.

Diffusion à titre gratuit uniquement.