Chevalley-Warning et Erdös-Ginzburg-Ziv

Théorème 1. Soient p premier, $r \in \mathbb{N}^*$, $q = p^r$. Soient $f_1, \dots, f_s \in \mathbb{F}_q[X_1, \dots, X_n]$ tels que $\sum \deg f_i < n$. Le cardinal de l'ensemble ci-dessous (ensemble des racines communes à tous les f_i) est nul $\mod p$:

$$V = \left\{ x \in \mathbb{F}_q^n,\ \forall i \in \{1, \dots, s\},\ f_i(x) = 0 \right\}.$$

Démonstration. Soit $x \in \mathbb{F}_q^n$. Considérons le polynôme de $\mathbb{F}_q[X_1, \dots, X_n]$ et les applications suivants :

$$P = \prod_{i=1}^{s} (1 - f_i^{q-1}),\ \ S : f \mapsto \sum_{x \in \mathbb{F}_q^n} f(x),\ \ s : f \mapsto \sum_{x \in \mathbb{F}_q} f(x).$$

— Si $x \in V$, alors $P(x) = 1$.
— Sinon, il existe i_0 tel que $f_{i_0}(x)^{q-1} \neq 0$, donc $f_{i_0}(x)^{q-1} = 1$ dans $\mathbb{F}_q$, ce qui donne $P(x) = 0$.
De là, $S(P) = \mathrm{Card} V \mod q$ (et $\mod p$ car $q = p^r$).

Lemme 2. Si $u = 0$ ou $(q-1) \nmid u$, alors $s(X^u) = 0$ avec pour convention $0^0 = 1$.

Démonstration. Si $u \neq 0$, alors par division euclidienne, $u = (q-1)k + r$ avec $0 < r < q-1$. Soit y un générateur de $\mathbb{F}_q^*$ cyclique.

$$s(X^u) = \sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q^*} (yx)^u = y^u s(X^u).$$

Donc $(1 - y^u) s(X^u) = 0$, ce qui donne $s(X^u) = 0$ par intégrité de $\mathbb{F}_q$ puisque $y^u = y^r \neq 1$. □

Par hypothèse, $\deg P < n(q-1)$. On écrit donc P sous la forme suivante :

$$P = \sum_{|\underline{u}| < n(q-1)} \alpha_{\underline{u}} X^{\underline{u}},$$

où $\alpha_{\underline{u}} \in F_q$, avec les notations $X^{\underline{u}} = X_1^{u_1} \dots X_n^{u_n}$ et $|\underline{u}| = \sum_{j=1}^{n} u_j$. Si $|\underline{u}| < n(q-1)$, alors

$$S(X^{\underline{u}}) = \sum_{x \in \mathbb{F}_q^n} x_1^{u_1} \dots x_n^{u_n} = \left(\sum_{x_1 \in \mathbb{F}_q} x_1^{u_1} \right) \dots \left(\sum_{x_n \in \mathbb{F}_q} x_n^{u_n} \right) = \prod_{i=1}^{n} s(X^{u_i}) = 0,$$

car il existe j_0 tel que $u_{j_0} < q-1$, donc $s(X^{u_{j_0}}) = 0$ d'après le lemme précédent. Ainsi $S(P) = 0$, d'où le résultat. □

Théorème 3. Soient p premier et $(a_1, \dots, a_{2p-1}) \in \mathbb{Z}^{2p-1}$. On peut en trouver p dont la somme est divisible par p.

Démonstration. Posons $P_1 = \sum_{k=1}^{2p-1} X_k^{p-1}$ et $P_2 = \sum_{k=1}^{2p-1} \overline{a_k} X_k^{p-1}$ dans $\mathbb{F}_p[X_1, \dots, X_{2p-1}]$. D'après le théorème précédent ($\deg P_1 + \deg P_2 < 2p-1$ et $(0, \dots, 0)$ est une racine commune), il existe au moins une autre racine commune à P_1 et P_2, notée $x = (x_1, \dots, x_{2p-1})$. Puisque $x_i^{p-1} \in \{0, 1\}$ et $P_1(x) = 0$, comme les x_i sont non tous nuls, il y en a p non nuls, notés $x_{n_1}, \dots, x_{n_p}$ et la relation $P_2(x) = 0$ donne le résultat : $\sum \overline{a_{n_i}} = 0$. □