# Polynômes irréductibles sur les corps finis

Arnaud Bodin

Laboratoire Paul Painlevé – Université Lille 1

Inria Rocquencourt, 15 décembre 2008

# Les polynômes d'une variable

$\mathbb{F}_{q,d}[x]$ l'ensemble des polynômes unitaires de degré $d$ sur $\mathbb{F}_q$

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \qquad a_i \in \mathbb{F}_q$$

$$N_d = \#\mathbb{F}_{q,d}[x] = q^d$$

$$I_d = \#\{P \in \mathbb{F}_{q,d}[x] \mid P \text{ est irréductible}\}$$

## Théorème

$$I_d = \frac{1}{d}\sum_{k|d} \mu(k) q^{\frac{d}{k}}$$

# Les polynômes d'une variable

## Théorème

$$I_d = \frac{1}{d} \sum_{k|d} \mu(k) q^{\frac{d}{k}}$$

Preuve : $x^{q^n} - x$ est le produit des polynômes unitaires irréductibles dans $\mathbb{F}_q[x]$ dont le degré $d$ divise $n$

$$q^n = \sum_{d|n} d I_d$$

Par la formule d'inversion de Moebius

$$n I_n = \sum_{d|n} \mu(d) q^{\frac{n}{d}}$$

## Corollaire

$$\frac{I_d}{N_d} \sim \frac{1}{d}$$

# Les polynômes de plusieurs variables

$$K[x_1, \ldots, x_n]$$

$$P(x, y) = \sum a_{i,j} x^i y^j$$

$P$ est réductible si $P = Q \times R$

$Q, R \in K[x_1, \ldots, x_n]$ non constants

Exemple : $P(x, y) = x^3 - 2x^2y - xy^3 + 2y^4 = (x - 2y)(x^2 - y^3)$

# Les polynômes sur $\mathbb{F}_q$

$$\mathbb{F}_q[x_1, \ldots, x_n]$$

$$N_d = \#\mathbb{F}_{q,d}[x_1, \ldots, x_n]$$

$$I_d = \#\{P \in \mathbb{F}_{q,d}[x_1, \ldots, x_n] \mid P \text{ est irréductible}\}$$

- Formules pour $I_d$
- Proportion $\frac{I_d}{N_d} \longrightarrow 1$
- Estimation de l'erreur $1 - \frac{I_d}{N_d}$

# Une formule de récurrence

$$N_d = I_d + R_d$$

$$P = \underbrace{(Q_1 \times Q_2 \times \cdots)}_{\alpha_1 \text{ facteurs irréd. de degré 1}} \times \underbrace{(Q_1' \times Q_2' \times \cdots)}_{\alpha_2 \text{ facteurs irréd. de degré 2}} \times \cdots$$

Les facteurs sont uniques et de degré $< d$

$$1\alpha_1 + 2\alpha_2 + \cdots + (d-1)\alpha_{d-1} = d$$

Il y a $\binom{I_k + \alpha_k - 1}{\alpha_k}$ choix pour le terme produit des facteurs de degré $k$

## Lemme

$$I_d = N_d - \sum_{1\alpha_1 + 2\alpha_2 + \cdots + (d-1)\alpha_{d-1} = d} \binom{I_1 + \alpha_1 - 1}{\alpha_1} \times \cdots \times \binom{I_{d-1} + \alpha_{d-1} - 1}{\alpha_{d-1}}$$

# Algorithme

$$N_d = \left(\frac{q^{d+1}-1}{q-1}\right) \cdot q^{\frac{d(d+1)}{2}} \qquad (n=2)$$

1. Initialiser $I_1 = N_1 = q(q+1)$
2. Supposons que nous avons calculer $I_2, \ldots, I_{d-1}$
3. Appliquer la formule de récurrence

$$I_d = N_d - \sum_{1\alpha_1+2\alpha_2+\cdots+(d-1)\alpha_{d-1}=d} \binom{I_1+\alpha_1-1}{\alpha_1} \cdots \binom{I_{d-1}+\alpha_{d-1}-1}{\alpha_{d-1}}$$

# Exemple : polynômes irréductibles dans $\mathbb{F}_2[x, y]$

| $d$ | $N_d$ | $I_d$ | $\frac{I_d}{N_d}$ | $1 - \frac{3}{2^d}$ |
|---|---|---|---|---|
| 1 | 6 | 6 | 1 | -0.5 |
| 2 | 56 | 35 | 0.625 | 0.25 |
| 3 | 960 | 694 | 0.72291... | 0.625 |
| 4 | 31744 | 26089 | 0.82185... | 0.8125 |
| 5 | 2064384 | 1862994 | 0.90244... | 0.90625 |
| 6 | 266338304 | 253247715 | 0.95084... | 0.95312... |
| 7 | 68451041280 | 66799608630 | 0.97587... | 0.97656... |
| 8 | 35115652612096 | 34698378752226 | 0.98811... | 0.98828... |
| 9 | 35993612646875136 | 35781375988234520 | 0.99410... | 0.99414... |
| 10 | 73750947497819242496 | 73534241823793715433 | 0.99706... | 0.99707... |

# Estimation

## Théorème

$n = 2$

$$1 - \frac{I_d}{N_d} \sim \frac{q+1}{q^d}$$

En particulier $\frac{I_d}{N_d} \to 1$ quand $d \to +\infty$

Idée de la preuve : Les polynômes réductibles qui comptent le plus sont ceux de la forme :

$$P = \underbrace{Q}_{\text{degré } 1} \times \underbrace{R}_{\text{degré } d-1}$$

Il y en a environ $I_1 \times I_{d-1}$

# Preuve : borne supérieure

$$I_{d_1} \otimes I_{d_2} \otimes \cdots \otimes I_{d_k} \leqslant q^6 \cdot N_{d-2}$$

$$R_d \leqslant I_1 \otimes I_{d-1} + P_d \cdot q^6 \cdot N_{d-2}$$

Hardy et Ramanujan

$$P_d \sim \frac{1}{4d\sqrt{3}} \exp\left(\pi\sqrt{\frac{2d}{3}}\right) \quad \text{et} \quad P_d < \exp\left(\pi\sqrt{\frac{2d}{3}}\right)$$

pour $d$ assez grand $\quad R_d \leqslant N_1 \cdot N_{d-1} \cdot \left(1 + \frac{1}{d}\right)$

# Preuve : borne inférieure

$$\begin{aligned} R_d &\geqslant I_1 \otimes I_{d-1} \\ &= N_1 \cdot I_{d-1} \\ &= N_1 \cdot \left(N_{d-1} - R_{d-1}\right) \\ &\geqslant N_1 \cdot \left(N_{d-1} - N_1 \cdot \left(1 + \tfrac{1}{d-1}\right) \cdot N_{d-2}\right) \\ &\geqslant N_1 \cdot N_{d-1} \cdot \left(1 - \tfrac{1}{d}\right) \end{aligned}$$

Bilan : pour $d$ assez grand $d$

$$N_1 \cdot N_{d-1} \cdot \left(1 - \frac{1}{d}\right) \leqslant R_d \leqslant N_1 \cdot N_{d-1} \cdot \left(1 + \frac{1}{d}\right)$$

$$\frac{N_1 \cdot N_{d-1}}{N_d} \cdot \left(1 - \frac{1}{d}\right) \leqslant 1 - \frac{I_d}{N_d} = \frac{R_d}{N_d} \leqslant \frac{N_1 \cdot N_{d-1}}{N_d} \cdot \left(1 + \frac{1}{d}\right)$$

# Applications

## Théorème (Ostrowski)

*Si $P \in \mathbb{Z}[x_1, \ldots, x_n]$ est irréductible sur $\mathbb{C}$ alors pour $p$ premier assez grand $(P \bmod p)$ est irréductible sur $\overline{\mathbb{F}_p}$*

## Théorème (Ragot)

*Soit $P \in \mathbb{Z}[x_1, \ldots, x_n]$. Si $(P \bmod p)$ est irréductible sur $\overline{\mathbb{F}_p}$ et de même degré que $P$ alors $P$ est irréductible sur $\mathbb{C}$*

# Extensions

- Constantes explicites $I_d/N_d$ : J. von zur Gathen
- DL à l'ordre $n$
- DL à l'ordre 1 en fonction du bidegré $(\deg_x P, \deg_y P)$

# Polynômes indécomposables

Définition : $P \in K[x_1, \ldots, x_n]$ est *décomposable* sur $K$ s'il existe $Q \in K[x_1, \ldots, x_n]$ et $h \in K[t]$, $\deg h \geqslant 2$ tels que

$$P = h(Q)$$

Exemple : $P(x, y) = x^2y^2 + xy + 1$, $h(t) = t^2 + t + 1$, $Q(x, y) = xy$
Si $P$ est décomposable alors pour tout $\lambda \in K$, $P(x_1, \ldots, x_n) - \lambda$ est réductible

## Théorème (Stein & co)

*$K = \overline{K}$. Si $P$ est indécomposable alors*

1. *Le spectre $\sigma_P = \left\{\lambda \in K \mid P(x_1, \ldots, x_n) - \lambda$ est réductible sur $K\right\}$ est fini*
2. $\#\sigma_P < \deg P$

# Polynomes indécomposables modulo $p$

## Théorème (Bodin-Dèbes-Najib, Buzé-Chèze-Najib)

*Soit $P$ indécomposable à coefficients entiers,*

1. *alors pour $p$ assez grand $(P \bmod p)$ est indécomposable*
2. *et le spectre de $(P \bmod p)$ est la réduction de $\sigma_P$ modulo $p$ :*

$$\sigma_{(P \bmod p)} = (\sigma_P) \bmod p$$

# Polynômes indécomposables sur $\mathbb{F}_q$

## Théorème

1. $J_d/N_d \to 1$
2. 
   - $d = p$ : $D_d = q^d(q^n - 1)$
   - $d = p^2$ : $D_d = q^{p-1}N_p + (q^d - q^{2p-1})(q^n - 1)$
   - $d = pp'$, $p < p'$ : $D_d = q^{p-1}N_{p'} + q^{p'-1}N_p + (q^d - 2q^{p+p'-1})(q^n - 1)$
3. *$n = 2$, $d$ est le produit de plus de 3 premiers :*

$$\left|\frac{D_d}{N_d} - \alpha_d\right| \leqslant \alpha_d \cdot \beta_d \qquad \textit{avec} \quad \begin{cases} \alpha_d = \dfrac{q^{\ell - 1 + \frac{1}{2}(\frac{d}{\ell}+1)(\frac{d}{\ell}+2)}}{q^{\frac{1}{2}(d+1)(d+2)}} \\ \beta_d = \dfrac{d}{q^{\frac{d}{\ell}}} \end{cases}$$

*où $\ell > 1$ est le premier diviseur de $d$*

# Idées de la preuve

$P = h \circ Q$, décomposition unique si :

1. $h \in K[t]$, $\deg h \geqslant 2$, $Q \in K[x_1, \ldots, x_n]$
2. $Q$ est indécomposable et unitaire, $Q(0, \ldots, 0) = 0$

## Lemme

$$J_d = N_d - \sum_{d' | d, d' < d} q^{\frac{d}{d'} - 1} \times J_{d'}$$

Les polynômes décomposable de degré $d$ en plus grand nombre sont les $h \circ Q$ avec $\deg h = \ell > 1$ le plus petit diviseur de $d$