



Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation
ESA - CNRS 6090

Sur la distribution du nombre de zéros des fonctions polynômes sur les corps finis

Jean-François Ragot

Rapport de recherche n° 2002-07

Université de Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex
Tél. 05 55 45 73 23 - Fax. 05 55 45 73 22 - laco@unilim.fr

<http://www.unilim.fr/laco/>

SUR LA DISTRIBUTION DU NOMBRE DE ZÉROS DES POLYNÔMES SUR LES CORPS FINIS

JEAN-FRANÇOIS RAGOT

ABSTRACT. On considère l'ensemble des polynômes en r indéterminées sur le corps fini \mathbb{F}_q et de degré borné par d . Nous étudions la variable nombre de zéros d'un tel polynôme aléatoire. Nous récapitulons des résultats permettant d'établir que cette variable suit une loi binomiale pour $d \geq q^r$, et montrons que cette condition peut être affaiblie à $d \geq r(q-1)$.

INTRODUCTION

Soit $\mathcal{F} = \mathbb{F}_q[x_1, \dots, x_r]$ l'espace vectoriel des polynômes en r indéterminées sur le corps fini à q éléments, et soit $\mathcal{F}_d = \{f \in \mathcal{F} : \deg(f) \leq d\}$ le sous-espace vectoriel des éléments de \mathcal{F} de degré total au plus d . Pour f dans \mathcal{F} , on note $N(f)$ le nombre de zéros distincts de f dans \mathbb{F}_q^r . L'ensemble \mathcal{F}_d étant muni de la probabilité uniforme, N définit alors une variable aléatoire à valeurs entières. L'objectif de cet article est d'établir le résultat suivant :

Proposition 1. *Si $d \geq r(q-1)$, la variable aléatoire N suit une loi binomiale de paramètres q^r et $\frac{1}{q}$.*

Ce résultat est connu pour d suffisamment grand; Dans [Odo], R.W.K. Odoni montre en particulier que $\frac{N(f) - q^{r-1}}{\sqrt{q^{r-1} - q^{r-2}}}$ tend vers une loi de Gauss réduite quand q et d tendent vers l'infini. Bien qu'il ne l'expose pas explicitement, Odoni prouve "au passage" la proposition 1 pour d plus grand que q^r .

Dans [Rag], nous avons déjà utilisé ces résultats pour calculer le nombre de polynômes ayant (au moins) un zéro dans \mathbb{F}_q^r (i.e. la probabilité $Pr(N \geq 1)$), et nous avons montré que le résultat reste valable quand on affaiblit la condition à $d \geq r(q-1)$.

Nous généralisons ceci à la distribution complète de N , et donnons une démonstration plus élémentaire du passage de $d \geq q^r$ à $d \geq r(q-1)$.

Ce résultat est obtenu en calculant la *fonction génératrice des moments* de N . La fonction génératrice est une notion fondamentale du calcul des probabilités. Elle établit le lien entre les probabilités et les *moments factoriels* d'une variable aléatoire discrète. Or les moments factoriels de N sont directement liés aux cardinaux de certains sous-espaces de \mathcal{F}_d , cardinaux que nous calculons pour $d \geq r(q-1)$.

Dans la première section, nous donnons les résultats fondamentaux concernant la fonction génératrice d'une variable aléatoire discrète. En section 2 nous mettons en relation moments factoriels de N et sous-espaces polynomiaux. Ces sous-espaces sont dénombrés en section 3. Enfin en section 4, nous reconstituons la fonction génératrice de N , que l'on reconnaît comme étant celle d'une variable binomiale.

1. FONCTION GÉNÉRATRICE D'UNE VARIABLE ALÉATOIRE DISCRÈTE

On appelle *moment factoriel* d'ordre k (k entier positif) d'une variable aléatoire X l'espérance mathématique de $X(X-1) \cdots (X-k+1)$:

$$\mu_k(X) = E(X(X-1) \cdots (X-k+1)) .$$

Pour une variable aléatoire discrète à valeurs entières non négatives, on a, en désignant par p_x la probabilité attachée à la valeur x et par $\binom{u}{v}$ le coefficient binomial standard :

$$\begin{aligned}\mu_k(X) &= \sum_{x \geq 0} p_x x(x-1) \cdots (x-k+1) \\ &= \sum_{x \geq k} p_x x(x-1) \cdots (x-k+1) \\ &= k! E \left(\binom{X}{k} \right).\end{aligned}$$

On appelle *fonction génératrice des moments* d'une variable aléatoire discrète X à valeurs entières non négatives l'espérance de u^X où u est une quantité certaine non négative.

$$\begin{aligned}g_X(u) &= E(u^X) \\ &= \sum_{x \geq 0} p_x u^x.\end{aligned}$$

Si la variable X est à nombre fini de valeurs, on peut dériver sous le signe \sum et

$$g_X^{(k)}(u) = \sum_{x \geq k} p_x x(x-1) \cdots (x-k+1) u^{x-k}.$$

Pour $u = 1$

$$g_X^{(k)}(1) = \mu_k(X),$$

la fonction génératrice fournit les moments factoriels par ses dérivées successives en $u = 1$.

Inversement, si on peut développer $g_X(u)$ en série entière au voisinage de 1, ce qui est le cas si X est à nombre fini de valeurs, on obtient :

$$\begin{aligned}g_X(u) &= \sum_{k \geq 0} \frac{(u-1)^k}{k!} g_X^{(k)}(1) \\ &= \sum_{k \geq 0} \frac{(u-1)^k}{k!} \mu_k(X).\end{aligned}$$

La connaissance des moments factoriels de X permet de reconstituer sa fonction génératrice, puis d'obtenir les probabilités par le calcul de ses dérivées successives en 0.

Pour terminer cette section, rappelons que n étant un entier non nul et a un réel plus grand que 1, on désigne par *variable binomiale* de paramètres n et $\frac{1}{a}$ une variable aléatoire X à valeurs dans $\{x \in \mathbb{N} : x \leq n\}$ telle que $p_x = \binom{n}{x} \left(\frac{1}{a}\right)^x \left(1 - \frac{1}{a}\right)^{n-x}$. Sa fonction génératrice est

$$\begin{aligned}g_X(u) &= \sum_{x \geq 0} p_x u^x = \sum_{x \geq 0} \binom{n}{x} \left(\frac{1}{a}\right)^x \left(1 - \frac{1}{a}\right)^{n-x} u^x \\ &= \left(\frac{u+a-1}{a}\right)^n.\end{aligned}$$

2. MOMENTS FACTORIELS DE N ET SOUS-ENSEMBLES POLYNOMIAUX

La variable aléatoire N prend ses valeurs dans $\{0, 1, \dots, q^r\}$. Notons p_n la probabilité attachée à chacune de ces valeurs :

$$p_n = \frac{1}{\#\mathcal{F}_d} \sum_{\substack{f \in \mathcal{F}_d \\ N(f)=n}} 1.$$

Par définition (section 1),

$$E \left(\binom{N}{k} \right) = \sum_{n \geq k} p_n \frac{n(n-1) \cdots (n-k+1)}{k!};$$

On a alors

$$\begin{aligned} E \left(\binom{N}{k} \right) &= \frac{1}{\#\mathcal{F}_d} \sum_{f \in \mathcal{F}_d} \frac{N(f)(N(f)-1) \cdots (N(f)-k+1)}{k!} \\ &= \frac{1}{\#\mathcal{F}_d} \sum_{f \in \mathcal{F}_d} \#\{A \subset \mathbb{F}_q^r; \#A = k; f \text{ s'annule en tout point de } A\} \\ &= \frac{1}{\#\mathcal{F}_d} \sum_{\substack{A \subset \mathbb{F}_q^r \\ \#A = k}} \#\{f \in \mathcal{F}_d; f \text{ s'annule en tout point de } A\}. \end{aligned}$$

Etant donné un sous-ensemble A de \mathbb{F}_q^r , il nous faut calculer le cardinal du sous-ensemble des polynômes de \mathcal{F}_d s'annulant en tout point de A .

3. DÉNOMBREMENT DES POLYNÔMES DE \mathcal{F}_d S'ANNULANT SUR UN SOUS-ENSEMBLE DE \mathbb{F}_q^r

Soit I un idéal de \mathcal{F} ; notons $I_d = I \cap \mathcal{F}_d$. Pour A sous-ensemble de \mathbb{F}_q^r , on note $I(A)$ l'idéal des éléments de \mathcal{F} qui s'annulent en tout point de A , et $I_d(A) = I(A) \cap \mathcal{F}_d$. Nous calculons ici le cardinal de $I_d(A)$ pour d suffisamment grand.

Les ensembles \mathcal{F}_d , I_d et \mathcal{F}_d/I_d sont des espaces vectoriels sur \mathbb{F}_q de dimensions finies et

$$\dim(I_d) + \dim(\mathcal{F}_d/I_d) = \dim(\mathcal{F}_d).$$

Dénombrer les éléments de I_d revient donc à calculer sa dimension sur \mathbb{F}_q .

Proposition 2. *Soit A un sous-ensemble de k points de \mathbb{F}_q^r ; si $d \geq k$*

$$\#I_d(A) = q^{-k} \#\mathcal{F}_d.$$

Cette proposition est une conséquence des deux lemmes suivants,

Lemme 1. *Si $\dim(\mathcal{F}/I)$ est finie, alors pour $d \geq \dim(\mathcal{F}/I)$*

$$\dim(\mathcal{F}_d/I_d) = \dim(\mathcal{F}/I).$$

On trouvera la preuve de ce lemme dans [Odo], lemme 1.1.

Lemme 2. *Soit A un sous-ensemble de k points de \mathbb{F}_q^r ;*

$$\dim(\mathcal{F}/I(A)) = k.$$

La preuve de ce dernier lemme est une application du théorème Chinois. On en trouvera le détail dans la section 2 de [Rag].

Proposition 3. *Soit A un sous-ensemble de k points de \mathbb{F}_q^r ; si $d \geq r(q-1)$*

$$\#I_d(A) = q^{-k} \#\mathcal{F}_d.$$

Pour faire la preuve de cette proposition, il nous faut établir un résultat intermédiaire.

Posons $b = r(q-1)$ et notons $\deg_i(f)$ le degré de f en l'indeterminée x_i . Soit

$$R = \{f \in \mathcal{F} : \deg_i(f) \leq q-1\}$$

(Notons que R est un sous-espace vectoriel de \mathcal{F}_b) et soit J l'idéal de \mathcal{F} engendré par les polynômes $x_1^q - x_1, \dots, x_r^q - x_r$. Remarquons que si f appartient à J , il s'annule en tout point de \mathbb{F}_q^r .

Lemme 3. *Si $d \geq b$, \mathcal{F}_d/J_d est isomorphe à R .*

Preuve Montrons tout d'abord que pour tout f dans \mathcal{F} , il existe un unique \bar{f} de R tel que $f \equiv \bar{f} \pmod{J}$.

Existence : par récurrence sur r . Pour $r = 1$, le reste dans la division Euclidienne de f par $x_1^q - x_1$ répond au problème. Supposons donc que

$$\forall f \in \mathbb{F}_q^{r-1}, \exists \bar{f} \in R \text{ tel que } \bar{f} \equiv f \pmod{J}.$$

Soit $f \in \mathbb{F}_q^r$

$$f(x_1, \dots, x_r) = \sum_{k=0}^{\deg_r(f)} f_k(x_1, \dots, x_{r-1})x_r^k.$$

D'après l'hypothèse de récurrence, pour tout k il existe \bar{f}_k dans R tel que $\bar{f}_k \equiv f_k \pmod{J}$. D'autre part, soit $g_k(x_r)$ le reste dans la division Euclidienne de x_r^k par $x_r^q - x_r$, alors g_k est dans R et $g_k(x_r) \equiv x_r^k \pmod{J}$. Construisons le polynôme $\bar{f} = \sum_{k=0}^{\deg_r(f)} \bar{f}_k g_k$. Pour tout i de 1 à $r - 1$, $\deg_i(\bar{f}) = \deg_i \bar{f}_k$ et $\deg_r(\bar{f}) = \deg(g_k)$ ce qui prouve que \bar{f} appartient à R . Enfin, on a clairement $\bar{f} \equiv f \pmod{J}$.

Unicité. Soit \bar{f} et \bar{g} dans R tels que $\bar{f} \equiv \bar{g} \pmod{J}$; Alors $\bar{f} - \bar{g}$ appartient à J et s'annule donc en tout point de \mathbb{F}_q^r ; Ainsi $\bar{f} - \bar{g}$ a q^r solutions.

D'autre part, $\bar{f} - \bar{g}$ appartient à R , il est donc de degré strictement inférieur à q en chaque indéterminée. Il ne peut ainsi pas avoir q^r solutions à moins d'être nul (preuve par récurrence sur r), ce qui entraîne que $\bar{f} = \bar{g}$ (ceci entraîne en outre que J est *exactement* l'idéal des polynômes qui s'annulent en tout point de \mathbb{F}_q^r).

Pour terminer, si $d \geq b$, l'homomorphisme de \mathcal{F}_d dans R qui associe \bar{f} à f est surjectif d'où le lemme. \square

Preuve de la proposition 3. Nous allons montrer que pour $d \geq b$,

$$\frac{\#I(A)_d}{\#\mathcal{F}_d} = \frac{\#(I(A)_b \cap R)}{\#R}.$$

et ne dépend donc pas de d .

En effet on a $R + I_d(A) \subset \mathcal{F}_d$ et $\mathcal{F}_d = R + J_d \subset R + I_d(A)$ (l'égalité étant une conséquence du lemme 3). Ainsi $\mathcal{F}_d = R + I_d(A)$ et

$$\mathcal{F}_d/I_d(A) = (R + I_d(A))/I_d(A).$$

Comme $(R + I_d(A))/I_d(A)$ est isomorphe à $R/R \cap I_d(A)$, on arrive à

$$\mathcal{F}_d/I_d(A) \approx R/R \cap I_d(A). \quad (1)$$

et on obtient le résultat sur les cardinaux en remarquant que $R \cap I_d(A) = R \cap I_b(A)$ et en comparant les dimensions dans (1). Il ne reste alors plus qu'à appliquer la proposition 2. \square

4. FONCTION GÉNÉRATRICE DE N

Pour terminer, reconstituons la fonction génératrice de N .

Proposition 4. *Si $d \geq q(r - 1)$,*

$$g_N(u) = \left(\frac{u + q - 1}{q} \right)^{q^r}.$$

Preuve A la fin de la section 2, Nous avons vu que

$$E \left(\binom{N}{k} \right) = \frac{1}{\#\mathcal{F}_d} \sum_{\substack{A \subset \mathbb{F}_q^r \\ \#A=k}} \#I_d(A).$$

On tire des propositions 2 et 3 que pour A sous-ensemble de k points de \mathbb{F}_q^r et si $d \geq \min(k, r(q-1))$,

$$\#I_d(A) = q^{-k} \#\mathcal{F}_d;$$

On en déduit que si $d \geq \min(k, r(q-1))$,

$$E \left(\binom{N}{k} \right) = \binom{q^r}{k} q^{-k}.$$

En appliquant les définitions de la section 1 à N on a

$$g_N(u) = \sum_{k=0}^{q^r} \frac{(u-1)^k}{k!} \mu_k(N)$$

et

$$\mu_k(N) = k! E \left(\binom{N}{k} \right).$$

On a donc

$$g_N(u) = \sum_{k=0}^{q^r} (u-1)^k E \left(\binom{N}{k} \right)$$

et pour $d \geq r(q-1)$

$$g_N(u) = \sum_{k=0}^{q^r} (u-1)^k \binom{q^r}{k} q^{-k}.$$

dont le calcul donne le résultat par le binôme de Newton □

On reconnaît la fonction génératrice d'une variable binomiale de paramètres q^r et $\frac{1}{q}$, ce qui prouve la proposition 1.

REFERENCES

- [Cal] G. CALOT : *Cours de calcul des probabilités*. Dunod (1967).
- [Odo] R.W.K. ODONI : *Zeros of random polynomials over finite fields*. Mathematical Proceedings of the Cambridge Philosophical Society, Vol. 111, March 1992, Part2, pg 193-197 (1992).
- [Rag] J.F. RAGOT : *Counting Polynomials with Zeros of Given Multiplicities in Finite Fields*. Finite Fields and Their Applications 5, 219-231 (1999)