ASYMPTOTIQUE ET FONCTIONS GÉNÉRATRICES

Philippe Flajolet

Cours de remplacement du 3 novembre 2005

Version du 4 novembre 2005

Ces notes télégraphiques font le point de quelques techniques fondamentales concernant l'**analyse asymptotique des coefficients de fonctions génératrices.**

On a déjà présenté les **méthodes symboliques** : on se dote d'un langage de constructions approprié et on en déduit de manière automatique les équations de séries génératrices associées à la description (ou "spécification") d'un problème combinatoire. En interpretant ces séries génératrices, jusqu'ci des séries formelles comme des objets de l'**analyse classique**, c'est-à-dire des **fonctions**, il devient possible d'obtenir directement des informations **asymptotiques** sur les coefficients. De la sorte, les méthodes symboliques se greffent naturellement sur les méthodes analytiques et il n'est pas nécessaire de développer explicitement[1] une série pour en estimer les coefficients. Cette chaîne est l'épine dorsale du domaine appelé *combinatoire analytique*. Les techniques s'organisent de la manière suivante :

– Cas d'une fonction $f(z)$ en une variable : on tire de l'information asymptotique sur $f_n = [z^n]f(z)$ à partir de données analytiques sur $f(z)$. Ce cas recouvre les dénombrements (par OGF ou EGF) ainis que les fonctions en une variables issues des moments de paramètres (et tirées de BGF par $\frac{\partial}{\partial u} f(z, u)$ suivi de la réduction $u \mapsto 1$.)

– Cas d'une fonction $f(z, u)$ en deux variable : on tire de l'information asymptotique sur $f_{n,k} = [z^n u^k]f(z, u)$ à partir de données analytiques sur $f(z, u)$ En ce cas, on caractérise de fait des "lois limites"de probabilité.

1. Séries et fonctions

Soit $f(z) = \sum f_n z^n$ une série entière (par exemple une série génératrice). Les f_n sont *a priori* des complexes quelconques (pour nous, de fait, des réels positifs et souvent même des rationnels ou des entiers). Ce cas recouvre donc les OGFs et les EGFs. La propriété de base est la suivante :

Propriété. *Il existe un nombre R avec $0 \leq R \leq +\infty$ tel que la série $f(z)$ converge pour $|z| < R$ et diverge pour $|z| > R$. Le disque (cercle) de rayon R est appelé le disque (cercle) de convergence de la série.*

[1] développement n'existent que très sporadiquement et pour des problèmes assez simples. Exemples : les mots (2^n) ; les compositions en sommants 1 ou 2 (Fibonacci), les nombres de Catalan qui comptent triangulations, arbres généraux et arbres binaires dans le cas planaire et non étiqueté ; les nombres de Stirling liés aux partitiosn d'ensemble et aux surjections.

PREUVE. Facile : si le terme général $f_n z^n$ reste borné en $z = r > 0$, on a convergence (géométrique) en tout $r' < r$. Alors R est le sup de ces r. On dispose ensuite de l'inégalité triangulaire pour l'extension aux complexes. □.

Une forme équivalente (pour $R \neq 0, +\infty$) est : *pour tout* $\epsilon > 0$, *on a*

$$f_n(R-\epsilon)^n \to 0; \qquad f_n(R+\epsilon)^n \quad \text{non borné.}$$

Ou encore, les coefficients vérifient

$$f_n = R^{-n}\theta(n).$$

On appelle le terme en R^{-n} le *taux de croisance exponentiel*. La fonction $\theta(n)$, dite *facteur subexponentiel*, croît moins vite que toute exponentielle croissante ($(1+\eta)^n$) et domine infiniment souvent toute exponentielle décroissante ($(1-\eta)^n$). Typiquement, ici, $\theta(n)$ sera de la forme asymptotique $n^\kappa (\log n)^r$.

EXEMPLES : Mots binaires, $\sum 2^n z^n$ ($R = 1/2$) ; Fibonacci $\sum F_n z^n$ ($R = 1/\varphi$ où φ est le nombre d'or) ; Nombres de Catalan [arbres binaires, généraux, triangulations] $(1-\sqrt{1-4z})/(2z)$ avec $R = \frac{1}{4}$ et, de fait, $C_n \sim 4^n n^{-3/2}$ par Stirling, une fois obtenue la forme explicite de C_n.

CONCLUSION. *La connaissance du rayon de convergence d'une fonction génératrice nous renseigne au moins grossièrement (taux exponentiel) sur l'asymptotique de ses coefficients.*

2. COEFFICIENTS DES FONCTIONS RATIONNELLES

L'objectif de cette section est la détermination de R et θ dans le cas simple des fractions rationnelles. Rappeleons que la fonction $f(z)$ est rationnelle si $f(z) = \frac{P(z)}{Q(z)}$ avec P, Q polynômes. On suppose P, Q premiers entre eux et $Q(0) \neq 0$. On a :

Propriété. *Si* f *est rationnelle et* $\deg(P) < \deg(Q)$ [2]*, alors elle se décompose en une somme finie d'éléments simples :*

$$f(z) = \sum_{a,r} \frac{c}{(z-a)^r}.$$

(Les a, possiblement complexes, sont les pôles de f, soit les zéros du dénominateur $Q(z)$. Le r maximum pour un pôle a donné est appelé *ordre* de ce pôle. La preuve se fait par "déflation".)

• Calcul du coefficient d'un élément simple :

$$[z^n]\frac{c}{(z-a)^r} = c(-a)^{-r} \cdot a^{-n} \cdot \binom{n+r-1}{r-1} \sim c(-a)^{-r} \cdot a^{-n} \frac{n^{r-1}}{(r-1)!}.$$

(Découle du binome de Newton avec exposant négatif.)

[2] Ce à quoi on peut toujours se ramener par division !

ALGORITHME : f_n est une somme finie de termes de la forme

$$a^{-n}n^s \qquad (s \text{ entier} \geq 0),$$

où a est un pôle est s est $\leq$ l'ordre du pole diminué de 1.

Les a de plus petit module apportent donc une contribution en a^{-n} qui domine[3] les autres. En cas d'ex aequo, ce sont ensuite les ordres ples plus grand les plus grands qui importent. Ceci permet d'analyser simplement les coefficients de la plupart des fractions rationnelles qui se présentent en combinatoire.

EXEMPLES : Fibonacci et le nombre d'or. Que dire de $(1-z)^{-4}(1-2z)^{-3}(1-3z)^{-2}$? De $(1-z)^{-5}(1+z)^{-3}$? [Trouver la base de l'exponentielle et le degré du polynôme dans chaque cas. On ne demande pas les constantes.]

APPLICATIONS : Les dénumérants, comme par exemple

$$\frac{1}{(1-z)(1-z^2)(1-z^3)}$$

(réponse de l'ordre de n^2 à cause du pôle triple en $z = 1$). PLus généralement, les partitions en sommants $\leq r$: le coefficient est $\sim \dfrac{n^{r-1}}{r!(r-1)!}$. Partitions en au plus r sommants, en exactement r sommants (par la symétrie horizontale-verticale des escaliers).

Exercices non traités : Le codage d'un ensemble A par un ensemble C nécessite $a \leq c$ où $a = \text{card}(A)$ et $c = \text{C}$. Cas où C est l'ensemble des mots binaires : on cherche un codage succint dóbjets structurés (par exemple, les triangulations en $2n$ bits). Cas dual où A est l'ensemble des mots binaires et C un langage contraint : c'est la problématique duale di codage de canal (par un canal contraint) : exemple des messages recodés sans occurrence de $aaaa$. Les mots excluant un motif $\mathfrak{p}$ donné.

CONCLUSION : *Pour les fractions rationnelles on localise les pôles, on extrait les pôles dominant, on examine les ordres correspondants, on conclut quant à une forme $f_n \sim A^n\theta(n)$ (avec $A = 1/a$) où θ est un polynôme. Pour ces fonctions rationnelles, la forme asymptotique des coefficients est donc bien caractérisé par la position (donnant le taux exponentiel) et la nature (donnant le facteur subexponentiel) des pôles.*

[3]Noter que le rayon de convergence est alors nécessairement égal au module des pôles les plus proches de l'origine (sinon, la fraction rationnelle resterait finie dans un disque trop grand !).

3. L'analyse de singularités

Sous des conditions qu'on ne peut expliciter à ce stade[4] et qu'on appelera **SAC** [*Singularity Analysis Conditions*], on dispose d'une traduction qui généralise de façon très vaste l'analyse des fractions rationnelles. On considère d'abord le cas où le rayon de convergence est égal à 1.

En preambule, on commence par observer ce qui se passe pour $(1-z)^{-r}$ (r entier) et $(1-z)^{-1/2} = \sum \binom{2n}{n} 4^{-n} z^n$ [qui s'analyse par Stirling, comme pour les nombres de Catalan]. On voit sur tous ces cas au moins que

$$\boxed{\text{coeff } [z^n](1-z)^{-\alpha} \sim C_\alpha \cdot n^{\alpha-1}.}$$

On a $C_{1/2} = 1/\sqrt{\pi}$ et $C_r = 1/(r-1)!$.

Théorème d'analyse de singularité : *Sous conditions SAC, une* arroximation *de la fonction au point spécial*[5] 1

$$f(z) \underset{z\to 1^-}{\sim} (1-z)^{-\alpha}, \qquad \alpha \notin \{0, -1, -2, \ldots\},$$

se "transfère" en une estimation asymptotique des coefficients

$$f_n \equiv [z^n] f(z) \underset{n\to\infty}{\sim} \frac{n^{\alpha-1}}{\Gamma(\alpha)}.$$

La fonction Γ utilisée ici généralise la factorielle ($\Gamma(m) = (m-1)!$) et est définie par les deux règles :

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1}\, dt; \qquad \Gamma(s+1) = s\Gamma(s).$$

(La première règle vaut pour $\Re(s) > 0$.) Noter que $\Gamma(\frac{1}{2}) = \sqrt{\pi}$, ce qui est équivalent à l'intégrale classique "gaussienne" qu'on retrouvera plus tard : $\int_{-\infty}^{\infty} e^{-t^2/2}\, dt = \sqrt{2\pi}$.

$\rightsquigarrow$ La preuve nécessite les notions de base de fonctions analytiques (ou holomorphes) et n'est pas envisagée dans cet exposé. Voir *Analytic Combinatorics*, Chapitres IV [bases de la théorie] et VI [analyse de singularité], pour les curieux.

Le fait de considérer une fonction $g(z)$ de rayon de convergence R (au lieu de 1 précédemment) induit un facteur[6] R^{-n}. On retiendra ainsi (sous conditions SAC au voisinage de R) :

---

[4] Pour mémoire : "positivité des coefficients impliquant Pringsheim ; unicité de la singularité dominante (ici 1) ; prolongement analytique dans un Camembert et validité dans cette région de l'approximation de la fonction". Cf Chapitre VI de *Analytic Combinatorics*.

[5] Pour simplifier le rayon de convergence ici supposé égal à 1. Techniquement : une singularité !

[6] Car si $f(z) = g(Rz)$, alors $f(z)$ a rayon de convergence 1 (et le théorème s'y applique), tandis que $[z^n]f(z) = R^n [z^n] g(z)$.

Principe de transfert :

$$\boxed{g(z) \underset{z\to R^-}{\sim} C(1-z/R)^{-\alpha} \quad \Longrightarrow \quad [z^n]f(z) \underset{n\to\infty}{\sim} CR^{-n}\frac{n^{\alpha-1}}{\Gamma(\alpha)}.}$$

Observations. Il existe toute une panoplie de résultats du même acabit :
(*i*) on peut remplacer $\sim$ par O ou o ;
(*ii*) on peut prendre en compte des puissances de log, soit $L(z) = (\log(1-z)^{-1})^k$, qui se transfèrent en un facteur $L(n)$ additionnel pour les coefficients.
iii) Des développements asymptotiques complets sont possibles.
Examples. Les nombres de Fibonacci et les fractions rationnelles (on retrouve ce que l'on savait déjà). La fonction de Catalan. Les nombres harmoniques (on retrouve ce que l'on savait déjà).

• Les arbres unaires binaires. On part de $\mathcal{U} = \mathcal{Z} + \mathcal{Z}\mathcal{U} + \mathcal{Z}\mathcal{U}\mathcal{U}$. Donc $U(z)$ vérifie une équation quadratique et

$$U(z) = \frac{1-z-\sqrt{(1+z)(1-3z)}}{2z}.$$

On a $U_n \leq 3^n$ par codage par un alphabet de symboles fonctionnels $\{f_0, f_1, f_2\}$ et parcours préfixe. On admet que $R = \frac{1}{3}$. Il suffir alors d'observer que

$$U(z) \underset{z\to\frac{1}{3}}{\sim} 1 - c\sqrt{1-3z}$$

pour traduire en

$$U_n \underset{n\to\infty}{\sim} \frac{3^n}{\sqrt{n^3}}.$$

[Non traité, mais accesible de la même manière a partir de la BGF : Le nombre moyen de feuilles dans un arbre unaire-binaire : réponse $\sim n/3$.]

Conclusion. *La nature d'une fonction génératrice en sa "singularité" R (son rayon de convergence) nous livre, sous des conditions très générales, le facteur subexponentiel de ses coefficients. Il est remarquable quúne approximation en un tel point suffise à livrer l'asymptotique des coefficients.*

4. La loi gaussienne

On appelle *loi de Gauss* ou *loi normale* la loi de probabilité d'une variable aléatoire Y définie par

$$\Pr[Y \in (y, y+dy)] = g(y)dy, \qquad g(y) = \frac{1}{\sqrt{2\pi}}e^{-y^2/2}.$$

La densité de présence au voisinage de y est $g(y)$; cette fonction est une belle courbe en cloche. Une autre manière de dire est

$$\Pr[Y \leq y] = \Phi(y) \equiv \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{y} e^{-t^2/2}\,dt.$$

Le membre droit s'appelle la fonction d'erreur de Gauss[7]. Par extension $Z = \mu + \sigma Y$ est une variable gaussienne de moyenne μ et écart type σ. Une loi Gaussienne est assez "resserrée"autour de son centre : la probabilité est de respectivement $0.682, 0.954, 0.997$ d'observer une valeur à moins de $1, 2, 3$ écarts types.

La force de cette loi, découverte par De Moivre, Laplace et Gauss est son universalité dans les problèmes mettant en jeu la résultante d'un grand nombre de composantes aléatoires[8] plus ou moins indépendantes.

Theorème central limite[9] : *Soit $X_1, X_2, \ldots$ une suite de variables aléatoires indépendantes identiquement distribuées de moyenne μ et écart type σ. Les sommes $S_n = X_1 + X_2 + \cdots + X_n$, ou, plus proprement, leur version standardisée,*

$$S_n^\star = \frac{S_n - n\mu}{\sigma\sqrt{n}}$$

convergent vers la loi de Gauss au sens où, pour tout $y \in \mathbb{R}$,

$$\Pr\left[S_n^\star \leq y\right] \to \Phi(y),$$

lorsque $n \to \infty$.

NOTE. La preuve part de l'observation[10] que la fonction génératrice de probabilités [PGF] de S_n vaut $p(u)^n$ où $p(u)$ est la PGF de X_1. On joue alors avec la série génératrice des moments (ou transformée de Laplace) : en général, c'est

$$\lambda(s) = \mathbb{E}(e^{sX}).$$

Pour une variable discrète, on a $\lambda(s) = p(e^s)$ où $p(u)$ est la PGF. On peut alors calculer la Laplace d'une gaussienne ainis que la Laplace de S_n puis de $S_n^\star$. On vérifie la convergence en tout point $s = it$ avec $i = \sqrt{-1}$, ce qui, d'après un théoréme "de continuité" donne le résultat de convergence en loi. (On nage dans de l'analyse de Fourier en fait.)

EXERCICE. (non traité) Vérifier le théorème dans le cas du jeu à pile ou face équitable $(\frac{1}{2}, \frac{1}{2})$ où les probabilités sont $p_{n,k} := \frac{1}{2^n}\binom{n}{k}$ [loi de Bernoulli]. (Utiliser une analyse élémentaire : prendre pour simplifier $n = 2\nu$ et calculer le logarithme de $p_{2\nu,\nu+\ell}/p_{2\nu,\nu}$ pour $\ell = x\sqrt{\nu}$.) Ce cas correspond au paramètre qui vaut le nombre de lettres b dans un mot binaire aléatoire de longueur n.

CONCLUSION. *La loi de Gauss est universelle pour la résultante d'un grand nombre de facteurs indépendants.*

Lire pour se détendre le très joli texte historique de Bernard Ycart :

---

[7] En MAPLE : $\frac{1}{2}(1 + \mathrm{erf}(y/\sqrt{2}))$.

[8] Par exemple des erreurs de mesure dans des observations physiques ou géodésiques ; des jeux de hasard.

[9] Ou théorème de la limite centrale ou *Central Limit Theorem [CLT].*

[10] Lemme : La PGF d'une somme de variables aléatoires indépendantes est égale au produit des PGF des variables entrant dans la somme : $p_{X+Y}(u) = p_X(u)p_Y(u)$. La preuve est facilitée si l'on remarque que $p(u) \equiv \mathbb{E}(u^X)$, mais un calcul direct est possible. Rappelons que X et Y sont indépendantes si $\Pr(X = x, Y = y) = \Pr(X = x)\Pr(Y = y)$.

`http ://www-lmc.imag.fr/lmc-sms/Bernard.Ycart/emel/articles/etoiles/etoiles.html`
également accessible depuis Google avec recherche : `bernard ycart meridien`.

5. Loi de Gauss et combinatoire analytique

Il ne s'agit ici que de quelques repères pour la suite. Une grande quantité de développements asymptotiques s'obtiennent à partir d'OGF ou EGF qui sont des fonctions d'une variable par l'analyse de singularités. Ceci nous a conduit à des estimations asymptotiques très utiles concernant les suites de dénombrement, comme vu dans les sections précédentes.

Lorsqu'on examine des *paramètres*, on cherche des lois de probabilité valables asymptotiquement. Celles-ci nous fournissent des informations asymptotiques sur des suites à deux indices $f_{n,k}$ associées à leur BGF $f(z,u)$. La loi gaussienne se retrouve asymptotiquement très souvent—notamment concernant les paramètres érités ou additifs. Parmi les exemples de paramètres vus en cours, citons ainsi :

> Le nombre de sommants dans les compositions ou partitions d'entiers ; le nombre de classes (blocs) dans une partition d'ensemble ; le nombre de feuilles dans un arbre [Catalan, binaire, etc].

Voici brièvement un schéma heuristique qui explique cet état de fait.

Principe de la loi limite Gaussienne en combinatoire analytique.

– On part d'une fonction bivariée (BGF) baptisée $f(z,u)$. Rappelons que $f(z,1)$ dénombre les objets combinatoires de base. On suppose que l'analyse de $f(z,1)$ peut être effectuée par une forme d'analyse de singularité, de sorte que
$$f_n = [z^n]f(z,1) \sim C\rho^{-n}n^{\alpha-1}.$$

– On examine ensuite $f(z,u)$ pour u dans un petit voisinage de 1. Soit alors $\rho(u)$ le rayon de convergence de $f(z,u)$ à u fixé. Si l'analyse de singularité s'étend à ces cas, on obtient une bonne estimation :
$$f_n(u) = [z^n]f(z,u) \sim C(u)\rho(u)^{-n}n^{\alpha-1}.$$
En particulier la PGF du paramètre χ associé à $f(z,u)$ vérifie :
$$\frac{f_n(u)}{f_n(1)} \sim \frac{C(u)}{C(1)} \cdot \left(\frac{\rho(1)}{\rho(u)}\right)^n.$$

– Dans ces conditions, tout se passe (analytiquement) au membre droit comme si on avait une décomposition (S_n est χ appliqué aux objets de taille n)
$$S_n = A + R_1 + \cdots + R_n,$$
où A est une variable de PGF $C(u)/C(1)$ et chaque R_j a pour PGF $\rho(1)/\rho(u)$. On conclut par un raisonnement analogue à la preuve du Théorème Central Limite Classique[11].

[11]Ceci cache un théorème dit *Théorème des Quasi-Puissances* : si la PGF de S_n ressemble à une puissance $n$ème, il y a convergence en loi vers une gaussienne, lorsque $n \to \infty$ [au sens du CLT].

En termes plus pompeux, la loi gaussienne apparaît comme résultant d'un développement perturbatif uniforme en une singularité et d'un théorème dit des Quasi-Puissances qui est très analogue dans son esprit au CLT.

Conclusion. *Pour des raisons analytiques maîtrisables, on est en droit d'attendre très souvent l'apparition de lois asymptotiquement Gaussiennes pour les paramètres additifs de très grandes structures combinatoires.*