ÉVALUATION DE PROTOCOLES DE COMMUNICATION: ASPECTS MATHÉMATIQUES

PHILIPPE FLAJOLET (*)
INRIA, Rocquencourt
78150-Le Chesnay

L'idée a germé, il y a une quinzaine d'années, de faire communiquer un grand nombre de stations par l'intermédiaire d'un canal partagé. D'où l'éclosion de réseaux locaux dont la mise en place pose des problèmes algorithmiques délicats. Cette conférence se propose de montrer la variété des outils mathématiques nécessaires à l'évaluation des protocoles (algorithmes) probabilistes utilisés pour gérer la communication. On y retrouve des techniques liées à l'analyse d'algorithmes classique, à l'analyse combinatoire, aux modèles probabilistes discrets et continus, à la théorie analytique des nombres ou encore aux équations fonctionnelles.

1. Contexte historique

C'est sous le chaud soleil de l'archipel d'Hawaï que commence l'histoire, vers la fin des années soixante. A cette époque, l'Université d'Hawaï est répartie sur plusieurs campus aux noms évocateurs de Manoa, Hilo, Oahu, Kauai et Maui. En septembre 1968, fut conçu, sous l'impulsion d'Abramson (Hawaï), le plan de partager les ressources informatiques, et c'est de là que naîtra le premier réseau informatique radio, baptisé du nom d'ALOHA.

Les interconnections classiques de systèmes utilisaient à l'époque exclusivement des liaisons point-à-point, inspirées de la téléphonie classique. Il s'agissait au contraire ici d'organiser la communication dans un contexte très décentralisé, et c'est ainsi, après des tâtonnements divers, que naquit le premier réseau ALOHA. L'idée de base était tout simplement que tout site – nous emploierons aussi le mot de *station* – émettait directement les messages qu'elle avait à transmettre sur le canal radio partagé par l'ensemble. En cas de "brouillage" – nous dirons aussi *collision* – né d'une émission simultanée, chaque station essaye de nouveau ultérieurement. Le nom du réseau, ALOHA, résume bien cette approche "libertaire" du problème de la communication, car il signifie *bienvenue* en Hawaïen:

> *Chaque station est libre d'émettre dès qu'elle en a envie, et l'on règle plus tard les conflits éventuels.*

C'est alors qu'intervint une idée simple, mais *osée* dans le contexte de l'époque, l'idée de départager les opposants par tirage au sort:

> *Chaque station tire aux dés, honnêtement, pour déterminer quand elle va essayer de nouveau de lancer son message.*

On compte ainsi sur les *probabilités* pour régler les problèmes. Le mode de tirage, l'algorithme, qui détermine les essais est appelé de nos jours un *protocole*; un protocole sera d'autant plus efficace

(*) Conférence présentée à la Journée Annuelle de la Société Mathématique de France, Paris, le 23 Janvier 1988.

qu'il ne crée pas d'engorgement du système et qu'en "moyenne" les délais ne sont pas trop élevés. ALOHA dont le principe sera décrit plus en détail est un protocole particulier:

> ALOHA: *En cas de conflit, on ré-essaye, à chaque instant et jusqu'au succès final, avec une probabilité fixe* $p \in [0, 1]$.

Des premières analyses, en grande partie heuristiques, furent faites lors de la conception d'ALOHA afin d'en déterminer les caractéristiques. On pensait alors qu'il pouvait supporter un taux d'arrivée de messages (défini comme le nombre moyen d'arrivées par tranche unitaire de temps) voisin de $e^{-1} \approx 37\%$.

ALOHA donna semble-t-il, pour l'essentiel, satisfaction dans le contexte dans lequel il était utilisé, à savoir un petit nombre de stations et un trafic sporadique. Cependant, les expériences – simulées ou réelles – posaient quelques questions sur sa robustesse, dans le cas d'un trafic plus intense ou de réseaux comprenant un plus grand nombre de stations. De tels réseaux commençaient en effet à voir le jour au début des années soixante-dix. L'idée de Metcalfe (Harvard) qui devait donner lieu au protocole ETHERNET fut que cette instabilité apparente était sans doute liée au caractère peu *adaptatif* du protocole ALOHA. L'idée à la base d'ETHERNET, lequel connaît un succès considérable se comptant en dizaines de milliers de réseaux[†] était d'ajuster la variable p en fonction du trafic:

> ETHERNET: *En cas de conflit, on ré-essaye, à chaque instant et jusqu'au succès final, avec une probabilité variable* $p \in [0, 1]$*, où* p *est divisée par 2 à chaque tentative infructueuse due à une collision.*

Les doutes sur la stabilité d'ALOHA devaient être justifiés peu après. Plusieurs probabilistes appliqués (Fayolle *et al.*, Paris) obtinrent en effet le théorème suivant: ALOHA *est instable*. Plus précisément sous un modèle de flot d'arrivées Poissonnien de taux λ, le taux de message acheminés avec succès tend vers 0 quelque soit λ non nul, les délais et le nombre de message en attente tendent vers l'infini! Le même problème, qui se trouvait posé pour ETHERNET ne devait être résolu que 10 ans plus tard par Aldous (Berkeley): ETHERNET *est aussi instable*. Les méthodes utilisées pour l'obtention de ces résultats reposent sur la théorie des chaînes de Markov et des martingales. Des analyses du temps de déstabilisation (Ruget, Paris; Greenberg *et al*, Murray Hill, dans le cas d'ALOHA) résultent de la théorie des grandes déviations: ces temps sont très important à très faible charge, où le système est quasi-stable, mais deviennent très réduits lorsque la charge augmente et le système se congestionne très rapidement. Ainsi se trouvent réconciliées théorie (instabilité) et pratique (comportement utilisable à charge modérée).

Il restait la question essentielle de l'existence d'un protocole stable. C'est vers 1977 qu'indépendamment, Capetanakis (MIT) et Tsybakov-Mikhailov (Moscou) découvrirent le premier algorithme stable. Celui-ci, appelé *protocole en arbre* (ou CTM d'après les initiales de ses inventeurs), est très simple:

> ARBRE: *En cas de collision entre un groupe de station, chaque station effectue un tirage à pile-ou-face; les stations se répartissent ainsi en 2 groupes et chaque groupe résout, indépendamment de l'autre et récursivement, ses collisions.*

Curieusement, ce protocole qui procède par dichotomie récursive ouvre des possibilités de modélisation analytique *exacte* plus complètes que les protocoles "linéaires" précédents. En tout cas, il apparut que *le protocole en arbre est stable jusqu'à des taux d'arrivée voisins de* 35%.

Tous les espoirs étaient-ils permis? Pouvait-on approcher une transmission parfaite à 100%? Vers 1978, Pippenger (Yorktown Heights) montre, par des arguments de théorie de l'information, que "tout" protocole est nécessairement instable au delà de 75%. Ce résultat fut amélioré, et il y a de bonnes raisons de conjecturer désormais qu'on ne peut dépasser une efficacité du canal de 52%.

[†] En fait ETHERNET désigne une norme industrielle, fondée sur le protocole que nous décrivons.

Dans le même temps, des modifications apportées au protocole en arbre permettaient d'atteindre des taux de stabilité de 48% (Gallager, MIT). On disposait ainsi de méthodes quasi-optimales.

Une bonne partie de cet exposé est dédiée à la présentation de l'analyse du protocole en arbre, à l'histoire elle-même quelque peu chaotique. Supposons que n stations entrent en compétition, et soit l_n le temps moyen de résolution de leur collision initiale. On observe numériquement, ce que confirme un argument probabiliste "plausible", que $l_n/n \to c$ lorsque $n \to \infty$, où c vaut environ $2,88$. Vvedenskaya (Moscou) observa la première, par des calculs numériques très minutieux vers 1980, que l_n/n fluctue asymptotiquement au niveau de la cinquième décimale. On se rendit compte peu après que ce phénomène avait été démontré par Knuth (Stanford) sur des suggestions de De Bruijn (Eindhoven), dans un tout autre contexte – celui de l'analyse de certaines structures de données – dix ans auparavant! Or, si l'incidence pratique directe de cette cinquième décimale était faible, les calculs de l'*ordre de grandeur* de la variance (en $O(n)$) étaient invalidés et beaucoup d'"évaluations" étaient à revoir.

Que le mathématicien pur se rassure! Les choses sont désormais rentrées dans l'ordre. Ces analyses en moyenne, variance et même distributions limites sont désormais bien comprises. Les paramètres en jeu s'analysent par des méthodes liées au traitement d'équations fonctionnelles aux différences (linéaires et non linéaires) ainsi qu'à la transformation de Mellin, introduite comme on sait par Riemann en rapport avec le théorème des nombres premiers. Les pourcentages qui ont essaimé cette introduction sont des racines de diverses équations transcendantes, et non pas des quantités issues de l'analyse numérique. L'étude de variance, par exemple, met en jeu des quantités qui se simplifient (Kirschenhoffer *et al.*, Vienne) grâce à des identités issues de la théorie des formes modulaires et dues à Ramanujan etc.

2. Le canal partagé

Le modèle de base suppose un temps discret $t = 0, 1, 2, \ldots$, A l'instant t, selon une loi que l'on suppose ici de Poisson avec taux λ, arrive un nombre variable A de messages:

$$\Pr\{A = k\} \equiv a_k = e^{-\lambda}\frac{\lambda^k}{k!}. \tag{2.1}$$

On sait, par un résultat classique et élémentaire, que ce modèle approche un processus d'arrivées (dit de Bernoulli), dans lequel N acteurs (N grand) deviennent indépendamment actifs avec probabilité λ/N. Le modèle poissonien est ainsi raisonnablement justifiable dans le cas de "grands" réseaux à trafic sporadique.

Dans le cas qui nous intéresse, chaque message est issu d'une station qui applique un certain algorithme probabiliste dit *protocole*. Le déroulement du protocole à l'instant t par une station est fondé sur la situation de ses arrivées et sur l'état "observable" du canal aux instants précédents $0, 1, \ldots, t-1$. A un instant quelconque, l'état observable, qui est accessible à toutes les stations, représente une vision partielle de l'état réel du canal réduite aux 3 possibilités suivantes[†]:

- **0 :** Aucune station n'a tenté d'émettre; il y silence sur le canal.
- **1 :** Un seul message a été émis; il y a transmission avec succès.
- **2^+:** Deux messages ou plus sont entrés en collision; il y a brouillage et les messages entrés en collision devront être retransmis à une époque ultérieure. Dans ce cas, la multiplicité de la collision n'est pas déterminable.

Le tableau suivant représente une activité possible de canal (les lettres identifiant indifféremment des messages ou des stations) et la suite des états observables.

[†] On ne sait ainsi compter que par 0, 1, beaucoup! Cette contrainte est de nature électrique.

t:	0	1	2	3	4	5	6	7	8	9	10	11
État:	–	A	–	B,C	–	C	B,D,E	–	B,D	D	B	E
Observable	0	1	0	2^+	0	1	2^+	0	2^+	1	1	1

Sur l'exemple, B arrive en $t = 3$ où il entre en collision avec C (qui ré-émet avec succès en $t = 5$), refait une tentative en $t = 6$ (collision avec D et E), puis $t = 8$ (collision avec D encore), puis finit par passer en $t = 10$.

3. Les protocoles Aloha et Ethernet

Le protocole le plus simple est le protocole ALOHA déjà mentionné.

Chaque message est transmis dans la tranche de temps suivant immédiatement son arrivée.
*En cas de conflit, la politique d'*ALOHA *consiste à retransmettre à chaque instant avec probabilité p, et ce jusqu'au succès final.*

Soit $N(t)$ la cardinalité de la population de messages en attente à l'instant t. On désigne par $P_{k,\ell}$ les probabilités de transition

$$P_{k,\ell} = \Pr\{N(t+1) = \ell \mid N(t) = k\}. \tag{3.1}$$

Ces probabilités sont clairement indépendantes de t, de sorte que le comportement d'ALOHA est décrit par une *chaîne de Markov* à états dénombrables et temps discret. Il est facile de caractériser les probabilités de transition de cette chaîne de Markov, a_j désignant la probabilité de j arrivées:

$$\begin{cases} P_{k,k-1} & = a_0 kp(1-p)^{k-1} \\ P_{k,k} & = a_0(1 - kp(1-p)^{k-1}) + a_1(1-p)^k \\ P_{k,k+1} & = a_1(1-(1-p)^k) \\ P_{k,k+j} & = a_j \qquad (j \geq 2). \end{cases} \tag{3.2}$$

Par exemple la première de ces équations se lit: "Il y a transmission avec succès lorsqu'il n'y a pas d'arrivées et que l'une des stations déjà en attente transmet".

La question de la stabilité d'ALOHA fut pour la première fois résolue par Fayolle *et al* [1975], [1977]: ALOHA *est instable.* L'énoncé qui suit est dû à Kelly *et al* [1987] ainsi que Ross [1987]:

THÉORÈME 1. *Avec probabilité 1, le nombre de messages transmis avec succès par le protocole* ALOHA *est fini.*

En d'autres termes, le protocole fonctionne "un certain temps" puis finit par s'engorger ne laissant plus passer aucun message, par suite de collisions répétées de plus en plus nombreuses.

PREUVE. Le terme d'état réfère comme précédemment au nombre de messages en attente au début d'une période de temps. On considère la variable aléatoire I_k qui vaut 1 si le premier départ de l'état k se fait vers l'état $k-1$, et 0 sinon. On convient également que $I_k = 0$ si l'état k n'est jamais atteint. Par exemple, si la suite d'états est $0, 1, 4, 4, 3, 6, 5, 8, 9, 9, \ldots$, alors $I_4 = 1$ tandis que $I_5 = 0$.

Considérons la quantité $Q = \sum_{k \geq 1} I_k$. On a alors

$$\begin{aligned} \mathbf{E}\{Q\} = \sum_{k\geq 1} \Pr\{I_k = 1\} &\leq \sum_{k \geq 1} \Pr\{I_k = 1 \mid k \text{ est visité}\} \\ &= \sum_{k\geq 1} \frac{P_{k,k-1}}{1 - P_{k,k}} \end{aligned} \tag{3.3}$$

D'après la forme des probabilités, on se convainc aisément que $\mathbf{E}\{Q\} < \infty$.

Le théorème de Borel-Cantelli (loi zéro-un) s'énonce: *Soit $\mathcal{I}_k$ une suite d'évènements indépendants. Alors, presque sûrement, le nombre d'évènements réalisés est fini ou infini selon que $\sum_k \Pr\{\mathcal{I}_k\}$ converge ou diverge.*

Il en résulte qu'avec probabilité 1, $Q = \sum I_k$ est fini. Le nombre d'états quittés sur une transmission avec succès a ainsi une valeur finie N avec probabilité 1. Lorsque le nombre de messages dans le système dépasse N (ceci se produit nécessairement avec probabilité 1, à cause de la propriété Markovienne), le système ne génère plus aucune transission avec succès. ■

Ce résultat très général est valable non seulement pour des arrivées poissoniennes, mais encore pour toute loi d'arrivée non triviale (telle que $a_0 + a_1 < 1$). Cette instabilité se manifeste pratiquement par un engorgement du canal non résorbable après une pointe de trafic importante. Le résultat peut être raffiné de diverses manières. Il apparaît que le système possède un mode d'équilibre transitoire *"pseudo-stable"*, et qu'en choisissant une valeur de p très petite, le temps de déstabilisation peut être très grand. C'est ainsi qu'en utilisant la théorie des grandes déviations d'Azencott et Ruget [1977], Greenberg et Weiss [1986] ont montré que $\lambda = 0,1$ et $p = 0,01$ conduisent à des temps de déstabilisation voisins de $\approx e^{346}$. La sous-utilisation du canal est cependant évidente, car dans ce cas, après une collision, le temps moyen de retransmission est égal à 100, ce malgré un taux d'arrivées peu important (10%).

Le protocole ETHERNET dû à Metcalfe [1976] vise à éliminer ces effets de congestion, en *adaptant* les probabilités de retransmission à la charge instantanée.

> *Chaque message est transmis dans la tranche de temps suivant immédiatement son arrivée. En cas de conflit, la politique de retransmission d'*ETHERNET *consiste à retransmettre jusqu'au succès avec probabilité $p_i = 2^{-i}$ où i est le nombre de collisions déjà subies par le message.*

Ainsi, si M arrive et entre en collision immédiatement, on utilise la probabilité de retransmission $p_1 = 1/2$. Si, lors de la tentative suivante de retransmission, il y a de nouveau collision, on utilise $p_2 = 1/4$ etc.

Le problème de la stabilité d'ETHERNET est resté ouvert une dizaine d'années avant d'être résolu par Aldous [1987].

THÉORÈME 2. *Le protocole* ETHERNET *est instable: pour tout $\lambda > 0$, $N(t)$ désignant le nombre de messages transmis avec succès dans l'intervalle de temps $[0, t]$, on a presque sûrement $N(t)/t \to 0$*

Ainsi le taux de transmission tend-il vers 0 lorsque $t \to \infty$. La plupart des messages attendent des temps de plus en plus longs par suite de collisions répétées.

On observe que l'état du système à un instant quelconque t est représenté par un vecteur $X(t) = (X_1, X_2, \ldots)$ dans lequel X_i représente le nombre de messages en attente ayant déjà subi i collisions. Les probabilités de transition se calculent aisément en fonction de l'état de départ et définissent une chaîne de Markov à espace d'état dénombrable. Cette chaîne est transiente. La preuve est relativement élémentaire (propriétés des chaînes de Markov et martingales) mais délicate. Elle repose sur l'étude du comportement de la fonction

$$f(X(t)) = \sum_{i \geq 1} 2^{-i} X_i.$$

Lorsque $\lambda > \log 2$, Kelly *et al.* [1985,1987] ont montré qu'ETHERNET était instable en un sens plus fort, comparable au phénomène de congestion d'ALOHA (*cf* Théorème 1):

THÉORÈME 3. *Lorsque le taux d'arrivées vérifie $\lambda > \log 2 = 0,69$, le nombre de messages transmis par* ETHERNET *est fini avec probabilité 1.*

4. Un protocole stable: Le protocole en arbre

Capetanakis [1979] ainsi que Tsybakov *et al* furent les premiers à découvrir un protocole stable. Le principe de cet algorithme appelé Algorithme en Arbre ou Algorithme en Pile est le suivant:

> *Lorsqu'un groupe G de stations entrent en collision, le groupe se sépare en deux groupes G_0 et G_1, chaque $g \in G$ décidant de son appartenance à G_0 ou G_1 par tirage au sort. Le groupe G_0 transmet tout d'abord et résout récursivement ses collisions. Le groupe G_1 transmet lorsque toutes les collisions entre éléments de G_0 ont été résolues.*

Un déroulement de cet algorithme de partage récursif est représenté naturellement par un arbre (voir Figure 1).

Figure 1. Un déroulement possible du protocole en arbre pour un groupe $G = \{A, B, C, D, E\}$ et sa réalisation temporelle.

En fait, il existe deux modes permettant de tenir compte de la possibilité de nouvelles arrivées:

1. *Accès bloqué*: Après une collision initiale d'un groupe G, les nouveaux arrivants attendent que la résolution de G soit terminée pour transmettre. Il se constitue ainsi un groupe G^* qui résout ses collisions par le même algorithme etc. On appelle *session* l'intervalle de temps correspondant à la résolution de collisions entre un groupe de stations.
2. *Accès libre*: Tout message est transmis dès qu'il arrive. Il convient alors de modifier la définition de l'algorithme: Si G se sépare en G_0 et G_1, alors on résout d'abord $G_0' = G_0 + X$, puis $G_1' = G_1 + Y$ où X et Y représentent de nouvelles arrivées (aux débuts de G_0 et G_1).

Nous allons considérer dans cette section le cas du protocole avec *accès bloqué* où le temps est subdivisé en sessions, et plus précisément, nous intéresser à la durée L_n d'une session correspondant à un groupe initial de n stations. Il s'agit d'une variable aléatoire dont on peut chercher moyenne, variance ou même distribution.

Bien que ce protocole récursif paraisse plus compliqué que les protocoles “linéaires” précédents, il est néammoins susceptible de *modélisation analytique* exacte. Les deux premiers théorèmes, dus à Knuth [1973] et De Bruijn et bien antérieurs au protocole en arbre, avaient pour origine l'analyse de la structure de données “arbre digital” en informatique.

Implémentation. La formulation récursive associée à un arbre de résolution est la plus claire conceptuellement, et aussi celle qui se prête le plus directement à l'analyse. Il n'est cependant pas clair a *priori* qu'un tel protocole soit implémentable, en utilisant uniquement les observables du canal. Pour obtenir ce résultat (essentiel), on note d'abord que tout arbre ayant n sommets binaires comporte nécessairement $n+1$ sommets externes. De la sorte, le protocole en arbre peut être implémenté, chaque station mettant à jour un "indice de priorité" qui lui est propre et qui est un entier positif ou nul. Lors de son arrivée, le message reçoit la priorité 0 qui signifie, en général, la permission d'émettre. Lorsqu'il a la priorité 0, il la conserve s'il tire *pile*, sinon, il descend à la priorité 1. Ensuite, un message ayant priorité $j \geq 1$ est en attente. Sur une collision, il effectue la mise à jour $j \leftarrow j+1$; sur un silence où une transmission avec succès, il effectue $j \leftarrow j-1$. ■

On suppose ici les tirages indépendants et non biaisés ($\Pr\{g \in G_0\} = \Pr\{g \in G_1\} = \frac{1}{2}$).

Théorème 4. *Le temps moyen l_n de résolution d'une collision de multiplicité n par le protocole en arbre – dans la version à accès bloqué – est donné par*

$$l_n = \mathbf{E}\{L_n\} = 1 + 2\sum_{k\geq 0} 2^k \big[1 - (1-\frac{1}{2^k})^n - \frac{n}{2^k}(1-\frac{1}{2^k})^{n-1}\big]. \tag{4.1}$$

Preuve. Soit K la variable aléatoire représentant l'effectif du premier groupe G_0, sachant que $|G| = n$. Il s'agit d'une variable de Bernoulli, et l'on a

$$\Pr\{K = k\} = \frac{1}{2^n}\binom{n}{k}. \tag{4.2}$$

La nature récursive du processus de partitionnement conduit à la récurrence entre variables aléatoires

$$L_n = 1 + L_K + L_{n-K} \qquad (n \geq 2); \qquad L_0 = L_1 = 1. \tag{4.3}$$

En prenant les espérances dans (4.3), et en utilisant (4.2), l'on obtient, pour $n \geq 2$:

$$l_n = 1 + \frac{1}{2^n}\sum_{k=0}^{\infty}\binom{n}{k}(l_k + l_{n-k}). \tag{4.4}$$

Cette récurrence permet de calculer de proche en proche les l_n qui sont des nombres rationnels. L'idée de base pour obtenir une forme explicite consiste à introduire la série génératrice exponentielle des espérances,

$$l(z) = \sum_{n\geq 0} l_n \frac{z^n}{n!},$$

et un calcul simple montre que la recurrence (4.4) se traduit par une *équation fonctionnelle aux différences* pour $l(z)$, à savoir

$$l(z) = e^z - 2 - 2z + 2e^{z/2} l(\frac{z}{2}). \tag{4.5}$$

Une équation fonctionnelle telle

$$f(z) = a(z) + b(z) f(\frac{z}{2}) \tag{4.6}$$

se résout formellement par itération:

$$f(z) = a(z) + b(z)a(z/2) + b(z)b(z/2)a(z/4) + b(z)b(z/2)b(z/4)a(z/8) + \cdots \tag{4.7}$$

L'application de ce schéma à l'équation de base (4.5) relayée par un développement de Taylor élémentaire fournit la forme explicite de l_n. ■

La stabilité de l'algorithme en arbre (avec accès bloqué) est déterminée par le comportement de l_n/n, quantité qui représente, dans la terminologie des files d'attente un "temps de service moyen". D'après cette théorie, on s'attend à avoir stabilité lorsque le taux de service est supérieur au taux d'arrivée, et instabilité sinon. Il est ainsi nécessaire d'évaluer le comportement asymptotique de l_n/n, lequel réserve quelques surprises.

On part de l'approximation exponentielle $(1-a)^n \approx e^{-na}$, qui appliquée à (4.1) fournit

$$l_n = 2nF(n) + O(\sqrt{n}) \qquad \text{où} \qquad F(x) = \sum_{k\geq 0} f(x/2^k), \quad f(x) = \frac{1}{x}[1-(1+x)e^{-x}]. \tag{4.8}$$

Ainsi le comportement asymptotique de l_n se ramène-t-il à l'étude de sommes de type $\sum_k f(x/2^k)$. La difficulté provient de *fluctuations périodiques* dont la mise en évidence se fait par la *transformation de Mellin*, outil classique de théorie analytique des nombres introduit par Riemann.

LEMME 1. *Soit $f(x)$ une fonction analytique pour $x \geq 0$, vérifiant $f(0)=0$ et telle que $f(x) = x^{-1} + O(e^{-\alpha x})$ à l'infini. La fonction $F(x) = \sum_{k\geq 0} f(x/2^k)$ possède lorsque $x \to \infty$ un développement asymptotique de la forme*

$$F(x) = \frac{1}{\log 2}\int_0^\infty f(t)\,\frac{dt}{t} + P_f(\log_2 x) + \frac{1}{x} + O(\frac{1}{x^M}), \tag{4.9}$$

où M est un entier arbitraire et $P_f(u)$ représente une série de Fourier (dépendant de f) de valeur moyenne nulle.

PREUVE. La transformé de Mellin d'une fonction $g(x)$, notée $g^*(s)$ est définie par

$$g^*(s) = \int_0^\infty g(x)x^{s-1}\,dx. \tag{4.10}$$

On vérifie de manière élémentaire que, dans le cas de $F(x) = \sum_{k\geq 0} f(x/2^k)$, on a

$$F^*(s) = \frac{f^*(s)}{1-2^s}. \tag{4.11}$$

Il existe une correspondance classique [Doetsch 1955] entre comportement asymptotique de $g(x)$ et singularités de la transformé $g^*(s)$. Ainsi, le fait que $\zeta(s)$ ait résidu 1 en $s=1$ "correspond" au coefficient 1 devant $x/\log x$ dans le théorème des nombres premiers et les zéros complexes de $\zeta(s)$ (de partie réelle 1/2?) sont liés aux fluctuations (en $O(x^{1/2})$?) des termes d'erreur dans le comportement de la fonction $\pi(x) = \sum_{p<x} 1$, la sommation étant effectuée sur les p premiers.

Cette correspondance fondamentale se vérifie à partir de la formule d'inversion de type Fourier

$$g(x) = \frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty} g^*(s)x^{-s}\,ds \tag{4.12}$$

au moyen d'un calcul de résidus. En effet, si $g^*(s)$ n'a que des pôles simples et est bien conditionnée, on tire de (4.12) le développement asymptotique

$$g(x) \sim \sum_{\Re(\tau)>c} \mathrm{Res}[g^*(s), s=\tau]\cdot x^{-\tau}.$$

Les fluctuations périodiques sont ici liées aux pôles complexes en $s = \chi_k = 2ik\pi/\log 2$ de $1/(1-2^s)$. ∎

Dans le cas de la fonction $F(x)$ qui intervient dans l'analyse du protocole à accès bloqué, la transformée de Mellin de $f(x)$ s'exprime au moyen de la fonction Gamma: $f^*(s) = -s\Gamma(s-1)$.

L'application du Lemme 1 à l_n fournit immédiatement:

Théorème 5. *Le temps moyen de résolution d'une n-collision par le protocole en arbre à arrivées bloquées s'estime asymptotiquement par*

$$l_n \sim \frac{2}{\log 2} n + nP(\log n) + o(n), \tag{4.13a}$$

où $P(u)$ fluctue avec une amplitude inférieure à 10^{-5}.

Le comportement asymptotique de l_n est donc entièrement caractérisé et $l_n \approx 2,8853n$. La série de Fourier $P(u)$ possède une forme explicite où interviennent les valeurs de la fonction Γ le long de l'axe imaginaire:

$$P(u) = -\frac{2}{\log 2} \sum_{k \in \mathbf{Z} \setminus \{0\}} \chi_k \Gamma(\chi_k - 1) e^{2ik\pi u} \qquad \text{où} \qquad \chi_k = \frac{2ik\pi}{\log 2} \tag{4.13b}$$

Théorème 6. *Le protocole en arbre à arrivées bloquées est stable pour des taux d'arrivées $\lambda < \lambda_{\max} - \epsilon$ et instable pour des taux d'arrivées $\lambda > \lambda_{\max} + \epsilon'$ où $\lambda_{\max} = \log 2/2 = 0,34657$ et $\epsilon, \epsilon' < 10^{-5}$.*

Preuve. Soient $\lambda_{\max} - \epsilon$ et $\lambda_{\max} + \epsilon'$ les quantités $\liminf$ et $\limsup$ de n/l_n. D'après ce qui précède, ϵ et ϵ' sont inférieurs à 10^{-5}.

Soit S_j le nombre de stations au début de la j-ième session, et $A(v)$ une VA de Poisson d'intensité v. On a alors la relation Markovienne

$$S_{j+1} = A(\lambda L_{S_j}). \tag{4.14}$$

Montrons par exemple la stabilité pour $\lambda < \lambda_{\max} - \epsilon$. On utilise un argument de "dérive" (*drift*), ou Lemme de Pakes. On a

$$\mathbf{E}\{S_{j+1} - S_j \mid S_j\} = \lambda l_{S_j} - S_j, \tag{4.15}$$

et cette espérance est négative dès que S_j est assez grand. En terme concret, la chaine de Markov associée aux S_j est ergodique car on se trouve "ramené" vers de plus petites valeurs pour S_{j+1}. ∎

La région de stabilité du protocole en arbre est ainsi (pratiquement) complètement caractérisée, et l'on a obtenu un premier protocole stable jusquà $\lambda = 0,346$.

Plusieurs résultats intéressants se greffent sur cette analyse. Notamment Jacquet et Régnier [1987] ont montré l'existence d'une loi limite pour L_n.

Théorème 7. *Soit σ_n^2 la variance de L_n. La variable normalisée $L_n^* = (L_n - l_n)/\sigma_n$ possède une distribution qui converge vers une loi gaussienne $\mathcal{N}(0;1)$ lorsque $n \to \infty$.*

Preuve. On se contentera de quelques indications. La nature récursive du processus de partitionnement conduit à une *équation fonctionnelle non-linéaire à deux variables* pour une série génératrice double des probabilités $\Pr\{L_n = k\}$:

$$P(z,u) = uP(z/2,u)^2 + (1-u)(1+z) \qquad \text{avec} \qquad P(z,u) = e^{-z} \sum_{k,n \geq 0} \Pr\{L_n = k\} u^k \frac{z^n}{n!}. \tag{4.16}$$

Il s'agit donc de résoudre un double problème d'inversion, l'équation (4.16) n'ayant pas de solution explicite.

On applique d'abord une méthode de quasi-linéarisation à (4.16), en considérant $L(z,u) = \log P(z,u)$. L'utilisation de la transformation de Mellin permet d'obtenir le comportement de

$L(z,u)$ (donc $P(z,u)$) lorsque $u = e^{it}$. On trouve alors que la quantité $P(z, e^{it})$ convenablement normalisée tend vers la fonction caractéristique (transformé de Fourier) d'une distribution gaussienne. Le résultat de cette première analyse s'interprète directement par le théorème de continuité des fonctions caractéristiques (Lévy): lorsque N est une VA de Poisson de grand paramètre, la distribution de L_N normalisée tend vers une loi Gaussienne.

Il reste alors à passer du cas Poisson au cas Bernoulli. Ceci utilise les estimations précédentes de $P(z,u)$ et un calcul de coefficients de $[z^n]$ dans $P(z,u)$ par la méthode de col. L'on peut alors conclure par le théorème de continuité. ■

En passant, la preuve nécessite d'établir un résultat non trivial, à savoir l'ordre de grandeur de σ_n qui est en $O(n)$. L'estimation précise suivante est due à Kirschenhoffer *et al* [1987].

THÉORÈME 8. *La variance de L_n vérifie*

$$\sigma_n^2 = \frac{2n}{\log 2}\Big[\frac{1}{2} - \frac{1}{\log 2} - 2\sum_{j\geq 1}\frac{(-1)^j}{2^j-1} + Q(\log_2 n)\Big] + O(1) \approx 3,384n \tag{4.17}$$

où $Q(u)$ représente une fonction périodique avec $|Q(u)| < 10^{-4}$.

PREUVE. La difficulté provient ici de l'annulation des termes en $O(n^2)$ dans la différence entre $\mathbf{E}\{L_n^2\}$ et $\mathbf{E}\{L_n\}^2$. Il est en particulier nécessaire d'évaluer la valeur moyenne du *carré* de la fonction $P(u)$ qui apparaît dans les équations (4.13), laquelle s'exprime (cf (4.13)) au moyen de la quantité

$$V = \sum_{k\neq 0} |\chi_k|^2 |\Gamma(\chi_k - 1)|^2. \tag{4.18}$$

Par la formule des compléments de la fonction Γ, on trouve directement

$$V = 2L\sum_{j\geq 0}(-1)^j\big(\frac{L^2}{4\pi^2}\big)^j(\gamma_j(\alpha) - \gamma_j(2\alpha)) \tag{4.19a}$$

avec

$$L = \log 2, \qquad \alpha = \frac{\pi^2}{L}, \qquad \gamma_j(\alpha) = \sum_{k\geq 1}\frac{k^{-1-2j}}{e^{2\alpha k} - 1}. \tag{4.19b}$$

Les fonctions $\gamma_j(x)$ sont liées aux formes modulaires et à la fonction η de Dedekind. Par exemple,

$$\gamma_0(x) = \log\prod_{\ell\geq 1}(1 - e^{2\ell x})^{-1}. \tag{4.20}$$

Ces fonctions vérifient des équations de transformations "modulaires", la plus classique étant

$$\gamma_0(\alpha) - \frac{1}{4}\log\alpha + \frac{\alpha}{12} = \gamma_0(\beta) - \frac{1}{4}\log\beta + \frac{\beta}{12},$$

lorsque $\alpha\beta = \pi^2$. Ces relations ont été généralisées par Ramanujan qui a fourni des formules de réciprocité liées aux valeurs de $\zeta(2r+1)$:

$$\alpha^{-r}\left[\frac{1}{2}\zeta(2r+1) + \gamma_r(\alpha)\right] - (-\beta)^{-r}\left[\frac{1}{2}\zeta(2r+1) + \gamma_r(\beta)\right] = S \tag{4.21a}$$

où la somme *finie* S vaut (les B_m sont les nombres de Bernoulli)

$$2^{2r}\sum_{k=0}^{r+1}(-1)^{r-1}\frac{B_{2k}}{(2k)!}\frac{B_{2r+2-2k}}{(2r+2-2k)!}\alpha^{r+1-k}\beta^k. \tag{4.21b}$$

L'énoncé du théorème s'obtient à partir de (4.19) au moyen des identités (4.21) par réarrangement des termes. ■

5. Théorie de l'information d'un canal partagé

A ce stade, nous avons obtenu un protocole qui est stable, lorsque le taux d'arrivées vérifie $\lambda < 0,35$. Pippenger [1981] a montré qu'il existait une borne supérieure, voisine de 75%, à l'efficacité de tout protocole de communication (Théorème 9), et que cette borne est fortement liée au caractère incomplet des "observables" – 0,1,beaucoup – (Théorème 10).

THÉORÈME 9. *Sous le modèle d'arrivées poisoniennes de taux λ, tout protocole est nécessairement instable, lorsque $\lambda > \xi$ où ξ est la plus petite racine positive de l'équation*

$$-\xi \log \xi - (1-\xi)\log(1-\xi) + (1-\xi)\log 2 = \xi \log e. \tag{5.1}$$

Soit λ le taux d'arrivées; on examine le comportement d'un protocole arbitraire sur l'intervalle $[0,T]$ avec $T \to \infty$. Par normalisation, on peut se ramener à un flot de taux $\nu = \lambda T$ sur l'intervalle $[0,1]$.

Selon l'expression de Berger [1981], le problème est ainsi de "*pêcher dans un flot de Poisson*" de sorte à isoler les éléments. A chaque étape, le protocole pose une question sur un ensemble mesurable, et les collisions sont résolues dès qu'a été trouvée une partition en blocs de $[0,1]$ – appelée *résolution* – telle que chaque bloc contienne exactement un élément (message).

On peut voir la spécification d'un protocole comme un arbre de décision ternaire (Figure 2). Un sommet de l'arbre est étiqueté par un ensemble mesurable X, et les trois branches correspondent aux trois possibilités $\mathrm{card}(E \cap X) = 0, 1, 2^+$, où E est l'ensemble aléatoire des arrivées.

Comme il est classique en théorie de l'information, la preuve utilise la notion d'*entropie* d'une distribution. Si $\mathbf{p} = \{p_i\}$ représente une suite de nombres positifs, l'entropie est définie par

$$H(\mathbf{p}) = -\sum_i p_i \log p_i. \tag{5.2}$$

L'entropie [McEliece 1977] est une mesure de l'incertitude d'une distribution: en substance, elle représente le nombre moyen de question binaires qu'il est nécessaire de poser pour retrouver un élément aléatoire, ou encore le nombre moyen de bits d'information nécessaire au codage d'un élément aléatoire (les logarithmes étant pris en base 2). L'entropie est nulle pour une distribution déterministe (qui attribue la probabilité 1 à une seule valeur) et maximale dans le cas où tous les p_i sont égaux. Si $\mathbf{q} = \{q_j\}$ est un raffinement de $\mathbf{p} = \{p_i\}$, alors $H(\mathbf{p}) \le H(\mathbf{q})$.

PREUVE. La démonstration se décompose en deux étapes.

1. Soit U une résolution de l'ensemble $\mathbf{E}$ des arrivées, et $p(U)$ sa probabilité. On introduit l'entropie

$$H_1 = -\sum_U p(U) \log p(U). \tag{5.3}$$

   Si U est une partition en blocs de taille $u_1, u_2, \ldots, u_N$, alors chaque bloc contenant exactement un message,

$$p(U) \le \prod_{m=1}^{N} \big(u_m \nu \exp(-u_m \nu)\big) \le (\nu/N)^N e^{-\nu}.$$

   Un argument simple de convexité montre que

$$H_1 \ge \nu \log e. \tag{5.4}$$

Figure 2. Fragment d'un arbre de décision ternaire associé à un protocole. (Par exemple, s'il existe 2^+ éléments dans $[0,1)$, on examine $[0,1/2)$, puis s'il existe zéro ou un seul élément dans $[0,1/2)$, on examine ensuite $[1/2,1)$, sinon on examine $[0,1/4)$ etc).

Soit $p(L)$ la probabilité que l'exécution du protocole se termine sur la feuille L et

$$H_2 = -\sum_L p(L) \log p(L). \tag{5.5}$$

On observe que

$$H_2 \geq \nu \log e, \tag{5.6}$$

car L déterminant une résolution U, l'entropie de la distribution des L est minorée par l'entropie de la distribution des U.

2. Soit $p(K)$ la probabilité que l'exécution du protocole passe par le sommet K de l'arbre de décision. On a alors

$$\sum_K p(K) = \sigma \qquad \text{et} \qquad \sum_K p(K) q(K,1) = \nu, \tag{5.7}$$

où σ désigne le nombre moyen d'étapes de résolution et $q(K,j)$ la probabilité de sortie par la branche j à partir du sommet K. Soit $h(K)$ l'entropie de la distribution des $q(K,j)$, alors

$$H_2 = \sum_K p(K) h(K), \qquad \text{d'où d'après (5.6):} \qquad \sum_K p(K) h(K) \geq \nu \log e. \tag{5.8}$$

Ces préliminaires permettent de conclure. Soit

$$G(x) = -x \log x - (1-x) \log(1-x) + (1-x) \log 2$$

l'entropie d'une distribution de schéma $((1-x)/2, x, (1-x)/2))$. On a

$$h(K) \leq G(q(K,1)) \tag{5.9}$$

Donc, d'après (5.8),

$$\sum_K p(K) G(q(K,1)) \geq \nu \log e, \tag{5.10}$$

1. *Préparation.* Transmettre G. Si $|G| \leq 3$, utiliser le protocole en arbre arbre(G). Sinon, développer la branche gauche de arbre(G) de sorte à obtenir un ensemble Z tel que $|Z| = 2$. (Note: cet ensemble sert à poser des questions, tout en garantissant qu'aucun message ne soit transmis).
2. *Questions.* Soit $\mathcal{F}_j$ le sous-ensemble de $[1..B]$ dont le vecteur caractéristique est la j-ième colonne de la matrice T et $F_j = \bigcup_{s \in \mathcal{F}_j} X_s$. Transmettre $Z \cup F_j$ pour $j = 1..K$. Par le Lemme 2, on détermine le vecteur des N_j.
3. *Transmission.*
   - **3a.** Pour tout i tel que $N_i = 1$, transmettre X_i.
   - **3b.** Pour tout i tel que $N_i \geq 2$, utiliser arbre(X_i). [Le coût total de cette partie est en $o(N)$ par le Théorème 5].

Figure 3. Spécification d'un protocole permettant d'atteindre des taux de 100% (d'après Pippenger).

et d'après la concavité de $G(x)$,
$$\sigma G(\nu/\sigma) \geq \nu \log e.$$
Or l'égalité $G(x) \geq x \log e$ n'est valide que si $x \leq \xi$ dans le domaine $0 \leq x \leq 1$. ■

En revanche, si les multiplicités exactes des collisions sont "observables", on peut approcher un taux de transmission de 100%.

Théorème 10. *Pour un canal dans lequel sont connues à chaque instant les multiplicités de collision, il est possible de construire un protocole stable pour tout taux d'arrivée $\lambda < 1$.*

Preuve. [Esquisse] Soit N la multiplicité d'une collision, supposée rapportée à l'intervalle de temps normalisé $[0, 1]$. L'idée de base consiste à subdiviser l'intervalle de recherche $X = [0, 1]$ en B sous-intervalles $X_1, \ldots, X_B$ de longueur ϵ régulièrement espacés, en choisissant
$$B = \lceil N\sqrt{\log N}\rceil \qquad \text{et} \qquad \epsilon = 1/B. \tag{5.11}$$
Soit N_j l'effectif de X_j. Le point essentiel est que le vecteur $\mathbf{v}$ des N_j peut être déterminé en $o(N)$ étapes. Les groupes X_j tels que $N_j = 1$ sont alors isolés. Pour les autres, qui sont en nombre $o(N)$, on utilise le protocole en arbre pour les séparer.

La clef consiste à déterminer ceux des N_j qui sont non-nuls en posant des questions appropriées. Ceci est clairement possible en B étapes. Ce qui est surprenant, c'est la possibilité de le faire en un nombre K d'étapes qui vérifie
$$K = O(B/\log B) \ll N \ll B,$$
les questions étant du type "$\sum_{j\in J} N_j$?". Ces questions sont construites à partir de matrices binaires dont l'existence est garantie par le lemme suivant:

Lemme 2. *On appelle B-composition un vecteur $\mathbf{v} = (v_1, \ldots, v_B)$ tel que $v_1 + \cdots + v_B \leq B$. Il existe alors un entier $K = O(B/\log B)$ et une matrice binaire de codage $T \in \{0,1\}^{B\times K}$ telle que toute composition $\mathbf{v}$ est uniquement déterminée par le vecteur $T\mathbf{v}$ (de dimension K).*

La preuve de ce lemme s'établit par des méthodes non constructives dans le style d'Erdös et Renyi: on montre que, pour K convenablement choisi, *presque toute* matrice binaire de $\{0,1\}^{B\times K}$ vérifie la condition de codage du Lemme, l'ensemble des exceptions étant, par comptage, de densité nulle. ■

La borne supérieure du Théorème 9 a été améliorée par Molle qui obtient $\xi = 0,6731$, puis Tsybakov et Likhanov [1987] qui obtiennent $\xi = 0,5683$, et Berger [1981] donne même de bonnes raisons de conjecturer que $\xi = 0,5254$. En tout cas, Kelly [1985] a montré que tout protocole dans lequel un message qui arrive est immédiatement transmis ne peut tolérer un taux d'arrivée au delà de $\xi = 0,5671$ sans se déstabiliser. Dans cette catégorie particulière se rangent ALOHA, ETHERNET et le protocole en arbre à accès continu pour lequel on montrera que le débit avoisine 36%, ou 40% après optimisation.

6. Le protocole en arbre à accès libre

On considère ici la seconde version du protocole en arbre, avec accès libre. Cette version est plus proche de la philosophie d'ALOHA et ETHERNET, en ce sens qu'un message fait une tentative immédiate dès qu'il arrive. D'un point de vue pratique, cette version est avantageuse, car les stations n'ont besoin de suivre l'évolution du canal que lorsqu'elles sont actives. De surcroît, cette méthode se prête à des optimisations qui permettent facilement de dépasser des taux d'arrivées de 40%.

D'un point de vue mathématique, les séries génératrices vérifient des équations fonctionnelles non locales à semi-groupe d'itération non commutatif. Une partie du traitement par transformée de Mellin conduit à l'étude de séries de Dirichlet non classiques associées à ce semi-groupe. On dispose ainsi pour ce protocole d'un *modèle analytique* exact, et les différents paramètres (délai, probabilité de collision) peuvent être complètement analysés. [Fayolle et al 1985], [Fayolle et al 1986].

La nouveauté par rapport à la Section 4 réside dans le fait que la résolution de G met en œuvre la résolution de $G_0 + X$ et $G_1 + Y$ où G_0 et G_1 sont obtenus à partir de G par éclatement au moyen de tirages pile-face, et X et Y représentent des arrivées de Poisson. L'aspect profond des équations se révèle lorsqu'on permet la posssibilité de tirages biasés, de sorte que

$$\Pr\{g \in G_0\} = p, \qquad \Pr\{g \in G_1 = q\}, \qquad p + q = 1. \tag{6.1}$$

Cette section a pour but de monter divers résultats dont un corollaire direct est la caractérisation de la région de stabilité du protocole en arbre (à accès libre), que nous énoncerons ici dans le cas où $p = q$.

THÉORÈME 11. *Lorsque les tirages sont non biaisés ($p = q = \frac{1}{2}$), le protocole en arbre à accès libre est stable pour tout taux d'arrivées $\lambda < \lambda_{\max}$, où $\lambda_{\max} = 0.360177$ est la plus petite racine positive de l'équation $D(x) = -\frac{1}{2}$ avec*

$$D(x) = \frac{1}{1-2x} e^{-2x} \sum_{i \geq 0} 2^i e^{2x/2^{-i}} \left[e^{-x/2^i} (1 - \frac{x}{2^i}) - 1 + 2x2^{-i} - 2(x2^{-i})^2 \right]. \tag{6.2}$$

PREUVE. Revenons au cas de p et q généraux, avec $p + q = 1$. A cause des possibilités d'arrivées, la récurrence (4.3) décrivant le temps L_n de résolution de n collisions initiales devient

$$L_n = 1 + L_{K+X} + L_{n-K+Y}, \tag{6.3}$$

où X et Y représentent des arrivées de Poisson de taux λ. La différence provient de ce que les L_N sont ainsi liés à l'ensemble (infini) de tous les L_j. En passant aux espérances $l_n = \mathbf{E}\{L_n\}$, puis en introduisant les séries génératrices

$$l(z) = \sum_{n \geq 0} l_n \frac{z^n}{n!} \qquad \text{et} \qquad \hat{l}(z) = e^{-z} l(z), \tag{6.4}$$

on obtient d'abord une *récurrence infinie* sur les l_n, qui se traduit sur $l(z)$ et (plus simplement) sur $\hat{l}(z)$.

LEMME 3. *La série génératrice $\hat{l}(z)$ est solution de l'équation fonctionnelle*

$$\psi(z) - \psi(\lambda + pz) - \psi(\lambda + qz) = a(z) \tag{6.5}$$

dans laquelle $a(z)$ désigne la fonction entière

$$a(z) = 1 - Ce^{-z}(1 + Kz) \qquad \text{avec} \qquad C = \psi(\lambda) \quad \text{et} \quad K = \frac{e^{-\lambda/p} - e^{-\lambda/q}}{\frac{\lambda}{q}e^{-\lambda/q} - \frac{\lambda}{p}e^{-\lambda/p}}. \tag{6.6}$$

A l'opposé de (4.4), cette équation fonctionnelle est non locale (voir les remarques du point 1 *infra*). Pour la résoudre, on utilise une méthode d'itération (cf Eq (4.6), (4.7)) résumée par le lemme suivant.

LEMME 4. *Soient $\sigma_1(z) = \lambda + pz$, $\sigma_2(z) = \lambda + qz$ deux substitutions linéaires avec $p + q = 1$, $p, q > 0$. Alors l'équation fonctionnelle*

$$\psi(z) = a(z) + \alpha\psi(\sigma_1(z)) + \beta\psi(\sigma_2(z)) \tag{6.7}$$

où $a(z)$ est une fonction entière, et α, β sont des constantes positives vérifiant la condition de contraction $\alpha + \beta < 1$, possède une unique solution entière

$$\psi(z) = \sum_{\tau \in H} (\alpha;\beta)^\tau a(\tau(z)) \qquad \text{avec} \qquad (\alpha;\beta)^\tau = \alpha^{t_1}\beta^{t_2}, \quad t_1 = |\tau|_{\sigma_1}, t_2 = |\tau|_{\sigma_2}. \tag{6.8}$$

H étant le semi-groupe engendré par σ_1 et σ_2.

Les éléments τ du semi-groupe H sont assimilables à des mots sur l'alphabet $\{\sigma_1, \sigma_2\}$ et $|\tau|_\sigma$ désigne le nombre de lettres σ dans τ.

La preuve de Lemme 4 repose sur le fait que (6.8) est clairement une solution formelle. Analytiquement, pour obtenir la convergence de cette solution, il suffit d'observer les point suivants:

1. Les substitutions σ_1, σ_2 sont des contractions dont les deux points fixes sont $\xi_1 = \lambda/q$ et $\xi_2 = \lambda/p$. Les substitutions $\tau \in H$ ont leur points fixes entre ξ_1 et ξ_2 et ces points fixes forment un ensemble *dense* sur $[\xi_1, \xi_2]$. Les images d'un point z_0 par $\tau \in H$ forment ainsi un ensemble dont l'intervalle $[\xi_1, \xi_2]$ est l'ensemble des points d'accumulation (cf Figure 4).
2. La somme dans (6.7) converge alors de la même manière que le developpement en monômes non commutatifs
$$\frac{1}{1 - \alpha - \beta} = \sum_{w \in \{\alpha,\beta\}^*} w.$$

On peut alors résoudre l'équation (6.5) vérifiée par la série génératrice $\hat{l}(z)$ des l_n: (i) par dérivation deux fois, on obtient une équation qui vérifie la condition de contraction du Lemme 4; (ii) Le fait que la constante C qui apparaît dans $a(z)$ soit égale à $\psi(\lambda)$ impose une condition de "cohérence" du type $D(x) \neq -\frac{1}{2}$, $D(x)$ étant défini en (6.2) lorsque $p = q$.

De la sorte, on a montré l'existence (la finitude) des l_n, d'où l'on déduit la positivité (cf infra), lorsque $\lambda < \lambda_{\max}$. D'après la propriété des chaines de Markov: *le temps moyen de retour à un état est l'inverse de sa probabilité stationnaire*, on en déduit la stabilité lorsque $\lambda < \lambda_{\max}$. D'après le fait que chaque l_n est, par la nature du processus, une fonction croissante de λ, on en déduit l'instabilité lorsque $\lambda > \lambda_{\max}$. ■

Il est intéressant de connaître la nature asymptotique des l_n, car elle caractérise la réponse "impulsionnelle" lors d'une pointe de trafic. L'analyse par transformation de Mellin conduit à des développements nouveaux liés à une propriété *métrique* du semi-groupe H plus forte que la densité des images $\{\tau(z_0)\}$.

Figure 4. La suite des itérés par $\tau \in H$ d'un point z_0.

THÉORÈME 12. *Les quantités l_n représentant l'espérance du temps de retour à l'état inactif à partir d'une n-collision vérifient, lorsque $\lambda < \lambda_{\max}$,*

$$l_n = n[A + P(\log n)] + o(n) \tag{6.9}$$

où $A = A(\lambda, p, q)$ et $P(u)$ est: (i) une fonction périodique de petite amplitude lorsque $\log p / \log q$ est rationnel, (ii) une fonction tendant vers 0 dans le cas contraire.

PREUVE. La forme de $l(z)$ et $\hat{l}(z)$ fait intervenir, par (6.8), un opérateur de sommation indexé sur le semi-groupe H. Par transformation de Mellin sur la forme explicite des coefficients, on introduit ce qu'on peut appeler les *séries de Dirichlet* du semi-groupe H. Soit $r(u)$ une fonction définie pour $u \geq 0$, qu'on suppose plusieurs fois différentiable. Une telle série est définie par

$$\omega(s) = \sum_{\tau \in H} r(\tau(0))(p^s; q^s)^\tau \tag{6.10}$$

en utilisant la notation d'exposants de (6.8). L'analyse asymptotique des l_n nécessite la détermination des singularités de telles séries de Dirichlet du semi-groupe H.

LEMME 5. *Une série de Dirichlet $\omega(s)$ du semi-groupe H est méromorphe pour $\Re(s) > 0$. Ses singularités sont celles de $(1 - p^s - q^s)^{-1}$ et au voisinage de la singularité dominante $s = 1$, elle possède le développement local*

$$\omega(s) = \frac{C}{(s-1)} + C_0 + O(s-1) \tag{6.11}$$

où, $h(p,q) = p \log p^{-1} + q \log q^{-1}$ désignant la fonction d'entropie,

$$C = \frac{1}{h(p,q)} \cdot \frac{1}{\frac{\lambda}{q} - \frac{\lambda}{p}} \int_{\lambda/p}^{\lambda/q} r(u)\, du. \tag{6.12}$$

Il intervient ainsi dans la constante C l'entropie, et la valeur moyenne de la fonction $r(u)$ sur l'intervalle des points fixes de σ_1, σ_2. La preuve de ce résultat repose sur la propriété suivante:

> *Si l'on part d'un point quelconque z_0 et qu'on applique une suite de substitutions, σ_1 avec probabilité p et σ_2 avec probabilité q, on obtient lorsque le nombre de substitutions*

appliquées devient grand un ensemble d'images qui tend à couvrir l'intervalle des points fixes $[\lambda/p, \lambda/q]$ de manière uniforme.

C'est pour cette raison qu'apparaît la valeur moyenne de $r(u)$ sur l'intervalle des points fixes: si R est cette valeur moyenne, $\omega(s)$ diverge lorsque $s \to 1$ comme

$$R \sum_{\tau \in H} (p^s; q^s)^\tau \equiv \frac{R}{1 - p^s - q^s} \sim \frac{R}{h(p,q)} \cdot \frac{1}{s-1}. \tag{6.13}$$

La constante suivante C_0 s'exprime au moyen de fonctions "fractales" obtenues par superpositions de fonctions triangulaires, du type de l'exemple classique par Weierstrass d'une fonction continue nulle part différentiable.

Le caractère périodique ou non de $P(u)$ dépend de la position des zéros ($s \neq 1$) de $1 - p^s - q^s$, elle–même liée à des propriétés d'approximation diophantienne de $\log p / \log q$. ■

Signalons enfin que la valeur de la série génératrice $\hat{l}(z)$ en $z = \lambda$ possède elle-même une interprétation probabiliste:

$$\hat{l}(\lambda) = \sum_{n \geq 0} e^{-\lambda} \frac{\lambda^n}{n!} l_n. \tag{6.14}$$

Cette forme montre que $\hat{l}(\lambda)$ est la durée moyenne (en régime stationnaire) de l'intervalle entre deux périodes d'inactivité du canal.

De la même manière, on peut exprimer au moyen de sommations de type (6.8) espérance et variance du délai, probabilité de transmission immédiate etc. On peut ainsi développer une analyse à faible trafic ($\lambda \to 0$) et trouver que l'utilisation de probabilités biaisées $p = 2 - \sqrt{2}$ minimise alors le délai.

Les mêmes méthodes s'appliquent enfin à l'étude d'éclatements non binaires. Comme corollaire de ces méthodes d'analyse [Mathys *et al* 1985], un gain sensible – augmentation relative de 10% du débit – est obtenu en utilisant des éclatements ternaires.

COROLLAIRE 1. *Le protocole en arbre à arrivées libre et éclatements ternaires est stable pour tout taux d'arrivées* $\lambda < \lambda_{\max} = 0.401599$.

Le protocole en arbre à accès libre est ainsi le seul protocole pour lequel soit connu un *modèle analytique* exact.

7. Conclusions

La première conclusion qui s'impose est que, du point de vue théorique, le problème de l'accès multiple vis à vis du critère de débit maximum, est assez bien maîtrisé. Par les bornes de théorie de l'information, on ne saurait faire mieux que de transmettre à des taux de 56% (et même sans doute 52%); par ailleurs des adaptations (par Gallager et Tsybakov) du protocole en arbre permettent d'atteindre des taux de transmission de 48%.

Bien sûr la situation réelle est un peu plus complexe, et nous ne ferons qu'évoquer les problèmes: resistance aux erreurs du canal, réponse impulsionnelle, complexité d'observation du canal pour les stations, délai etc. Le protocole en arbre réalise sur ces différents points ce qui semble un bon compromis, et présente en tout cas, en accord avec la théorie, des avantages évidents sur ALOHA et ETHERNET, illustrés par les simulations de la Figure 5. La Figure 6 montre le gain supplémentaire obtenu par des arbres à éclatements optimaux ternaires plutôt que binaire (cf Th. 11 et Cor. 1).

Au risque de donner une impression de "bric-à-brac", nous avons choisi de passer en revue diverses facettes d'un unique problème. En fait, plusieurs des analyses données ici se rattachent

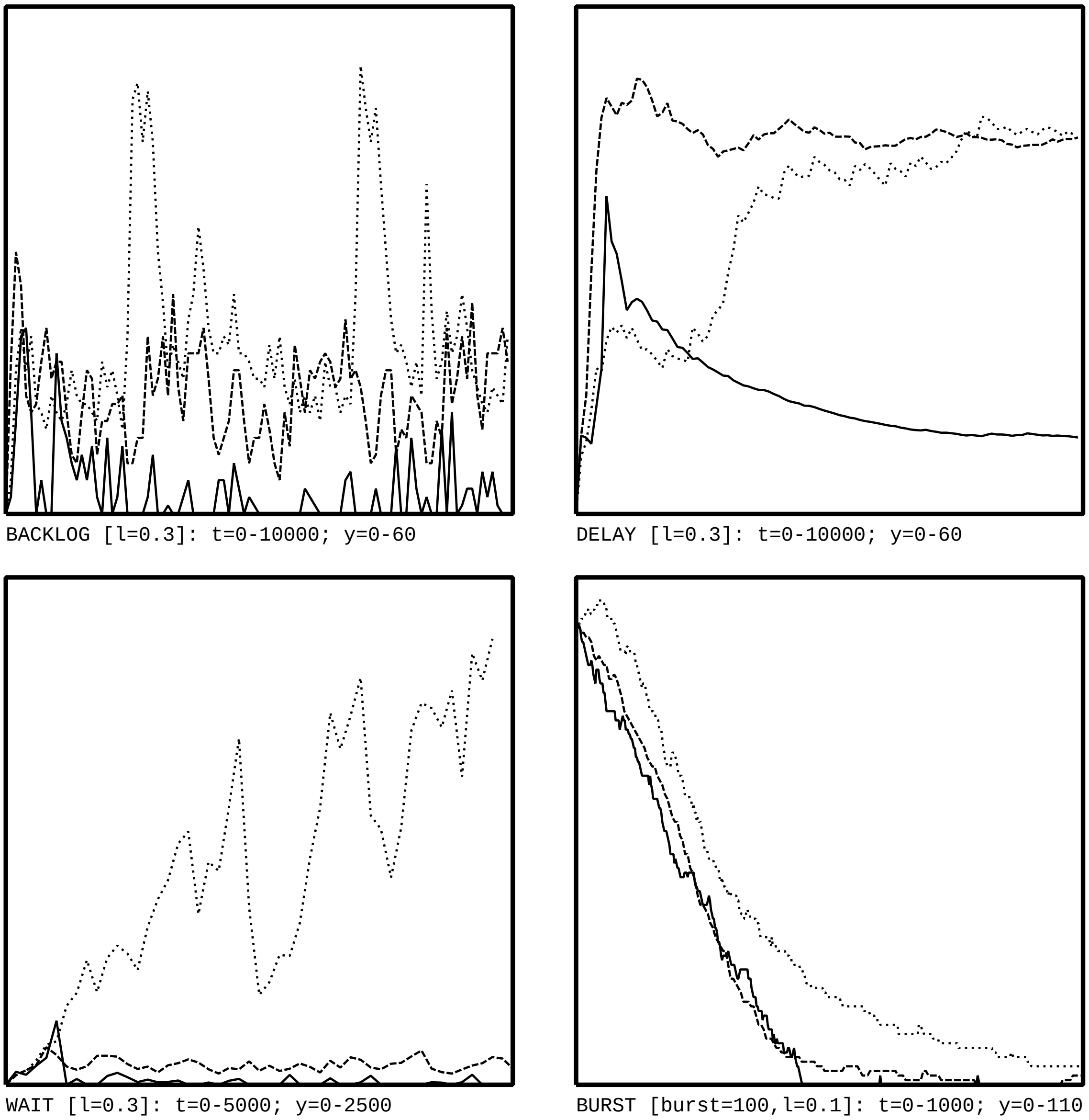

Figure 5. Simulations des protocoles Aloha (tirets) avec probabilité de retransmission p=0,02; Ethernet (pointillé); Arbre binaire avec accès libre (trait continu).

Le temps t est représenté en abscisse. Les trois premiers diagrammes décrivent l'évolution du système lorsque λ=0,3: (1) Taille de la population en attente de retransmission; (2) Délai moyen sur l'ensemble des messages déjà écoulés; (3) Temps de présence dans le système des messages en attente. (4) Le quatrième diagramme décrit l'évolution du système après injection de 100 messages, suivi d'arrivées à taux réduit (λ=0,1).

(1). Population en attente. On constate que le protocole en arbre revient "périodiquement" à l'état vide et tend à y demeurer. Par contraste, Aloha est dans un état quasi-stable où la file d'attente possède une taille voisine de 15, et la file d'Ethernet est plus importante.

(2). Délai. Le protocole en arbre se stabilise rapidement à des délais moyens voisins de 9, alors que les délais d'Aloha et Ethernet sont voisins de 40.

(3). Temps d'attente de la population bloquée. Cette caractéristique distingue nettement Ethernet des autres protocoles: sur 5000 étapes, plusieurs messages bloqués ont attendu un temps voisin de 2500, et ce paramèter ne fait que croître en accord avec le théorème d'instabilité. Aloha montre encore son régime quasi-stable (avec un temps de présence moyen voisin de 100).

(4). Réponse impulsionnelle. L'arbre "récupère"en un temps de l'ordre de 400, et Aloha en un temps de l'ordre de 600.

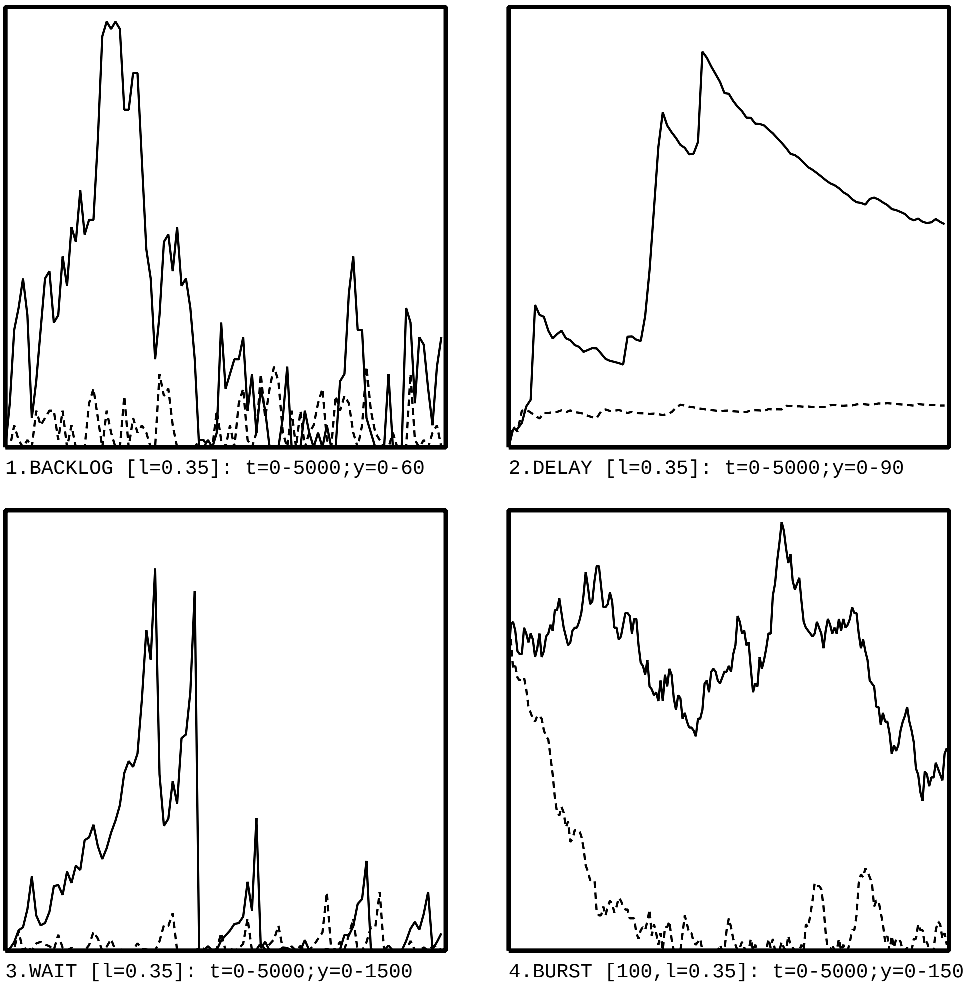

Figure 6. Comparaison du protocole en arbre avec branchement binaire (en trait continu) et ternaire (en tirets) selon les critères de la Figure 5. Les simulations sont relatives à un taux d'arrivées λ=0,35 (voisin du seuil critique de l'arbre binaire) et montrent dans cette région le gain important dû aux éclatements ternaires.

à un complexe de problèmes généraux et l'on se contentera de quelques brèves indications sur ce sujet.

1. *Tests de groupe.* Il existe un parallèle imprévu entre la résolution de collisions et des problèmes examinés par les statisticiens et connus sous le nom de "group testing" [Wolf 1985]. Durant la seconde guerre mondiale, l'administration militaire américaine avait eu le besoin d'effectuer des tests sanguins de syphillis portant sur des millions de personnes (test de Wasserman). Il n'était pas concevable de faire des tests individuels. L'idée naturelle est d'effectuer des mélanges de sang sur lesquels on fait un test global. Il s'agit alors de déterminer une stratégie de groupements de sorte à isoler les individus malades de manière efficace. Ce problème ressemble à la résolution de collisions, à ceci près que les observables sont réduites à 0 ou 1^+. Si l'on procéde par recherche

dichotomique, l'algorithme correspondant est alors très voisin du protocole en arbre et s'analyse de manière analogue.

2. *Arbres digitaux.* On peut utiliser l'idée du partitionnement récursif pour réaliser une allocation "spatiale" (plutôt que "temporelle") d'un ensemble d'enregistrements dans des bases de données ou en mémoire centrale d'ordinateur par exemple. La structure résultante est connue sous le nom d'arbre digital (*trie*) ou hachage dynamique [Knuth 1973], [Sedgewick 1988]. Dans ce cas, la condition d'arrêt du développement de l'arbre peut être $|G| \leq b$ où $b \geq 1$ représente la capacité d'une "page". Les paramètres à analyser sont la longueur de cheminement ou la hauteur de l'arbre, et les techniques d'équations fonctionnelles, de transformation de Mellin doivent alors être conjuguées avec d'autres méthodes asymptotiques comme la méthode de Laplace, ou la méthode de col [Flajolet, Steyaert 1982], [Régnier 1983], [Jacquet, Régnier 1986].

3. *Factorisation de polynômes.* L'algorithme de factorisation de polynômes (sur un corps fini) de Cantor-Zassenhaus-Lazard est fondé sur la construction d'"idempotents" [Knuth 1981]. L'analyse [Flajolet, Steyaert 1982] de cet algorithme met en jeu le problème suivant: *Etant donnés n vecteurs dans $\{0,1\}^d$, les probabilités de 0 et de 1 étant respectivement p et q, déterminer le nombre d'étapes de multiplication composante par composante nécessaires pour isoler les composantes 1.* Cette question se ramène simplement à l'analyse de la hauteur d'un arbre et lorsque $d \to \infty$, on trouve une série génératrice pour la distribution de hauteur

$$\prod_{k=0}^{n} \left(1 + p^k q^{n-k}\right)^{\binom{n}{k}},$$

et une hauteur moyenne $\approx \log n / \log(p^2 + q^2)^{-1}$.

4. *Architecture de systèmes multiprocesseurs.* Des protocoles d'un type voisin sont enfin utilisés pour organiser la communication entre processeurs et mémoire, sur un "bus", dans des machines multiprocesseur. (voir par exemple SLIC, System Link and Interrupt Controller [Beck *et al* 1987]).

Remerciements: Cette conférence est due de prime abord à l'indéfectible ténacité de Gérard Rauzy. Je tiens à remercier Guy Fayolle pour les patientes et nombreuses heures d'explications passées sur les questions probabilistes avec lesquelles je ne suis pas familier et Jean-Marc Steyaert ainsi que Robert Ehrlich pour une lecture critique du manuscript.

AMICIS AMICISQVE QVOTQVOT VBIQUE SVNT

Références

Pour une introduction au sujet discuté ici, les références principales sont [Longo 1981] (articles de Massey, Berger, Ruget) et [Massey 1985].

N. ABRAMSON [1985]. "Development of the ALOHANET", in Special Issue on Random-Access Communication, *IEEE Transactions on Information Theory* **IT-31**, 1985, 119-123.

D. ALDOUS [1987]. "Ultimate Instability of Exponential Back-Off Protocol for Acknowledgement-Based Transmission Control of Random Access Communication Channels", *IEEE Transactions on Information Theory* **IT-33**, 1987, 219-223.

T. M. APOSTOL [1976]. *Modular Functions and Dirichlet Series in Number Theory*, Graduate Texts in Mathematics, Springer verlag, 1976.

R. AZENCOTT, G. RUGET [1977]. "Mélanges d'équations différentielles et grands écarts à la loi des grands nombres", *Zeitschrift für Wahrscheinlichkeitstheorie* **38**, 1977, 1-54.

B. Beck, B. Kasten, S. Thakkar [1987]. "VLSI Assist for a Multiprocessor", in *Proc. Second International Conference on Architectural Support for Programming Languages and Operating Systems*, IEEE Computer Society, 1987.

B. C. Berndt [1977]. "Modular Transformations and Generalizations of Several Formulae of Ramanujan", *Rocky Mountain J. of Math.* **7**, 1977, 147-189.

T. Berger [1981]. "The Poisson Multiple-Access Conflict Resolution Algorithm", in *Multi-User Communication Systems*, G. Longo Editor, *CISM Courses and Lectures no.* **255**, Springer Verlag, Wien-New York, 1981, 1-27.

P. Billingsley [1986]. *Probability and Measure*, Wiley, New York, 1986 (2nd Edition).

B. Bollobás [1985] *Random Graphs*, Academic Press, London, 1985.

K. Chandrasekharan [1985]. *Elliptic Functions*, Grundlehren der mathematischen Wissenschaften **261**, Springer, Berlin, 1985.

J. I. Capetanakis [1979]. "Tree Algorithms for Packet Broadcast Channels", *IEEE Transactions on Information Theory* **IT-25**, 1979, 505-515.

G. Doetsch [1955]. *Handbuch der Laplace Transformation*, Birkhäuser Verlag, Basel, 1955.

G. Fayolle [1975]. "Etude du comportement d'un canal radio partagé entre plusieurs utilisateurs", Thèse de Docteur Ingénieur, Université Paris VI, 1975.

G. Fayolle [1986] "Ergodicity and Asymptotic Behaviour of Multitype Branching Processes Arising in Random Access Communication Systems", in *Proc. of the First World Congress of the Bernoulli Society*, Tashkent, 1986, 535-538.

G. Fayolle, P. Flajolet, M. Hofri [1986]. "On a Functional Equation Arising in the Analysis of a Protocol for a Multi-Access Broadcast Channel", *Advances in Applied Probability* **18**, 1986, 441-472.

G. Fayolle, P. Flajolet, M. Hofri, P. Jacquet [1985]. "Analysis of a Stack Algorithm for Random Multiple Access Communication", in Special Issue on Random-Access Communication, *IEEE Transactions on Information Theory* **IT-31**, 1985, 244-254.

G. Fayolle, E. Gelenbe, J. Labetoulle [1977]. "Stability and Optimal Control of the Packet Switching Broadcast Channel", *Journal of the ACM* **24**, 1977, 375-386.

P. Flajolet, J-M. Steyaert [1982]. "A Branching Process Arising in Dynamic Hashing, Trie Searching and Polynomial Factorization", in *Automata, Languages and Programming*, *Lect. Notes in Comp. Sc.* **140**, 1982, 239-251.

R. G. Gallager [1978]. "Conflict Resolution in Random Access Broadcast Networks", in *Proc. AFOSR Workshop on Communication Theory and Applications*, Provincetown, September 1978, 74-76.

R. G. Gallager [1985]. "A Perspective on Multi-Access Channels", in Special Issue on Random-Access Communication, *IEEE Transactions on Information Theory* **IT-31**, 1985, 124-142.

A. G. Greenberg, A. Weiss [1986]. "An Analysis of Aloha Systems via Large Deviations", ATT Technical Memorandum, April 1986, 18p.

G. H. Hardy [1978]. *Ramanujan, Twelve Lectures Suggested by his Life and Work*, Chelsea Pub. Co., 1978 (3rd Edition).

P. Jacquet, M. Régnier [1986]. "Trie Partitioning Process: Limiting Distributions", in *Proc. CAAP86*, *Lect. Notes in Comp. Sc.* **214**, Springer, 1986, 239-251.

P. Jacquet, M. Régnier [1987]. "Normal Limiting Distribution of the Size of Tries", in *Performance'87*, P-J. Courtois et G. Latouche Editors, Elsevier North Holland, 1987, 209-223.

F. P. Kelly [1985]. "Stochastic Models of Computer Communication Systems", *J. Royal Statistical Soc.* B **45**, 379-395.

F. P. Kelly, I. M. MacPhee [1986]. "The Number of Packets Transmitted by Collision Detect Random Access Channel", *Annals of Probability* **15**, 1986, 1557-1568.

P. Kirschenhofer, H. Prodinger [1987]. "On Some Applications of Formulae of Ramanujan in the Analysis of Algorithms", preprint, Technische Universität Wien, 1987, 22p.

D. E. Knuth [1973]. *The Art of Computer Programming*, Vol. 3, *Sorting And Searching*, Addison-Wesley, Reading, 1973.

D. E. Knuth [1981]. *The Art of Computer Programming*, Vol. 2, *Semi-Numerical Algorithms*, 2nd Edition, Addison-Wesley, Reading, 1981.

G. Longo [1981]. *Multi-User Communication Systems*, G. Longo Editor, *CISM Courses and Lectures no.* **255**, Springer Verlag, Wien-New York, 1981.

J. L. Massey [1981]. "Collision Resolution Algorithms and Random-Access Communications", in *Multi-User Communication Systems*, G. Longo Editor, *CISM Courses and Lectures no.* **255**, Springer Verlag, Wien-New York, 1981, 73-137.

J. L. Massey (Editor) [1985]. Special Issue on Random-Access Communication, *IEEE Transactions on Information Theory* **IT-31**, 1985.

P. Mathys, P. Flajolet [1985]. "Q-ary Collision Resolution Algorithms in Random Access Systems with Free or Blocked Access", in Special Issue on Random-Access Communication, *IEEE Transactions on Information Theory* **IT-31**, 1985, 217-243.

R. J. McEliece [1977]. *The Theory of Information and Coding*, Encyclopedia of Mathematics and Its Applications **3**, Addison-Wesley, Reading, 1977.

R. M. Metcalfe, D. Boggs [1976]. "Ethernet: Distributed Packet Switching for Local Computer Networks"", *Comm. ACM* **19**, 1976, 395-404.

N. Pippenger [1981]. "Bounds on the Performance of Protocols for a Multiple Access Broadcast Channel", *IEEE Transactions on Information Theory* **IT-27**, 1981, 145-151.

M. Régnier [1983]. "Evaluation des performances du hachage dynamique", Thèse de 3ième cycle, Université d'Orsay, 1983.

S. M. Ross [1987]. "A Simple Proof of Instability of a Random Access Communication Channel", *Probability in Engineering and Inf. Sc*, 1987 (to appear).

G. Ruget [1981]. "Some Tools for the Study of Channel-Sharing Algorithms", in *Multi-User Communication Systems*, G. Longo Editor, *CISM Courses and Lectures no.* **255**, Springer Verlag, Wien-New York, 1981, 201-231.

R. Sedgewick [1988]. *Algorithms*, 2nd Edition, Addison-Wesley, Reading, 1988.

B. S. Tsybakov [1985]. "Survey of USSR Contributions to Random Multiple-Access Communications", in Special Issue on Random-Access Communication, *IEEE Transactions on Information Theory* **IT-31**, 1985, 143-165.

B. S. Tsybakov, N. B. Likhanov [1987]. "An Upper Bound for Capacity of a Random Multiple-Access Channel", *Probl. Inform. Transmission* **23**, 1987, 64-78.

B. S. Tsybakov, V. A. Mikhailov [1979]. "Free Synchronous Packet Access in a Broadcast Channel with Feedback", *Probl. Inform. Transmission* **14**, 1979, 259-280.

J. K. Wolf [1985]. "Born Again Group Testing: Multiaccess Communication", in Special Issue on Random-Access Communication, *IEEE Transactions on Information Theory* **IT-31**, 1985, 185-191.