# Une théorie mathématique de la communication

C. E. Shannon

## Introduction

Le développement récent de diverses méthodes de modulation telles que MIC (modulation par impulsions et codage) et MIP (modulation d'impulsions en position) qui échangent une bande-passante pour un taux de signal-bruit a intensifié l'intérêt d'une théorie générale de la communication. Une base pour une telle théorie existe dans les articles importants de Nyquist [1] et Hartley [2] sur ce sujet. Dans le présent article, on étendra la théorie pour inclure un certain nombre de nouveaux facteurs, en particulier l'effet du bruit dans le canal, et les économies possibles dues à la structure statistique du message original et à la nature de la destination finale de l'information.

Le problème fondamental de la communication est de reproduire en un point soit exactement, soit approximativement, un message sélectionné en un autre point. Fréquemment, les messages ont du sens, c'est-à-dire qu'ils font référence ou sont liés à un certain système avec certaines caractéristiques physiques ou conceptuelles. Ces aspects sémantiques de la communication ne sont pas pertinents pour le problème d'ingénierie. L'aspect significatif est que le message réel est un message sélectionné parmi des messages possibles. Le système doit être conçu pour procéder pour chaque sélection possible, et non pas seulement pour celle qui sera choisie effectivement puisque celle-ci est inconnue au moment de la conception.

Si le nombre de messages dans l'ensemble est fini, alors ce nombre ou toute fonction monotone de ce nombre peut être considéré comme une mesure de l'information produite lorsqu'un message est choisi dans l'ensemble, tous les choix étant également possibles. Comme cela a été remarqué par Hartley, le choix le plus naturel est la fonction logarithmique. Bien que cette définition puisse être considérablement généralisée quand on considère l'influence des statistiques de messages et quand on a un domaine continu pour les messages, on utilisera dans tous les cas une mesure principalement logarithmique.

La mesure logarithmique est plus pratique pour diverses raisons :

1. Elle est pratiquement plus utile. Des paramètres importants en ingénierie tels que le temps, la bande-passante, le nombre de relais, etc., tendent à varier linéairement par rapport au logarithme du nombre de possibilités. Par exemple, ajouter un relais à un groupe double le nombre d'états possibles des relais. Cela incrémente de 1 le logarithme en base 2 de ce nombre. Doubler le temps élève grossièrement au carré le nombre de messages possibles, ou double le logarithme, etc.

---

https://people.math.harvard.edu/ ctm/home/text/others/shannon/entropy/entropy.pdf.
Reimprimé avec des corrections à partir du Journal technique des systèmes (Bell System Technical Journal), Vol. 27. pp. 379-423, 623-656, Juillet, Octobre, 1948.
Transcription LaTeX : Denise Vella-Chemla, mars 2025.

[1] Nyquist, H., "Certain Factors Affecting Telegraph Speed", *Bell System Technical Journal*, Avril 1924, p. 324 ; "Certain Topics in Telegraph Transmission Theory", A.I.E.E. Trans, v. 47, Avril 1928, p. 617.

[2] Hartley, R. V. L. "Transmission of Information", *Bell System Technical Journal*, July 1928, p. 535.

2. Cette mesure est plus proche de notre sensation intuitive de la mesure effective. Cela est fortement lié à (1) puisque nous mesurons intuitivement des données en les comparant linéairement aux données communes. On pense, par exemple, que deux cartes perforées ont deux fois plus de capacité qu'une pour le stockage de l'information, et que deux canaux ont deux fois plus de capacité qu'un seul canal pour transmettre de l'information.

3. C'est mathématiquement plus adéquat. Beaucoup des opérations de limitation sont simples à exprimer en fonction du logarithme mais nécessiterait une reformulation maladroite en fonction du nombre de possibilités.

Le choix d'une base logarithmique correspond au choix d'une unité pour mesurer l'information. Si la base 2 est utilisée, les unités résultantes peuvent être appelées chiffres binaires, ou plus brièvement bits, un mot suggéré par J. W. Tukey. Un dispositif à deux positions stables, tel qu'un relais ou un circuit flip-flop, peut stocker un bit d'information. $N$ tels dispositifs peuvent stocker $N$ bits, puisque le nombre total d'états est $2^N$ et $\log_2 2^N = N$. Si la base 10 est utilisée, les unités peuvent être appelées chiffres décimaux. Puisque

$$\begin{aligned} \log_2 M &= \log_{10} M / \log_{10} 2 \\ &= 3.32 \log_{10} M, \end{aligned}$$

un chiffre décimal correspond environ à $3\frac{1}{3}$ bits. Une roue de chiffres sur une machine de calcul de bureau a dix positions stables et par conséquent, a une capacité de stockage d'un chiffre décimal. Dans le travail analytique, où l'intégration et la différentiation interviennent, la base $e$ est parfois utile. Les unités résultantes d'information seront appelées unités naturelles. Passer de la base $a$ à la base $b$ nécessite simplement une multiplication par $\log_b a$.

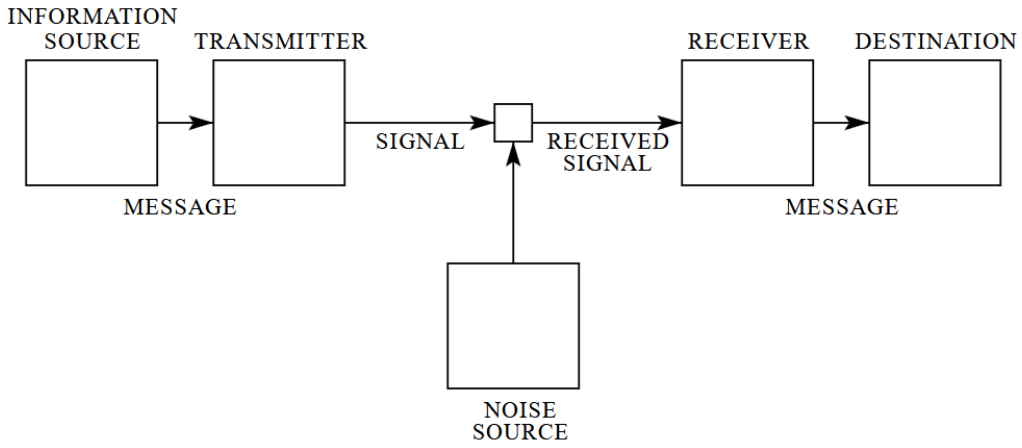



FIG. 1 : Diagramme schématique d'un système général de communication.

Par système de communication, on entendra système du type indiqué schématiquement dans la Fig. 1. Un tel système est principalement constitué de cinq parties :

1. *Une source d'information* qui produit un message ou une suite de messages qui doivent être communiqués au terminal de réception. Le message peut être de différentes sortes : (a) Une séquence de lettres comme dans un télégraphe d'un système de télétype ; (b) Une seule

fonction du temps $f(t)$ comme en radio ou téléphonie ; (c) Une fonction du temps et d'autres variables comme dans la télévision en noir et blanc. Ici on doit penser au message comme à une fonction $f(x, y, t)$ de deux coordonnées d'espace et d'une coordonnée de temps, l'intensité de la lumière au point $(x, y)$ et à l'instant $t$ sur une plaque à tube cathodique ; (d) deux ou plusieurs fonctions du temps, disons $f(t)$, $g(t)$, $h(t)$ - c'est le cas dans la transmission du son "tri-dimensionnelle" ou si le système est destiné à servir plusieurs canaux en multiplexe ; (e) plusieurs fonctions de plusieurs variables : dans la télévision en couleur, le message consiste en trois fonctions $f(x, y, t), g(x, y, t), h(x, y, t)$ définies dans un continuum tri-dimensionnel - on peut aussi penser à ces trois fonctions comme aux composantes d'un espace vectoriel défini dans une région ; similairement, plusieurs sources pour les télévisions noir et blanc produiront des "messages" consistant en un certain nombre de fonctions de trois variables ; (f) plusieurs combinaisons peuvent également avoir lieu, par exemple pour la télévision associée à un canal audio.

2. Un *émetteur* qui opère sur le message d'une certaine manière pour produire un signal adéquat pour la transmission sur le canal. En télégraphie, cette opération consiste simplement à changer la pression du son en un courant électrique proportionnel. En télégraphie, on a une opération d'encodage qui produit une séquence de points, de tirets, et d'espaces sur le canal, correspondants au message. Dans un système multiplexe MIC, des fonctions différentes du discours peuvent être échantillonées, compressées, quantifiées et encodées, et finalement mixées correctement pour construire le signal. Les systèmes vocodeurs, la télévision et la modulation de fréquence sont d'autres exemples d'opérations complexes appliquées au message pour obtenir le signal.

3. Le *canal* est simplement le medium utilisé pour transmettre le signal de l'émetteur au récepteur. Cela peut être une paire de fils, un câble coaxial, une bande de fréquences radio, un faisceau de lumière, etc.

4. Le *récepteur* procède habituellement à l'opération inverse de celle effectuée par l'émetteur, en reconstruisant le message à partir du signal.

5. Le *destinataire* est la personne (ou la chose) à qui le message est destiné.

On souhaite considérer certains problèmes généraux faisant intervenir des systèmes de communication. Pour faire cela, il est d'abord nécessaire de représenter les différents éléments intervenant comme des objets mathématiques, idéalisés adéquatement à partir de leur contrepartie physique. On peut grossièrement classer les systèmes de communication en trois catégories principales : discrets, continus et mixtes. Par système discret, on entendra tout système dans lequel à la fois le message et le signal sont des suites de symboles discrets. Le cas typique est la télégraphie où le message est une suite de lettres et où le signal est une suite de points, traits, et espaces. Un système continu est un système dans lequel le message et le signal sont tous les deux traités comme des fonctions continues, par exemple les signaux radio ou télévisuels. Un système mixte est un système dans lequel des variables discrètes et des variables continues apparaissent, par exemple la transmission MIC de la parole.

On considère d'abord le cas discret. Ce cas a des applications non seulement en théorie de la communication, mais également dans la théorie des machines à calculer, la conception des échanges

téléphoniques, et d'autres domaines. De plus, le cas discret forme le socle pour les cas continus et mixtes qui seront traités dans la seconde partie de l'article.

## PARTIE I : SYSTÈMES DISCRETS DÉPOURVUS DE BRUIT

### 1. Le canal discret non bruité

Le télétype et le télégraphe sont deux exemples simples d'un canal discret pour la transmission d'information. Généralement, un canal discret est un système dans lequel une suite de choix à partir d'un ensemble de symboles élémentaires $S_1, ..., S_n$, peut être transmise d'un point à un autre. Chacun des symboles $S_i$ est supposé avoir une certaine durée temporelle, $t_i$ secondes (cette durée n'est pas nécessairement identique pour des symboles $S_i$ différents, parr exemple les points et les traits en télégraphie). Il n'est pas nécessaire que toutes les suites possibles de $S_i$ puissent être transmises sur le système ; seules certaines suites peuvent être autorisées. Ces suites seront les signaux possibles pour ce canal. Ainsi, en télégraphie, supposons que les symboles soient : (1) un point, consistant à la fermeture de la ligne pendant une unité de temps et ensuite une ouverture de la ligne pendant une unité de temps ; (2) un trait, consistant en trois unités de temps de fermeture de la ligne et une unité d'ouverture ; (3) une lettre espace consistant en, disons, trois unités d'ouverture de la ligne ; (4) un mot espace de six unités d'ouverture de la ligne. On pourrait poser la restriction que les suites autorisées sont toutes les suites dans lesquelles aucune lettre espace n'en suit une autre (car si deux lettres espace se suivent, cela correspond à un mot espace). La question que nous considérons maintenant est celle de savoir comment on peut mesurer la capacité d'un tel canal pour transmettre de l'information.

Dans le télétype où tous les symboles ont la même durée, et dans lequel toute suite des 32 symboles est autorisée, il est facile de répondre. Chaque symbole représente cinq bits d'information. Si le système transmet $n$ symboles par seconde, il est naturel de dire que le canal a une capacité de $5n$ bits par seconde. Cela ne signifie pas que le canal du télétype sera toujours en train de transmettre de l'information à ce taux, c'est le taux maximum possible et le fait que le taux effectif atteigne ce taux maximum dépend de la source d'information qui nourrit le canal, comme cela apparaîtra ultérieurement.

Dans le cas plus général où il y a différentes longueurs de symboles ainsi que des contraintes sur les suites autorisées, on pose la définition suivante :

Définition : La capacité $C$ d'un canal discret est donnée par

$$C = \lim_{T \to \infty} \frac{\log N(T)}{T}$$

où $N(T)$ est le nombre de signaux autorisés de durée $T$.

On voit facilement que dans le cas du télétype, cela se réduit au résultat précédent. On peut montrer que la limite en question sera un nombre fini dans la plupart des cas présentant un intérêt. Supposons que toutes les suites des symboles $S_1, ..., S_n$, soient autorisées et que ces symboles aient

pour durées $t_1, \ldots, t_n$. Quelle est la capacité du canal ? Si $N(t)$ représente le nombre de suites de durée $t$, on a

$$N(t) = N(t - t_1) + N(t - t_2) + \ldots + N(t - t_n).$$

Le nombre total est égal à la somme des nombres de suites se terminant dans $S_1, S_2, \ldots, S_n$ et il y en a $N(t - t_1), N(t - t_2)...., N(t - t_n)$, respectivement. Selon un résultat bien connu dans les différences finies, $N(t)$ tend alors asymptotiquement pour de grandes valeurs de $t$ vers $X_0^t$ où $X_0$ est la plus grande solution réelle de l'équation caractéristique :

$$X^{-t_1} + X^{-t_2} + \ldots + X^{-t_n} = 1$$

et par conséquent

$$C = \log X_0.$$

Dans le cas où il y a des restrictions sur les suites autorisées, on peut encore souvent obtenir une équation aux différences de ce type et trouver $C$ à partir de l'équation caractéristique. Dans le cas de la télégraphie mentionné précédemment

$$N(t) = N(t-2) + N(t-4) + N(t-5) + N(t-7) + N(t-8) + N(t-10)$$

comme on le voit en comptant les suites de symboles selon le dernier ou l'avant-dernier symbole. Par conséquent, $C$ est égal à $-\log \mu_0$ où $\mu_0$ est la racine positive de $1 = \mu^2 + \mu^4 + \mu^5 + \mu^7 + \mu^8 + \mu^{10}$. En résolvant cela, on trouve $C = 0.539$.

Un type très général de restriction qu'on peut placer sur les séquences autorisées est le suivant : imaginons un nombre d'états possibles $a_1, a_2, \ldots, a_m$. Pour chaque état, seuls certains symboles de l'ensemble $S_1, ..., S_n$ peuvent être transmis (différents sous-ensembles pour les différents états). Quand l'un d'eux a été transmis, l'état devient un nouvel état dépendant à la fois de l'état précédent et du symbole particulier transmis. Le cas du télégraphe est un exemple simple de cela. Il y a deux états dépendant du fait qu'un espace ait été transmis en dernier ou pas. Si oui, alors seul un point ou un trait peut être envoyé ensuite et l'état change systématiquement. Sinon, tout symbole peut être transmis et l'état change si un espace est transmis, sinon, l'état reste le même. Les conditions peuvent être indiquées dans un graphique linéaire comme celui montré dans la Fig. 2. Les sommets du graphe correspondent aux états et les arêtes indiquent les symboles possibles dans un état et l'état résultant. En Appendice 1, on montre que si les conditions sur les suites autorisées peuvent être décrites sous cette forme, $C$ existe et peut être calculé selon le résultat suivant :

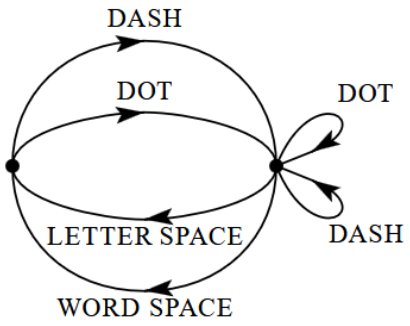



FIG. 2 : Représentation graphique des contraintes sur les symboles d'un télégraphe.

*Théorème 1 : Soit $b_{ij}^{(s)}$ la durée du $s^{\text{ième}}$ symbole qui est autorisé dans l'état $i$ et qui mène à l'état $j$. Alors la capacité du canal $C$ est égale à $\log W$ où $W$ est la plus grande racine réelle de l'équation déterminant :*

$$\left| \sum_s W^{-b_{ij}^{|s|}} - \delta_{ij} \right| = 0$$

où $\delta_{ij} = 1$ si $i = j$ et est nul sinon.

Par exemple, dans le cas du télégraphe (Fig. 2), le déterminant est :

$$\begin{vmatrix} -1 & (W^{-2} + W^{-4}) \\ (W^{-3} + W^{-6}) & (W^{-2} + W^{-4} - 1) \end{vmatrix} = 0.$$

Par développement, cela mène à l'équation donnée ci-dessus pour ce cas.

## 2. La source discrète de l'information

On a vu que sous certaines conditions très générales, le logarithme du nombre de signaux possibles dans un canal discret croît linéairement avec le temps. La capacité de transmettre de l'information peut être spécifiée en donnant le taux de cet accroissement, le nombre de bits par secondes requis pour spécifier le signal particulier qui a été utilisé.

Considérons maintenant la source d'information. Comment doit-on décrire mathématiquement la source d'information, et combien d'information, en bits par seconde, est produite dans une source donnée ? Le problème principal est l'effet de la connaissance statistique que l'on a de la source pour réduire la capacité requise par le canal, en utilisant un encodage correct de l'information. En télégraphie, par exemple, les messages à transmettre sont constitués de suites de lettres. Ces séquences, pourtant, ne sont pas complètement aléatoires. En général, elles forment des suites et ont une structure statistique de, disons la langue anglaise. Le lettre E est plus fréquente que la lettre Q, la suite TH plus fréquente que la suite XP, etc. L'existence de cette structure permet d'effectuer une économie en temps (ou en capacité du canal) en encodant correctement les suites du message en suites de signaux. Ceci est déjà fait dans une certaine mesure en télégraphie en utilisant le symbole de canal le plus court, un point, pour la lettre la plus fréquente en anglais, la lettre E ; alors que les lettres non fréquentes, Q, X, Z sont représentées par des séquences plus longues de points et traits. Cette idée est encore utilisée dans certains codes commerciaux où les mots et les phrases communs sont représentés par des groupes de code de quatre ou cinq lettres avec un temps moyen économisé considérable. Les salutations standardisées et les télégrammes d'anniversaire utilisent maintenant beaucoup cette idée de l'encodage d'une ou deux phrases en une suite relativement courte de nombres.

On peut penser à la source discrète comme générant le message, symbole par symbole. Elle choisira les symboles successifs selon certaines probabilités dépendant, en général, des choix précédents ainsi que des symboles particuliers en question. Un système physique, ou un modèle mathématique d'un système qui produit une telle séquence de symboles vérifiant un certain ensemble de probabilités est

appelé processus stochastique [3]. On peut considérer une source discrète, par conséquent, comme étant représentée par un processus stochastique. Inversement, tout processus stochastique qui produit une séquence discrète de symboles choisis dans un ensemble fini peut être considéré comme une source discrète. Cela inclura des cas comme :

1. les langages naturels écrits comme l'anglais, l'allemand, le chinois.

2. les sources d'information continues qui ont été discrétisées par un processus de quantification. Par exemple, le discours quantifié d'un transmetteur MIC, ou un signal télévisuel quantifié.

3. les cas mathématiques où l'on définit simplement abstraitement un processus stochastique qui engendre une suite de symboles. Les exemples qui suivent appartiennent à cette dernière sortes de source.

   (A) Supposons que l'on ait cinq lettres A, B, C, D, E qui sont choisies avec une probabilité égale à 0.2, les choix successifs étant indépendants. Cela amènerait à une suite de lettres dont celle ci-dessous est un exemple-type.

   BDCBCECCCADCBDDAAECEEAABBDAEECACEBCEAD.

   Elles ont été construites en utilisant une table de nombres aléatoires. [4]

   (B) En utilisant les mêmes cinq lettres, utilisons les probabilités $0.4, 0.1, 0.2, 0.2, 0.1$, respectivement, avec choix successifs indépendants. Un message typique d'une telle source peut être :

   AAACDCBDCEAADADACEDAEADCABEDADDCECAAAAAD.

   (C) Une structure plus compliquée est obtenue si les symboles successifs ne sont pas choisis indépendamment mais si leurs probabilités dépendent des lettres précédentes. Dans le cas le plus simple de ce type, un choix dépend seulement de la lettre précédente et non de celles qui précèdent cette dernière. La structure statistique peut alors être décrite par un ensemble de probabilités de transition $p_i(j)$, la probabilité que la lettre $i$ soit suivie par la lettre $j$. Les indices $i$ et $j$ parcourent le domaine des symboles possibles. Une seconde manière équivalente de spécifier la structure est de donner les probabilités sous la forme de "digrammes", $p(i,j)$ étant la fréquence relative du digramme $ij$. Les fréquences de lettres $p(i)$, (la probabilité de la lettre $i$), les probabilités de transition $p_i(j)$ et les probabilités des digrammes $p(i,j)$ sont liées par les formules suivantes :

$$\begin{aligned} p(i) &= \sum_j p(i,j) = \sum_j p(j,i) = \sum_j p(j)p_j(i) \\ p(i,j) &= p(i)p_i(j) \\ \sum_j pi(j) &= \sum_j p(i) = \sum_{i,j} p(i,j) = 1 \end{aligned}$$

[3] Voir, par exemple, S. Chandrasekhar, "Stochastic Problems in Physics and Astronomy", *Reviews of Modern Physics*, v. 15, No. 1, January 1943, p. 1.

[4] Kendall and Smith, *Tables of Random Sampling Numbers*, Cambridge, 1939.

Comme exemple spécifique, supposons qu'on a les trois lettres A, B, C avec les tables de probabilité :

| $p_i(j)$ | | $j$ | | |
|---|---|---|---|---|
| | | A | B | C |
| $i$ | A | 0 | $\frac{4}{5}$ | $\frac{1}{5}$ |
| | B | $\frac{1}{2}$ | $\frac{1}{2}$ | 0 |
| | C | $\frac{1}{2}$ | $\frac{2}{5}$ | $\frac{1}{10}$ |

| $i$ | $p(i)$ |
|---|---|
| A | $\frac{9}{27}$ |
| B | $\frac{16}{27}$ |
| C | $\frac{2}{27}$ |

| $p(i,j)$ | | $j$ | | |
|---|---|---|---|---|
| | | A | B | C |
| $i$ | A | 0 | $\frac{4}{15}$ | $\frac{1}{15}$ |
| | B | $\frac{8}{27}$ | $\frac{8}{27}$ | 0 |
| | C | $\frac{1}{27}$ | $\frac{4}{135}$ | $\frac{1}{135}$ |

Un message typique à partir de cette source est le suivant :

ABBABABABABABABBBABBBBBABABABABABBBACACABBABBBBABBABA.

La prochaine augmentation de la difficulté impliquera les fréquences des trigrammes mais pas davantage. Le choix d'une lettre dépendra des deux lettres précédentes mais pas sur le message avant ce point. Un ensemble de fréquences de trigrammes $p(i,j,k)$ ou, de façon équivalente, un ensemble de probabilités de transition $p_{ij}(k)$ serait nécessaire. En continuant sur cette voie, on obtient successivement des processus stochastiques plus compliqués. Dans le cas général du $n$-gramme, un ensemble de probabilités de $n$-grammes $p(i_1, i_2, ..., i_n)$ ou bien des probabilités de transition $p_{i_1,i_2,...,i_{n-1}}(i_n)$ sont nécessaires pour spécifier la structure statistique.

(D) Des processus stochastiques peuvent également être définis qui produisent un texte consistant en une suite de "mots." Supposons qu'on ait les cinq lettres A, B, C, D, E et 16 "mots" du langage avec leur probabilité associée :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0.10 | A | 0.16 | BEBE | 0.11 | CABED | 0.04 | DEB |
| 0.04 | ADEB | 0.04 | BED | 0.05 | CEED | 0.15 | DEED |
| 0.05 | ADEE | 0.02 | BEED | 0.08 | DAB | 0.01 | EAB |
| 0.01 | BADD | 0.05 | CA | 0.04 | DAD | 0.05 | EE |

Supposons que les "mots" successifs sont choisis indépendamment et sont séparés par des espaces. Un message typique pourrait être :

DAB EE A BEBE DEED DEB ADEE ADEE EE DEB BEBE BEBE BEBE ADEE BED DEED DEED CEED ADEE A DEED DEED BEBE CABED BEBE BED DAB DEED ADEB,

Si tous les mots sont de longueur finie, ce processus est équivalent à celui du type précédent, mais la description peut être plus simple en termes de structure des mots et probabilités. On peut aussi généraliser ici et introduire des probabilités de transition entre les mots, etc.

Ces langages artificiels sont utiles pour construire des problèmes simples et des exemples pour illustrer les diverses possibilités. On peut aussi approcher d'un langage naturel en utilisant une suite de langages artificiels. L'approximation à l'ordre zéro est obtenue en choisissant

toutes les lettres avec la même probabilité indépendamment. L'approximation à l'ordre un est obtenue en choisissant les lettres successives indépendamment mais chaque lettre a la même probabilité qu'elle a dans le langage naturel [5]. Ainsi, dans l'approximation à l'ordre un de l'anglais, E est choisie avec une probabilité de 0.12 (sa fréquence en anglais courant) et W a une probabilité de 0.02, mais il n'y a pas d'influence entre des lettres adjacentes et aucune tendance à former des digrammes préférentiels comme TH, ED, etc. Dans l'approximation du second ordre, la structure de digramme est introduite. Après qu'une lettre ait été choisie, la lettre suivante est choisie en accord avec les fréquences que suivent les différentes lettres pour suivre la première lettre en question. Cela nécessite d'avoir une table des fréquences des digrammes $p_i(j)$. Dans l'approximation d'ordre trois, la structure des trigrammes est introduite. Chaque lettre est choisie avec des probabilités dépendant des deux lettres précédentes.

## 3. Les suites d'approximations de la langue anglaise

Pour donner une idée visuelle de la façon dont cette suite de processus approxime un langage, des suites typiques dans les approximations de la langue anglaise ont été construites et sont fournies ci-dessous. Dans tous les cas, on a supposé un "alphabet" de 27 symboles, les 26 lettres et l'espace.

1. approximation à l'ordre 0 (symboles indépendants et équiprobables).

   XFOML RXKHRJFFJUJ ZLPWCFWKCYJ FFJEYVKCQSGHYD QPAAMK-BZAACIBZLHJQD.

2. approximation à l'ordre 1 (symboles indépendants mais avec les fréquences de textes anglais).

   OCRO HLI RGWR NMIELWIS EU LL NBNESEBYA TH EEI ALHE OOBTTVA NAH BRL.

3. approximation à l'ordre 2 (structure des digrammes comme en anglais).

   ON IE ANTSOUTINYS ARE T INCTORE ST BE S DEAMY ACHIN D ILONASIVE TU-COOWE AT TEASONARE FUSO TIZIN ANDY TOBE SEACE CTISBE.

4. approximation à l'ordre 3 (structure des trigrammes comme en anglais).

   IN NO IST LAT WHEY CRATICT FROURE BIRS GROCID PONDE-NOME OF DEMONSTURES OF THE REPTAGIN IS REGOACTIONA OF CRE.

5. approximation au premier ordre par des mots. Plutôt que de continuer avec les tétragrammes, voire la structure de $n$-grammes, il est plus facile et mieux à ce point-là du discours

[5] Les fréquences des lettres, digrammes, trigrammes sont fournies dans le livre *Secret and Urgent* de Fletcher Pratt, Blue Ribbon Books, 1939. Des tableaux des fréquences des mots sont fournis dans *Relative Frequency of English Speech Sounds*, G. Dewey, Harvard University Press, 1923.

de sauter aux unités mots. Ici les mots sont choisis indépendamment mais avec leurs fréquences appropriées.

REPRESENTING AND SPEEDILY IS AN GOOD APT OR COME CAN DIFFERENT NATURAL HERE HE THE A IN CAME THE TO OF TO EXPERT GRAY COME TO FURNISHES THE LINE MESSAGE HAD BE THESE.

6. approximation à l'ordre 2 par mots. Les probabilités de transitions entre mots sont correctes mais on ne rajoute pas davantage de structure.

   THE HEAD AND IN FRONTAL ATTACK ON AN ENGLISH WRITER THAT THE CHARACTER OF THIS POINT IS THEREFORE ANOTHER METHOD FOR THE LETTERS THAT THE TIME OF WHO EVER TOLD THE PROBLEM FOR AN UNEXPECTED.

La ressemblance avec l'anglais ordinaire augmente assez notablement à chacune des étapes ci-dessus. Notons que ces exemples ont une structure raisonnablement bonne d'environ deux fois le domaine qui est pris en compte dans leur construction. Par conséquent, en (3), le processus statistique assure un texte raisonnable par rapport aux suites de deux lettres, mais des suites de quatre lettres prise dans l'exemple peuvent habituellement se rencontrer dans des phrases du langage courant. Pour ce qui est de (6), les suites de quatre mots ou plus peuvent aisément être placées dans des phrases sans constructions inhabituelles. La suite particulière de 10 mots "attack on an English writer that the character of this" n'est pas du tout déraisonnable. Il apparaît alors qu'un processus stochastique suffisamment complexe donnera une représentation satisfaisante d'une source discrète.

Les deux premiers exemples ont été construits en utilisant le livre des nombres aléatoires en conjonction avec une table des fréquences des lettres (pour l'exemple 2). Cette méthode aurait pu être poursuivie pour (3), (4) et (5), puisque les digrammes, les trigrammes, et les tables de fréquences de mots sont disponibles, mais on a utilisé une méthode équivalente et plus simple.

Pour construire (3) par exemple, on ouvre un livre au hasard et on sélectionne une lettre au hasard sur la page. Cette lettre est enregistrée. On ouvre alors le livre à une autre page jusqu'à ce que cette lettre soit rencontrée. On enregistre alors la lettre qui la suit. On ouvre le livre à une autre page, on recherche la seconde lettre, et on enregistre la lettre qui la suit, etc. Un processus similaire a été utilisé pour (4), (5) et (6). Il serait intéressant de cons-truire d'autres approximations, mais le travail que cela nécessite devient énorme à la prochaine étape.

## 4. Représentation graphique d'un processus de Markoff

Les processus stochastiques du type décrit ci-dessus sont en mathématiques communément

appelés processus discrets de Markoff et ils ont été intensivement étudiés dans la littérature [6]. Le cas général peut être décrit comme suit : il existe un nombre fini d'"états" possibles d'un système ; $S_1, S_2, \ldots, S_n$. De plus, il y a un ensemble de probabilités de transition : $p_i(j)$ est la probabilité que si le système est dans l'état $S_i$, il sera ensuite dans l'état $S_j$. Pour faire de ce processus de Markoff une source d'information, on a seulement besoin de supposer qu'une lettre est produite pour chaque transition à partir d'un certain état vers un autre. Les états correspondent au "résidu d'influence" des lettres précédentes.

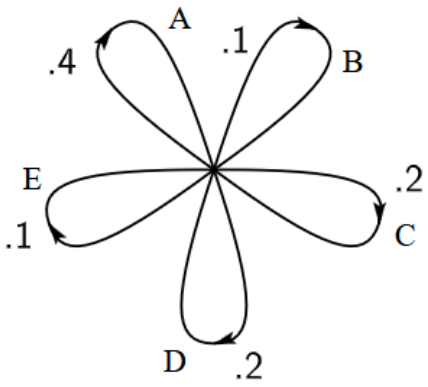



FIG. 3 : Un graphe correspondant à la source dans l'exemple B.

La situation peut être représentée graphiquement comme on le montre sur les Figs. 3, 4 et 5. Les "états" sont les sommets dans le graphe et les probabilités et les lettres produites par une transition sont données le long de la ligne correspondante. La Figure 3 est l'illustration de l'exemple B dans la Section 2, alors que la Fig. 4 correspond à l'exemple C. Dans la Fig. 3, il y a seulement un état puisque les lettres successives sont indépendantes. Dans la Fig. 4, il y a autant d'états que de lettres. Si un exemple de trigramme était construit, il y aurait au plus $n^2$ états correspondant aux paires possibles de lettres précédant la lettre qui a été choisie. La Figure 5 est un graphe pour le cas de la structure de mots dans l'exemple D. Ici $S$ correspond au symbole "espace".

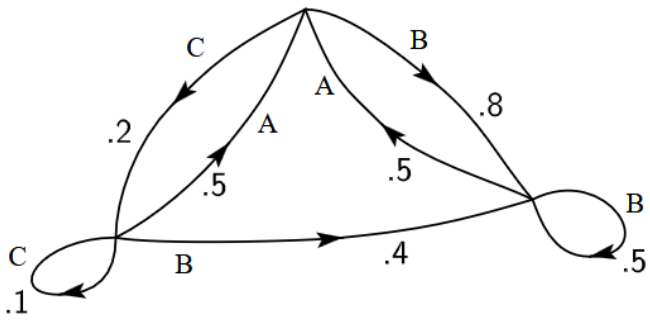



FIG. 4 : Un graphe correspondant à la source dans l'exemple C.

[6]Pour un traitement détaillé, voir M. Fréchet, Méthode des fonctions arbitraires. *Théorie des événements en chaîne dans le cas d'un nombre fini d'états possibles.* Paris, Gauthier-Villars, 1938.

## 5. Sources ergodiques et mixtes

Comme on l'a indiqué ci-dessus, une source discrète pour nos objectifs peut être représentée par un processus de Markoff. Parmi les processus de Markoff discrets, un groupe a des propriétés particulièrement importantes en théorie de la communication. Cette classe spéciale contient les processus "ergodiques" et on appellera les sources correspondantes les sources ergodiques. Bien qu'une définition rigoureuse d'un processus ergodique entre en ligne de compte, l'idée générale est simple. Dans un processus ergodique, toute suite produite par le processus a les mêmes propriétés statistiques. Ainsi les fréquences de lettre, les fréquences de digrammes, etc., obtenues à partir de suites particulières, approcheront, au fur et à mesure que les longueurs des suites s'accroissent, des limites définies indépendantes de la suite particulière considérée. En fait, ceci n'est pas vrai pour toute suite mais l'ensemble pour lequel cela est faux est de probabilité zéro. Grossièrement, la propriété d'ergodicité signifie homogénéité statistique.

Tous les exemples des langages artificiels donnés ci-dessus sont ergodiques. Cette propriété est liée à la structure du graphe correspondant. Si le graphe a les deux propriétés suivantes [7] le processus correspondant sera ergodique :

1. Le graphe n'est pas constitué de deux parties isolées A et B telles qu'il est impossible d'aller de sommets dans la partie A vers des sommets dans la partie B le long d'arêtes du graphe dans la direction des flèches et également impossible d'aller de sommets dans la partie B vers des sommets de la partie A.
2. Une suite fermée d'arêtes dans le graphe avec toutes les flèches sur les arêtes dirigées dans le même sens sera appelé un "circuit." La "longueur" d'un circuit est son nombre d'arêtes. Ainsi dans la Fig. 5, la suite BEBES est un circuit de longueur 5. La seconde propriété requise est que le plus grand commun diviseur des longueurs de tous les circuits dans le graphe soit 1.

Si la première condition est satisfaite mais si la seconde ne l'est pas en ayant un pgcd égal à $d > 1$, les suites ont un certain type de structure périodique. Les différentes suites tombent dans $d$ différentes classes qui sont statistiquement la même à un décalage depuis l'origine près (i.e. dont la lettre dans la séquence est appelée la lettre 1). Par un décalage de 0 à $d-1$, toute suite peut être rendue équivalente à n'importe quelle autre. Un simple exemple avec $d = 2$ est le suivant : il y a trois lettres possibles a, b, c. La lettre a est suivie soit par b soit par c avec les probabilités $\frac{1}{3}$ et $\frac{2}{3}$respectivement. Soit b, soit c est toujours suivie d'une lettre a. Ainsi, une suite typique est

abacacacabacababacac.

Ce type de situation n'a pas beaucoup d'importance pour notre travail.

[7] Ce sont des ré-énoncés en fonction du graphe de conditions fournies dans le livre de Fréchet.

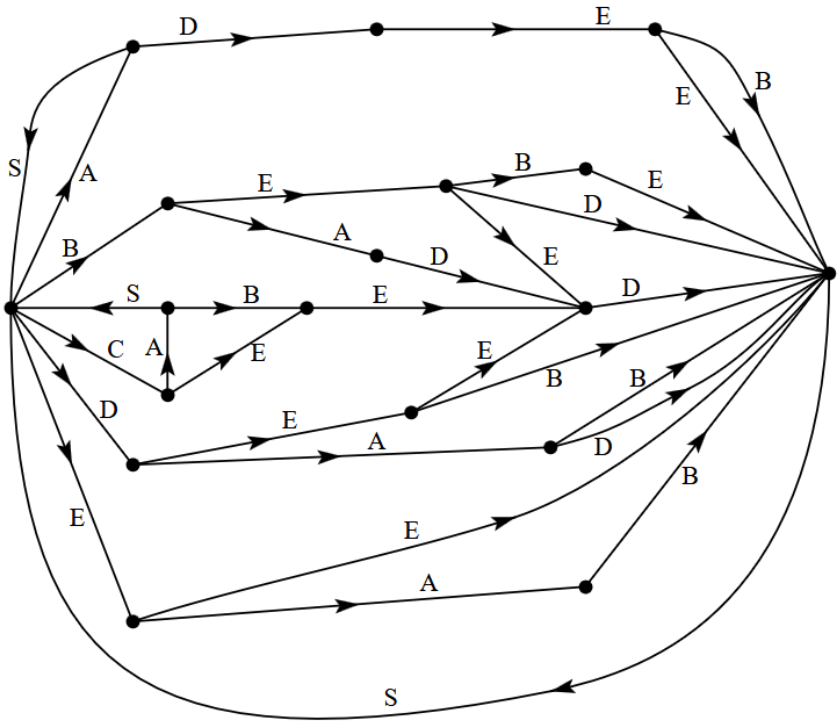



FIG. 5 : Un graphe correspondant à la source dans l'exemple D.

Si la première condition est violée, le graphe peut être séparé en un ensemble de sous-graphes, dont chacun vérifie la première condition. On supposera que la seconde condition est également satisfaite par chaque sous-graphe. On a dans ce cas ce que l'on peut appeler une source "mixte" constituée d'un certain nombre de composantes pures. Les composantes correspondent aux différents sous-graphes. Si $L_1, L_2, L_3$, sont les composantes sources, on peut écrire

$$L = p_1 L_1 + p_2 L_2 + p_3 L_3 + \ldots$$

où $p_i$ est la probabilité de la composante source $L_i$.

Physiquement, la situation représentée est celle-ci : il y a plusieurs différentes sources $L_1, L_2, L_3, ...$ qui sont chacune de structure statistique homogène (i.e. elles sont ergodiques). On ne sait pas a priori laquelle doit être utilisée, mais une fois que la séquence démarre avec une composante pure donnée $L_i$, elle continue indéfiniment selon la structure statistique de cette composante.

Comme exemple, on peut prendre deux des processus définis ci-dessus et supposer $p_1 = 0.2$ et $p_2 = 0.8$. Une suite à partir d'une source mixte

$$L = 0.2\ L_1 + 0.8\ L_2$$

serait obtenue en choisissant d'abord $L_1$ ou $L_2$ avec les probabilités 0.2 and 0.8 et après ce choix, en générant une suite à partir d'une suite quelconque qui a été choisie.

Excepté lorsqu'on spécifie le contraire, supposons qu'une source soit ergodique. Cette supposition nous rend capables d'identifier des moyennes le long d'une suite à des moyennes sur l'ensemble des suites possibles (la probabilité d'une divergence étant nulle). Par exemple, la fréquence relative de la lettre A dans une suite particulière infinie sera, avec probabilité 1, égale à sa fréquence relative dans l'ensemble des suites.

Si $P_i$ est la probabilité de l'état $i$ et $p_i(j)$ la probabilité de transition vers l'état $j$, alors, pour que le processus soit stationnaire, il est clair que les $P_i$ doivent satisfaire les conditions d'équilibre :

$$P_j = P_i p_i(j).$$

Dans le cas ergodique, on peut montrer qu'avec n'importe quelles conditions au départ, les probabilités $P_j(N)$ d'être dans l'état $j$ après $N$ symboles, approchent les valeurs d'équilibre lorsque $N \to \infty$.

## 6. Choix, incertitude et entropie

On a représenté une source d'information discrète comme un processus de Markoff. Peut-on définir une quantité qui mesurera, dans un certain sens, combien d'information est "produite" par un tel processus, ou mieux, à quel niveau l'information est-elle produite ?

Supposons que l'on ait un ensemble d'événements possibles dont les probabilités d'occurrence soient $p_1, p_2, \ldots, p_n$. Ces probabilités sont connues mais c'est tout ce que l'on sait concernant la susceptibilité d'un événement de se produire. Peut-on trouver une mesure de la façon dont tel "choix" intervient dans la sélection de l'événement ou de l'incertitude de la sortie ?

Si une telle mesure existe, disons $H(p_1, p_2, \ldots, p_n)$, il est raisonnable d'exiger d'elle qu'elle ait les propriétés suivantes :

1. $H$ devrait être une fonction continue des $p_i$.
2. Si tous les $p_i$ sont égaux, $p_i = \frac{1}{n}$ alors $H$ devrait être une fonction croissante monotone de $n$. Avec des événements également probables, il y a plus de choix, ou d'incertitude, quand il y a davantage d'événements.
3. Si un choix est scindé en deux choix successifs, le $H$ original devrait être la somme pondérée des valeurs individuelles de $H$. La signification de cela est illustrée dans la Fig. 6. Sur la gauche, on a trois

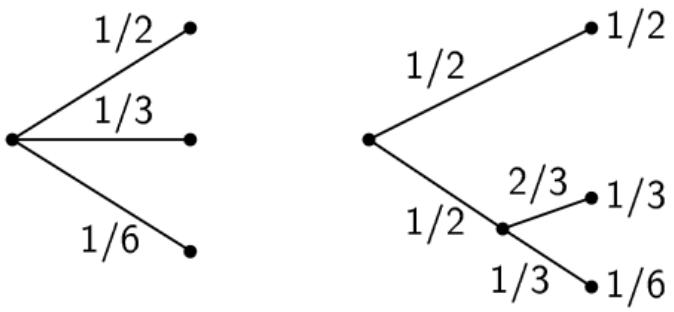


FIG. 6 : Décomposition d'un choix à partir de trois possibilités.

possibilités $p_1 = \frac{1}{2},\ p_2 = \frac{1}{3},\ p_3 = \frac{1}{6}$. Sur la droite, on a d'abord choisi entre deux possibilités chacune ayant sa probabilité, et si la seconde advient, on fait un autre choix avec les probabilités $\frac{2}{3}, \frac{1}{3}$. Les résultats finaux ont les mêmes probabilités que précédemment. On requiert dans ce cas particulier que

$$H\left(\frac{1}{2}, \frac{1}{3}, \frac{1}{6}\right) = H\left(\frac{1}{2}, \frac{1}{2}\right) + \frac{1}{2} H\left(\frac{2}{3}, \frac{1}{3}\right).$$

Le coefficient est $\frac{1}{2}$ parce que ce second choix a lieu seulement la moitié du temps.

Dans l'Appendice 2, le résultat suivant est établi :

*Théorème 2 : Le seul $H$ satisfaisant les trois énoncés ci-dessus est de la forme :*

$$H = -K \sum_{i=1}^{n} p_i \log p_i$$

*où $K$ est une constante positive.*

Ce théorème, et les hypothèses requises pour sa preuve, ne sont en aucun cas nécessaires pour la présente théorie. Il est principalement donné pour assurer une certaine plausibilité à quelques-unes de nos dernières définitions. La réelle justification de ces définitions, pourtant, résidera dans ce qu'elles impliquent.

Les quantités de la forme $H = -\sum p_i \log p_i$ (la constante $K$ correspond simplement au choix d'une unité de mesure) joue un rôle central dans la théorie de l'information en tant que mesures de l'information, choix et incertitude. La forme de $H$ sera reconnue comme celle de l'entropie telle que définie dans certaines formulations de la mécanique statistique [8] où $p_i$ est la probabilité d'un système d'être dans la cellule $i$ de son espace des phases. $H$ est alors, par exemple, le $H$ du célèbre théorème de Boltzmann. On appellera $H = -\sum p_i \log p_i$ l'entropie d'un ensemble de probabilités $p_1, ..., p_n$. Si $x$ est une variable aléatoire, on écrira $H(x)$ pour son entropie ; ainsi $x$ n'est pas un argument d'une fonction mais une étiquette pour un nombre, pour le différencier de $H(y)$ disons, l'entropie de la variable aléatoire $y$.

L'entropie dans le cas de deux possibilités $p$ et $q = 1 - p$ notamment

$$H = -(p \log p + q \log q)$$

est dessinée dans la Fig. 7 comme une fonction de $p$.

[8] Voir, par exemple, R. C. Tolman, *Principles of Statistical Mechanics*, Oxford, Clarendon, 1938.

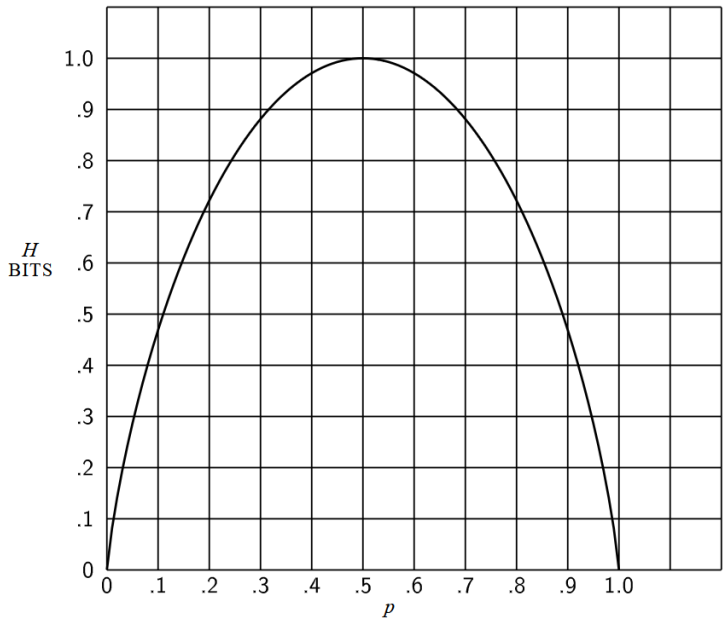



FIG. 7 : L'entropie dans le cas de deux possibilités de probabilités $p$ et $1-p$

La quantité $H$ a un certain nombre de propriétés intéressantes qui en feront une mesure raisonnable du choix ou de l'information.

1. $H = 0$ si et seulement si tous les $p_i$ sauf un sont nuls, ce dernier valant un. Ceci seulement lorsqu'on est certain que la sortie fait s'évanouir $H$. Sinon, $H$ est positif.
2. Pour un $n$ donné, $H$ est un maximum et il est égal à $\log n$ quand tous les $p_i$ sont égaux (i.e. $\frac{1}{n}$). Ceci est aussi intuitivement la situation la plus incertaine.
3. Supposons qu'il y ait deux événements, $x$ et $y$, considérés, avec $m$ possibilités d'advenir pour le premier et $n$ pour le second. Soit $p(i,j)$ la probabilité de l'occurrence conjointe avec valeur $i$ pour le premier et $j$ pour le second. L'entropie de l'événement conjoint est

$$H(x,y) = -\sum_{i,j} p(i,j) \log p(i,j)$$

alors que

$$\begin{aligned} H(x) &= -\sum_{i,j} p(i,j) \log \sum_{j} p(i,j) \\ H(y) &= -\sum_{i,j} p(i,j) \log \sum_{i} p(i,j). \end{aligned}$$

On montre facilement que

$$H(x,y) \leq H(x) + H(y)$$

avec égalité seulement si les événements sont indépendants (i.e. $p(i,j) = p(i)p(j)$). L'incertitude d'un événement conjoint est inférieure ou égale à la somme des incertitudes individuelles.

4. N'importe quel changement en vue d'une égalisation des probabilités $p_1, p_2, \ldots, p_n$, accroît $H$. Ainsi, si $p_1 < p_2$ et qu'on fait augmenter $p_1$, en faisant décroître $p_2$ d'un montant égal de telle façon que $p_1$ et $p_2$ soient un peu plus égales, alors $H$ croît. Plus généralement, si l'on procède à n'importe quelle opération de "calcul de la moyenne" sur les $p_i$ de la forme

$$p_i' = \sum_j a_{ij} p_j$$

où $\sum_i a_{ij} = \sum_j a_{ij} = 1$, et tous les $a_{ij} \geq 0$, alors $H$ s'accroît (excepté dans le cas particulier où ces transformations ne font rien de plus qu'une permutation des $p_j$ avec $H$ restant bien sûr le même).

5. Supposons deux variables aléatoires, $x$ et $y$ comme dans 3, non nécessairement indépendantes. Pour une quelconque valeur particulière $i$ que $x$ peut prendre, il existe une probabilité conditionnelle $p_i(j)$ que $y$ ait la valeur $j$. Celle-ci est donnée par

$$p_i(j) = \frac{p(i,j)}{\sum_j p(i,j)}.$$

On définit l'entropie conditionnelle de $y$, $H_x(y)$ comme la moyenne des entropies de $y$ pour chaque valeur de $x$, pondérée selon la probabilité d'obtenir cette valeur particulière de $x$. C'est-à-dire

$$H_x(y) = \sum_{i,j} p(i,j) \log p_i(j).$$

Cette quantité mesure notre incertitude sur la valeur de $y$ en moyenne lorsque nous connaissons $x$. En substituant la valeur de $p_i(j)$, on obtient

$$\begin{aligned} H_x(y) &= -\sum_{i,j} p(i,j) \log p(i,j) + \sum_{i,j} p(i,j) \log \sum_j p(i,j) \\ &= H(x) - Hx(y). \end{aligned}$$

ou

$$H(x,y) = H(x) + H_x(y).$$

L'incertitude (ou l'entropie) de l'événement conjoint $x, y$ est l'incertitude de $x$ plus l'incertitude de $y$ quand $x$ est connue.

6. De 3 et 5, on a

$$H(x) + H(y) \geq H(x,y) = H(x) + H_x(y).$$

Par conséquent

$$H(y) \geq H_x(y).$$

L'incertitude de $y$ n'est jamais accrue par la connaissance de $x$. Elle décroîtra à moins que $x$ et $y$ ne soient des événements indépendants, auquel cas elle n'est pas modifiée.

## 7. L'entropie d'une source d'information

Considérons une source discrète de type états finis considérée ci-dessus. Pour chaque état possible $i$, il y aura un ensemble de probabilités $p_i(j)$ de produire les différents symboles possibles $j$. Il y a donc une entropie $H_i$ pour chaque état. L'entropie de la source sera définie comme la moyenne de ces $H_i$ pondérée selon la probabilité d'occurrence des états en question :

$$\begin{aligned} H &= \sum_i P_i H_i \\ &= -\sum_{i,j} P_i p_i(j) \log p_i(j). \end{aligned}$$

Ceci est l'entropie de la source par symbole du texte. Dans le processus de Markoff selon lequel le processus s'exécute à un certain rythme temporel défini, il y a aussi une entropie par seconde

$$H' = \sum_i f_i H_i$$

où les $f_i$ sont les fréquences moyennes (les occurrences par seconde) de l'état $i$. Clairement

$$H' = mH$$

où $m$ est le nombre moyen de symboles produits par seconde. $H$ ou $H'$ mesurent le montant d'information engendré par la source par symbole ou par seconde. Si la base du logarithme est 2, ils représenteront des nombres de bits par symbole ou par seconde.

Si les symboles successifs sont indépendants alors $H$ est simplement égal à $-\sum p_i \log p_i$ où $p_i$ est la probabilité du symbole $i$. Supposons que dans un tel cas, on considère un long message de $N$ symboles. Il contiendra avec une forte probabilité environ $p_1 N$ occurrences du premier symbole, $p_2 N$ occurrences du second, etc. Par conséquent, la probabilité de ce message particulier sera grosso modo

$$p = p_1^{p_1 N} p_2^{p_2 N} \ldots p_n^{p_n N}$$

ou

$$\log p \doteq N \sum_i p_i \log p_i$$

$$\log p \doteq -NH$$

$$H \doteq \frac{\log 1/p}{N}.$$

$H$ est donc approximativement le logarithme de la probabilité réciproque d'une suite longue typique divisée par le nombre de symboles dans la suite. Le même résultat existe quelle que soit la source. Dit plus précisément, on a (voir Appendice 3) :

*Théorème 3 : Soient donnés $\epsilon > 0$ et $\delta > 0$, on peut trouver un nombre $N_0$ tel que les séquences de n'importe quelle longueur $N \geq N_0$ soient séparables en deux classes :*

1. *Un ensemble dont la probabilité totale est inférieure à* $\epsilon$.
2. *Le reste, dont tous les éléments ont des probabilités satisfaisant l'inégalité*

$$\left| \frac{\log p^{-1}}{N} - H \right| < \delta.$$

En d'autres termes, on est presque certain d'avoir $\dfrac{\log p^{-1}}{N}$ très proche de $H$ quand $N$ est grand.

Un résultat lié et proche concerne le nombre de suites de probabilités diverses. Considérons à nouveau les suites de longueur $N$ et arrangeons-les selon un ordre de probabilité décroissante. On définit $n(q)$ comme le nombre que l'on doit prendre dans cet ensemble en commençant par le plus probable dans le but d'accumuler une probabilité totale $q$ pour les éléments pris.

*Théorème 4 :*

$$\operatorname*{Lim}_{N\to\infty} \frac{\log n(q)}{N} = H$$

*quand* $q$ *n'est pas égal à 0 ou 1.*

On peut interpréter $\log n(q)$ comme le nombre de bits requis pour spécifier la suite quand on considère seulement les suites les plus probables avec une probabilité totale égale à $q$. Alors $\dfrac{\log n(q)}{N}$ est le nombre de bits par symbole pour la spécification. Le théorème dit que pour une grande valeur de $N$, cela sera indépendant de $q$ et égal à $H$. Le taux d'accroissement du logarithme du nombre des suites raisonnablement probables est donné par $H$, indépendamment de notre interprétation des termes "raisonnablement probable." Du fait de ces résultats, qui sont démontrés dans l'appendice 3, il est possible pour la plupart des objectifs de traiter les suites longues comme s'il n'y avait que $2^{HN}$ d'entre elles, chacune avec une probabilité de $2^{-HN}$.

Les deux prochains théorèmes montrent que $H$ et $H'$ peuvent être déterminés en limitant les opérations directement à partir des statistiques des suites du message, sans référence aux états et aux probabilités de transition entre les états.

*Théorème 5 : Soit* $p(B_i)$ *la probabilité d'une suite* $B_i$ *de symboles de la source. Soit*

$$G_N = -\frac{1}{N} \sum_i p(B_i) \log p(B_i)$$

*où la somme se fait sur toutes les suites* $B_i$ *contenant* $N$ *symboles. Alors* $G_N$ *est une fonction monotone décroissante de* $N$ *et*

$$\operatorname*{Lim}_{N\to\infty} G_N = H.$$

*Théorème 6 : Soit* $p(B_i, S_j)$ *la probabilité que la séquence* $B_i$ *soit suivie par le symbole* $S_j$ *et* $P_{B_i}(S_j) = p(B_i, S_j)/p(B_i)$ *la probabilité conditionnelle de* $S_j$ *après* $B_i$. *Soit*

$$F_N = -\sum_{i,j} p(B_i, S_j) \log p_{B_i}(S_j)$$

*où la somme est prise sur tous les blocs $B_i$ de $N-1$ symboles et sur tous les symboles $S_j$. Alors $F_N$ est une fonction monotone décroissante de $N$,*

$$F_N = NG_N - (N-1)G_{N-1},$$

$$G_N = \frac{1}{N}\sum_{n=1}^{N} F_n,$$

$$F_N \leq G_N,$$

*et* $\mathrm{Lim}_{N\to\infty} F_N = H$.

Ces résultats sont démontrés dans l'appendice 3. Ils montrent qu'une suite d'approximations de $H$ peut être obtenue en considérant seulement la structure statistique des suites s'étendant sur $1, 2, ..., N$ symboles. $F_N$ est la meilleure approximation. En fait, $F_N$ est l'entropie de l'approximation au $N^{\text{ième}}$ ordre de la source du type discuté ci-dessus. S'il n'y a pas d'influences statistiques s'étendant sur plus de $N$ symboles, c'est-à-dire si la probabilité conditionnelle du symbole suivant connaissant les $(N-1)$ symboles précédents n'est pas changée par une connaissance de tout ce qui est avant cela, alors $F_N = H$. $F_N$ bien sûr est l'entropie conditionnelle du prochain symbole quand les $(N-1)$ symboles précédents sont connus, alors que $G_N$ est l'entropie par symbole des blocs de $N$ symboles.

Le rapport de l'entropie d'une source à la valeur maximum qu'elle pourrait avoir bien que toujours restreinte aux mêmes symboles sera dénommée son entropie relative. C'est la compression possible maximum quand on encode dans le même alphabet. La différence entre 1 et l'entropie relative est la redondance. La redondance de l'anglais de base, sans considérer la structure statistique sur des distances d'environ 8 lettres est d'environ 50%. Cela signifie que quand on écrit de l'anglais, la moitié de ce que l'on écrit est déterminé par la structure de la langue et l'autre moitié est choisie librement. Le ratio de 50% a été trouvé par plusieurs méthodes indépendantes qui ont toutes donné des résultats dans ce voisinage. L'une des méthodes consiste à calculer l'entropie des approximations de l'anglais. Une seconde méthode est d'effacer une certaine fraction de lettres à partir d'un exemple de texte anglais et alors d'essayer de laisser quelqu'un le retrouver. S'il est possible de retrouver le texte quand 50% du texte a été effacé, la redondance est supérieure à 50%. Une troisième méthode dépend de certains résultats connus en cryptographie.

Deux cas extrêmes de la redondance de la prose anglaise sont représentés par le livre The Basic English et par le livre de James Joyce "Finnegans Wake". Le vocabulaire de The Basic English est limité à 850 mots et la redondance est très élevée. Cela se reflète dans le développement qui a lieu quand un passage est traduit vers Basic English. Le texte de Joyce d'un autre côté élargit le vocabulaire et est allégé pour compresser son contenu sémantique. La redondance d'une langue est liée à l'existence de mots croisés. Si la redondance est nulle, toute séquence de lettres est un texte raisonnable dans cette langue et n'importe quel arrangement bi-dimensionnel de lettres forme un mot croisé. Si la redondance est trop élevée, la langue impose trop de contraintes pour que des mots croisés de grande taille puissent être

possibles. Une analyse plus détaillée montre que si l'on suppose que les contraintes imposées à la langue sont de nature plutôt chaotique et aléatoire, des mots croisés de grande taille sont possibles quand la redondance est 50%. Si la redondance est 33%, des mots croisés tri-dimensionnels devraient être possibles, etc.

## 8. Représentation des opérations d'encodage et de décodage

On doit encore représenter mathématiquement les opérations effectuées par l'émetteur et le récepteur pour encoder et décoder l'information. Chacun de ces opérateurs sera appelé un transducteur discret. L'entrée du transducteur est une suite de symboles en entrée et sa sortie une suite de symboles en sortie. Le transducteur peut avoir une mémoire interne de telle sorte que sa sortie dépende non seulement du symbole en entrée effectif mais également de l'histoire passée. On suppose que la mémoire interne est finie, i.e. qu'il existe un nombre fini $m$ d'états possibles du transducteur et que sa sortie est une fonction de l'état présent et du symbole effectivement en entrée. Ainsi un transducteur peut être décrit par deux fonctions :

$$y_n = f(x_n, \alpha_n)$$

$$\alpha_{n+1} = g(x_n, \alpha_n)$$

où

- $x_n$ est le $n^{\text{ième}}$ symbole,
- $\alpha_n$ est l'état du transducteur quand le $n^{\text{ième}}$ symbole en entrée est introduit,
- $y_n$ est le symbole en sortie (ou la suite de symboles en sortie) produit quand $x_n$ est introduit si l'état est $\alpha_n$.

Si les symboles en sortie d'un transducteur peuvent être identifiés avec les symboles en entrée d'un second transducteur, on peut les connecter en tandem et le résultat est également un transducteur. S'il existe un second transducteur qui opère sur la sortie du premier et retrouve l'entrée originale, le premier transducteur sera dit non singulier et le second sera appelé son inverse.

*Théorème 7 : la sortie d'un transducteur à états finis conduite par une source statistique d'états finis est une source statistique d'états finis, ayant pour entropie (par unité de temps) une entropie inférieure ou égale à celle de l'entrée. Si le transducteur est non singulier, les entropies sont égales.*

Soit $\alpha$ l'état de la source qui produit une suite de symboles $x_i$ ; et soit $\beta$ l'état du transducteur, qui produit, en sortie des blocs de symboles $y_j$. Le système combiné peut être représenté par l'"espace état produit" des paires $(\alpha, \beta)$. Deux points dans l'espace $(\alpha_1, \beta_1)$ et $(\alpha_2, \beta_2)$, sont reliés par une arête si $\alpha_1$ peut produire un $x$ qui change $\beta_1$ en $\beta_2$, et cette arête est affectée de la probabilité de ce $x$ dans ce cas. L'arête est étiquetée avec le bloc de $y_j$ symboles produits par le transducteur. L'entropie de la sortie peut être calculée comme une somme pondérée

sur les états. Si on somme sur $\beta$, chaque terme résultant est inférieur ou égal au terme correspondant pour $\alpha$, par conséquent, l'entropie ne croît pas. Si le transducteur est non singulier, connectons sa sortie au transducteur inverse. Si $H'_1, H'_2$, et $H'_3$ sont les entropies en sortie de la source, du premier et du second transducteurs respectivement, alors $H'_1 \geq H'_2 \geq H'_3 = H'_1$ et par conséquent $H'_1 = H'_2$.

Supposons qu'on ait un système de contraintes sur les suites possibles de ce type qui peuvent être représentées par un graphique linéaire comme dans la Fig. 2. Si des probabilités $p_{ij}^{(s)}$ étaient affectées aux différentes arêtes connectant l'état $i$ à l'état $j$, cela deviendrait une source. Il y a une affectation particulière qui maximise l'entropie résultante (voir l'appendice 4).

*Théorème 8 : Soit le système de contraintes considéré comme un canal ayant une capacité égale à* $C = \log W$. *Si l'on assigne*

$$p_{ij}^{(s)} = \frac{B_j}{B_i} W^{-\ell_{ij}^{(x)}}$$

*où* $\ell_{ij}^{(s)}$ *est la durée du* $s^{\text{ième}}$ *symbole amenant de l'état* $i$ *à l'état* $j$ *et où les* $B_i$ *satisfont*

$$B_i = \sum_{s,j} B_j W^{-\ell_{ij}^{(x)}}$$

*alors* $H$ *est maximisé et est égal à* $C$.

Par une affectation correcte des probabilités de transition, l'entropie des symboles sur un canal peut être maximisée jusqu'à atteindre la capacité du canal.

## 9. Le théorème fondamental pour un canal non bruité

Nous allons maintenant justifier notre interprétation de $H$ comme taux de l'information génératrice, en prouvant que $H$ détermine la capacité du canal requise avec le codage le plus efficace.

*Théorème 9 : Soit une source ayant pour entropie* $H$ *(bits par symbole) et soit un canal ayant pour capacité* $C$ *(bits par seconde). Alors il est possible d'encoder la sortie de la source de telle façon à transmettre au taux moyen* $\frac{C}{H} - \epsilon$ *symboles par seconde sur le canal où* $\epsilon$ *est arbitrairement petit. Il n'est pas possible de transmettre à un taux moyen supérieur à* $\frac{C}{H}$.

La partie inverse du théorème, que $\frac{C}{H}$ ne peut pas être excédé, peut se prouver en notant que l'entropie de l'entrée du canal par seconde est égale à celle de la source, puisque le transmetteur doit être non singulier, et en notant également que cette entropie ne peut excéder la capacité du canal. Par conséquent, $H' \leq C$ et le nombre de symboles par seconde $= H'/H \leq C/H$.

La première partie du théorème sera démontrée de deux manières différentes. La première méthode consiste à considérer l'ensemble de toutes les suites de $N$ symboles produites par la source. Pour $N$ grand, on peut diviser celles-ci en deux groupes, l'un contenant moins de $2^{(H+\eta)N}$ éléments, et le second en contenant moins de $2^{RN}$ (où $R$ est le logarithme du nombre de symboles différents) et ayant une probabilité totale inférieure à $\mu$. Lorsque $N$ croît, $\eta$ et $\mu$ approchent de zéro. Le nombre de signaux de durée $T$ dans le canal est plus grand que $2^{(C-\theta)T}$ avec $\theta$ petit quand $T$ est grand. Si on choisit

$$T = \left(\frac{H}{C} + \lambda\right) N$$

alors il y aura un nombre suffisant de suites de symboles de canal pour le groupe à forte probabilité quand $N$ et $T$ sont suffisamment grands (bien que $\lambda$ soit petit) et aussi d'autres additionnels. Le groupe de probabilité élevée est codé d'une manière arbitraire bijective vers cet ensemble. Les suites restantes sont représentées par des suites plus grandes, commençant et se terminant par l'une des suites non utilisée pour le groupe de probabilité élevée. Cette suite particulière agit comme un signal démarrer-arrêter pour un code différent. Entre temps, un temps suffisant est alloué pour fournir suffisamment de suites différentes pour tous les messages de probabilité basse. Cela nécessitera

$$T_1 = \left(\frac{R}{C} + \varphi\right) N$$

où $\varphi$ est petit. Le taux moyen de transmission en symboles de message par seconde sera alors plus grand que

$$\left[(1-\delta)\frac{T}{N} + \delta\frac{T_1}{N}\right]^{-1} = \left[(1-\delta)\left(\frac{H}{C} + \lambda\right) + \delta\left(\frac{R}{C} + \varphi\right)\right]^{-1}.$$

Lorsque $N$ croît, $\delta$, $\lambda$ et $\varphi$ s'approchent de zéro et le taux avoisine $\dfrac{C}{H}$.

Une autre méthode pour calculer ce codage et ainsi prouver le théorème peut être décrite comme suit : arranger les messages de longueur $N$ dans un ordre de probabilité décroissant et supposons que leurs probabilités sont $p_1 \geq p_2 \geq p_3 \geq \ldots \geq p_n$. Soit $P_s = \sum_1^{s-1} p_i$ ; c'est-à-dire que $P_s$ est la probabilité cumulée jusqu'à $p_s$ non incluse. On encode d'abord dans un système binaire. Le code binaire pour le message $s$ est obtenu en développant $P_s$ comme un nombre binaire. Le développement est mené jusqu'à $m_s$ places, où $m_s$ est l'entier satisfaisant :

$$\log_2 \frac{1}{p_s} \leq m_s < 1 + \log_2 \frac{1}{p_s}.$$

Ainsi les messages de probabilité haute sont représentés par des codes courts et ceux de probabilité basse sont représentés par des codes longs. De ces inégalités, on a

$$\frac{1}{2^{m_s}} \leq p_s < \frac{1}{2^{m_{s-1}}}.$$

Le code pour $P_s$ diffèrera de tous les codes ultérieurs selon une ou plusieurs de ses $m_s$ places, puisque toutes les $P_i$ restantes sont au moins $\frac{1}{2^{m_s}}$ fois plus grandes que leur développement binaire et par conséquent diffèrent dans leurs premières $m_s$ places. Par conséquent, tous les codes sont différents et il est possible de retrouver le message à partir de son code. Si les suites du canal ne sont pas déjà des suites de chiffres binaires, on peut les astreindre à l'être de façon arbitraire et le code binaire sera alors traduit en signaux adaptés au canal.

Le nombre moyen $H'$ de chiffres binaires utilisés par symbole du message original est facilement estimé. On a

$$H' = \frac{1}{N} \sum m_s p_s.$$

Mais,

$$\frac{1}{N} \sum \left( \log_2 \frac{1}{p_s} \right) p_s \leq \frac{1}{N} \sum m_s p_s < \frac{1}{N} \sum \left( 1 + \log_2 \frac{1}{p_s} \right) p_s$$

et par conséquent,

$$G_N \leq H' < G_N + \frac{1}{N}.$$

Lorsque $N$ croît, $G_N$ s'approche de $H$, l'entropie de la source, et $H'$ s'approche de $H$.

On voit à partir de cela que l'inefficacité du codage, lorsque seulement un retard limité de $N$ est utilisé, n'a pas besoin d'être plus grand que $\frac{1}{N}$ plus la différence entre l'entropie réelle $H$ et l'entropie $G_N$ calculée pour des suites de longueur $N$. Le pourcentage d'excès de temps nécessité par rapport à l'idéal est donc inférieur à

$$\frac{G_N}{H} + \frac{1}{HN} - 1.$$

Cette méthode d'encodage est substantiellement la même qu'une méthode découverte indépendamment par R. M. Fano [9]. Sa méthode consiste à arranger les messages de longueur $N$ dans un ordre décroissant de probabilité. Diviser cette série en deux groupes de probabilités aussi proches l'une de l'autre que possible. Si le message est dans le premier groupe, le chiffre binaire sera 0, sinon, ce sera 1. Les groupes sont similairement divisés en deux sous-ensembles de probabilités presque égales et l'ensemble particulier détermine le second chiffre binaire. Ce processus est répété jusqu'à ce que chaque sous-ensemble ne contienne qu'un seul message. On voit aisément qu'à part des différences mineures (en général, le dernier chiffre), cela revient au même que le processus arithmétique qui a été décrit ci-dessus.

## 10. Discussion et exemples

Pour obtenir un transfert de puissance maximum d'un générateur de message à sa cible, un transcodeur doit en général être introduit de telle façon que le générateur, vue de la cible ait la résistance de la cible. La situation ici est grosso-modo analogue. Le transducteur qui effectue

[9] Technical Report No. 65, The Research Laboratory of Electronics, M.I.T., March 17, 1949.

l'encodage devrait adapter la source au canal en un sens statistique. La source vue depuis le canal à travers le transducteur devrait avoir la même structure statistique que la source qui maximise l'entropie du canal. Le contenu du théorème 9 est que, bien qu'une adaptation exacte ne soit en général pas possible, on puisse l'approcher d'aussi près qu'on le souhaite. Le ratio du taux effectif de transmission sur la capacité $C$ peut être appelé l'efficacité du système de codage. Ce ratio est bien sûr égal au ratio de l'entropie effective des symboles du canal sur l'entropie maximum possible.

En général, un encodage idéal ou presque idéal nécessite un long délai entre l'émetteur et le récepteur. Dans le cas non bruité qu'on a considéré, la fonction principale de ce délai est de permettre une adaptation raisonnablement bonne des probabilités aux longueurs des suites correspondantes. Avec un bon code, le logarithme de la probabilité réciproque d'un long message doit être proportionnel à la durée du signal correspondant ; en fait,

$$\left| \frac{\log p^{-1}}{T} - C \right|$$

doit être petit pour tous les messages longs sauf pour une petite fraction d'entre eux.

Si une source peut seulement produire un message particulier, son entropie est nulle, et aucun canal n'est requis. Par exemple, un calculateur conçu pour calculer les chiffres successifs de $\pi$ produit une suite définie ne contenant aucun élément aléatoire. Aucun canal n'est requis pour "transmettre" cela en un autre point. On pourrait construire une autre machine pour calculer la même séquence en ce second point. Pourtant, cela peut être impraticable. Dans un tel cas, on peut choisir d'ignorer une partie ou la totalité de la connaissance statistique que l'on a de la source. On peut considérer les chiffres de $\pi$ comme étant une suite aléatoire et on construit alors un système capable d'envoyer n'importe quelle suite de chiffres. D'une façon similaire, on peut choisir d'utiliser une partie de notre connaissance statistique de la langue anglaise pour construire un code, mais sans utiliser la totalité de cette connaissance statistique. Dans un tel cas, on considère la source d'entropie maximum par rapport aux conditions statistiques qu'on souhaite retenir. L'entropie de cette source détermine la capacité du canal qui est nécessaire et suffisant. Dans l'exemple, la seule information retenue est que tous les chiffres sont choisis dans l'ensemble 0, 1,...,9. Dans le cas de l'anglais, on peut souhaiter utiliser l'économie statistique possible du fait des fréquences des lettres, mais rien de plus. La source d'entropie maximum est alors la première approximation de l'anglais et son entropie détermine la capacité du canal requise.

Comme exemple simple de certains de ces résultats, considérons une source qui produit une suite de lettres choisies parmi A, B, C, D avec comme probabilités $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}$, les symboles successifs étant choisis indépendamment les uns des autres. On a

$$\begin{aligned} H &= -\left( \frac{1}{2} \log \frac{1}{2} + \frac{1}{4} \log \frac{1}{4} + \frac{2}{8} \log \frac{2}{8} \right) \\ &= \tfrac{7}{4} \text{ bits par symbole.} \end{aligned}$$

Ainsi, on peut approximer un système de codage pour encoder des messages à partir de cette sources en chiffres binaires avec une moyenne de $\frac{7}{4}$ chiffres binaires par symbole. Dans ce cas, on peut effectivement atteindre la valeur limite par le code suivant (obtenu par la méthode de la seconde preuve du théorème 9) :

$$\begin{array}{cc} A & 0 \\ B & 10 \\ C & 110 \\ D & 111 \end{array}$$

Le nombre moyen de chiffres binaires utilisé pour coder une suite de $N$ symboles sera

$$N\left(\frac{1}{2}\times 1+\frac{1}{4}\times 2+\frac{2}{8}\times 3\right)=\frac{7}{4}N.$$

On voit aisément que les chiffres binaires 0, 1 ont pour probabilités $\frac{1}{2}, \frac{1}{2}$, de telle façon que l'entropie $H$ pour la suite codée est un bit par symbole. Puisque, en moyenne, on a $\frac{7}{4}$ chiffres binaires par lettre originale, les entropies sur une base temporelle sont les mêmes. L'entropie maximum possible pour l'ensemble original est $\log 4 = 2$, qui advient lorsque A, B, C, D ont comme probabilités $\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}$. Par conséquent, l'entropie relative est $\frac{7}{8}$. On peut traduire les suites binaires dans l'ensemble original de symboles sur une base deux pour un par la table suivante :

$$\begin{array}{cc} 00 & \mathrm{A}' \\ 01 & \mathrm{B}' \\ 10 & \mathrm{C}' \\ 11 & \mathrm{D}' \end{array}$$

Ce processus double encode alors le message original dans les mêmes symboles mais avec un ratio de compression moyen de $\frac{7}{8}$.

Comme second exemple, considérons une source qui produit une suite de A et de B avec comme probabilité $p$ pour A et $q$ pour B. Donc $p \ll q$, on a

$$\begin{aligned} H &= -\log p^p (1-p)^{1-p} \\ &= -p \log p (1-p)^{(1-p)/p} \\ &\doteq p \log \frac{e}{p}. \end{aligned}$$

Dans un tel cas, on peut construire un assez bon codage du message sur un canal 0, 1 en envoyant une suite particulière, disons 0000, pour le symbole non fréquent A et en indiquant alors le nombre de B qui le suivent. Cela pourrait être indiqué par la représentation binaire de tous les nombres contenant la suite particulière qui a été effacée. Tous les nombres jusqu'à 16 sont représentés comme d'habitude ; 16 est représenté par le prochain nombre binaire après 16 qui ne contient pas quatre zéros, et qui est $17 = 10001$, etc.

On peut montrer que lorsque $p \to 0$, l'approche idéale du codage qui fournit la longueur d'une séquence spécifique est particulièrement pertinente.

# PARTIE II : LE CANAL DISCRET BRUITÉ

## 11. Représentation d'un canal discret bruité

On considère maintenant le cas où le signal est perturbé par du bruit durant la transmission ou bien sur l'un ou l'autre des terminaux. Cela signifie que le signal reçu n'est pas nécessairement le même que celui qui a été envoyé par l'émettteur. Deux cas doivent être distingués. Si un signal particulier transmis produit toujours le même signal reçu, i.e. le signal reçu est une fonction précisément définie du signal transmis, alors l'effet peut être appelé une distorsion. Si cette fonction a un inverse, deux signaux différents transmis ne produisant pas le même signal reçu, la distorsion peut être corrigée, au moins en principe, en effectuant simplement l'opération fonctionnelle inverse sur le signal reçu.

Le cas qui présente un intérêt ici est celui dans lequel le signal ne subit pas toujours le même changement pendant sa transmission. Dans ce cas, on peut supposer que le signal reçu $E$ est une fonction du message transmis $S$ et d'une seconde variable, le bruit $N$.

$$E = f(S, N)$$

Le bruit est considéré comme une variable aléatoire exactement comme c'était le cas du message, ci-dessus. En général, il peut être représenté par un processus stochastique adéquat. La sorte la plus générale de canal discret bruité que l'on va considérer est une généralisation du canal à état fini non bruité décrit précédemment. On suppose un nombre fini d'états et un ensemble de probabilités

$$p_{\alpha,i}(\beta, j).$$

Ceci est la probabilité, si le canal est dans l'état $\alpha$ et si le symbole $i$ est transmis, que le symbole $j$ soit reçu et que le canal soit laissé dans l'état $\beta$. Ainsi $\alpha$ et $\beta$ couvrent le domaine de tous les états possibles, $i$ le domaine de tous les signaux transmis possibles et $j$ le domaine de tous les signaux reçus possibles. Dans le cas où des symboles sucessifs sont indépendamment perturbés par le bruit, il y a seulement un état, et le canal est décrit par l'ensemble des probabilités de transition $p_i(j)$, la probabilité que le symbole transmis $i$ soit reçu comme un $j$.

Si l'on nourrit un canal bruité par une source, il y a deux processus statistiques à l'œuvre : la source et le bruit. Ainsi, un certain nombre d'entropies peuvent être calculées. D'abord, il y a l'entropie $H(x)$ de la source ou de l'entrée du canal (leurs valeurs seront égales si l'émetteur est non singulier). L'entropie de la sortie du canal, i.e. du signal reçu, sera notée $H(y)$. En cas d'absence de bruit, $H(y) = H(x)$. L'entropie conjointe de l'entrée et de la sortie sera $H(xy)$. Finalement, il y a deux entropies conditionnelles $H_x(y)$ et $H_y(x)$, l'entropie de la sortie quand l'entrée est connue et inversement. Entre ces quantités, on a les relations

$$H(x, y) = H(x) + H_x(y) = H(y) + H_y(x).$$

Toutes ces entropies peuvent être mesurées selon une base par seconde ou par symbole.

## 12. Équivoque et capacité du canal

Si le canal est bruité, il n'est en général pas possible de reconstruire le message original ou le signal transmis avec certitude par une quelconque opération sur le signal reçu $E$. Il y a, cependant, des moyens de transmettre l'information qui sont optimaux pour combattre le bruit. C'est ce problème que nous allons considérer maintenant.

Supposons qu'il y ait deux symboles possibles 0 et 1, et que l'on est en train de transmettre à un taux de 1000 symboles par seconde avec les probabilités $p_0 = p_1 = \frac{1}{2}$. Ainsi, notre source produit de l'information au taux de 1000 bits par seconde. Durant la transmission, le bruit introduit des erreurs de telle façon que, en moyenne, 1 bit sur 100 est reçu incorrectement (un 0 pour un 1, ou un 1 pour un 0). Quel est le taux de transmission de l'information ? Il est certainement inférieur à 1000 bits par seconde puisqu'environ 1% des symboles reçus sont incorrects. Notre premier réflexe pourrait être de dire que le taux est de 990 bits par seconde en soustrayant simplement le nombre attendu d'erreurs. Mais ceci n'est pas satisfaisant parce que cela échoue à prendre en compte le manque de connaissance du récepteur des endroits où se situent les erreurs. On peut aller vers un cas extrême et supposer que le bruit est si grand que les symboles reçus sont entièrement indépendants des symboles transmis. La probabilité de recevoir un 1 est $\frac{1}{2}$ quel que soit le symbole qui a effectivement été transmis et similairement pour 0. Alors environ la moitié des symboles reçus sont corrects à cause de l'aléa seul, et on devrait donner au système le crédit d'être capable de transmettre 500 bits par seconde alors qu'en fait aucune information n'est transmise du tout. Une transmission aussi "bonne" serait obtenue en se passant complètement du canal et en jetant une pièce à pile ou face au point de réception.

Évidemment, la bonne correction à appliquer à la quantité d'information transmise est cette quantité d'information qui manque dans le signal reçu, ou, alternativement, c'est l'incertitude, quand on a reçu un signal, de ce qui avait été effectivement transmis. De nos précédentes discussions sur l'entropie comme une mesure de l'incertitude, il semble raisonnable d'utiliser l'entropie conditionnelle du message, connaissant le message reçu, comme une mesure de cette information manquante. C'est en effet la définition correcte, comme on le verra. En suivant cette idée, effectivement, le taux de la transmission, $R$, serait obtenu en soustrayant du taux de production (i.e. l'entropie de la source) le taux moyen de l'entropie conditionnelle.

$$R = H(x) - H_y(x).$$

L'entropie conditionnelle $H_y(x)$ sera, pour des raisons pratiques, appelée l'équivoque. Elle mesure l'ambiguité moyenne du signal reçu.

Dans l'exemple considéré ci-dessus, si un 0 est reçu, la probabilité a posteriori qu'un 0 soit transmis est 0.99, et celle qu'un 1 soit transmis est 0.01. Ces schémas sont inversés si un 1 est reçu. Par conséquent

$$\begin{aligned} H_y(x) &= -[0.99 \log\ 0.99 + 0.01 \log\ 0.01] \\ &= 0.081 \text{ bits/symbole} \end{aligned}$$

ou 81 bits par seconde. On peut dire que le système transmet à un taux de $1000 - 81 = 919$ bits par seconde. Dans le cas extrême où un 0 a autant de chance d'être reçu qu'un 0 ou qu'un 1, et similairement pour 1, les probabilités a posteriori sont $\frac{1}{2}, \frac{1}{2}$, et

$$\begin{aligned} H_y(x) &= -\left[\tfrac{1}{2}\log\tfrac{1}{2} + \tfrac{1}{2}\log\tfrac{1}{2}\right] \\ &= 1 \text{ bit par symbole} \end{aligned}$$

soit 1000 bits par seconde. Le taux de transmission est alors 0 comme cela doit être.

Le théorème suivant donne une interprétation intuitive directe de l'équivoque et sert également à justifier cette mesure comme l'unique mesure appropriée. On considère un système de communication et un observateur (ou un dispositif auxiliaire) qui peut voir à la fois ce qui est envoyé et ce qui est rétabli (avec les erreurs dues au bruit). Cet observateur note les erreurs dans le message rétabli et transmet les données au point de réception sur un "canal de correction" pour permettre au récepteur de corriger les erreurs. La situation est présentée schématiquement sur la Fig. 8.

*Théorème 10 : Si le canal de correction a une capacité égale à $H_y(x)$, il est possible d'encoder ainsi les données de correction pour les envoyer sur ce canal et de corriger tout sauf une fraction arbitrairement petite des erreurs. Cela n'est pas possible si la capacité du canal est inférieure à $H_y(x)$.*

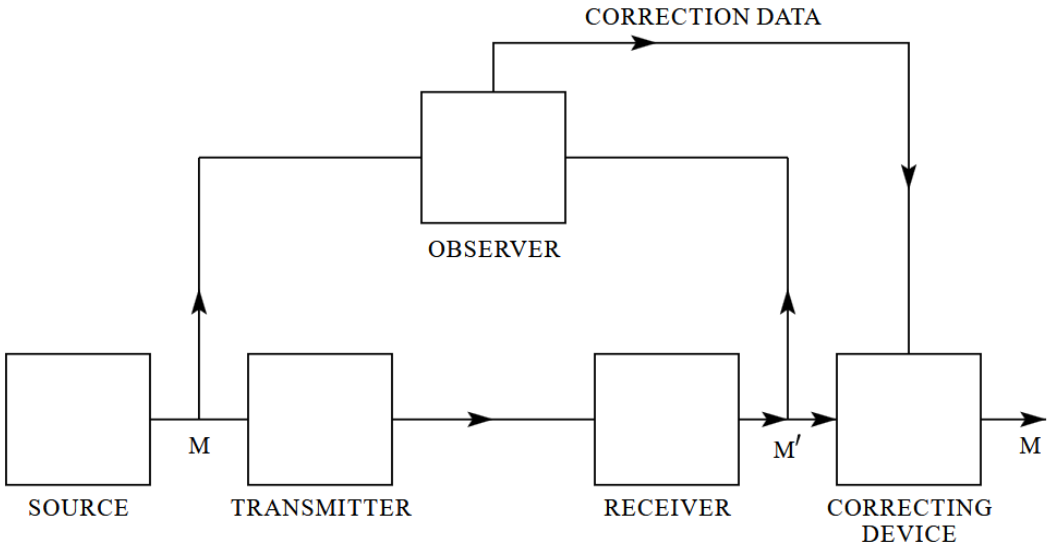



FIG. 8 : Diagramme schématique d'un système de correction.

Grossièrement alors, $H_y(x)$ est la quantité d'information additionnelle qui doit être fournie par seconde au point de réception pour corriger le message reçu.

Pour prouver la première partie, considérons de longues suites du message reçu $M'$ et le message correspondant original $M$. Il y aura logarithmiquement $TH_y(x)$ des $M$ qui devraient

raisonnablement avoir produit chaque $M'$. Ainsi on a $TH_y(x)$ chiffres binaires à envoyer toutes les $T$ secondes. Cela peut être fait avec une fréquence d'erreur de $\epsilon$ sur un canal de capacité $H_y(x)$.

La seconde partie peut être prouvée en notant, premièrement, que pour toutes variables aléatoires discrètes $x, y, z$

$$H_y(x, z) \geq H_y(x).$$

le côté gauche peut être développé pour donner

$$\begin{aligned} H_y(z) + H_{yz}(x) &\geq H_y(x) \\ H_{yz}(x) \geq H_y(x) - H_y(z) &\geq H_y(x) - H(z). \end{aligned}$$

Si on identifie $x$ à la sortie de la source, $y$ au signal reçu et $z$ au signal envoyé sur le canal de correction, alors le côté droit est l'équivoque inférieure au taux de transmission sur le canal de correction. Si la capacité de ce canal est inférieure à l'équivoque, le côté droit sera supérieur à zéro et $H_{yz}(x) > 0$. Mais ceci est l'incertitude sur ce qui a été envoyé, en connaissant à la fois le signal reçu et le signal de correction. Si cela est supérieur à zéro, la fréquence d'erreur peut être rendue arbitrairement petite.

> *Exemple* : Supposons que des erreurs ont lieu au hasard dans une suite de chiffres binaires : la probabilité qu'un chiffre soit faux est $p$ et celle qu'il soit juste est $q = 1-p$. Ces erreurs peuvent être corrigées si leur position est connue. Ainsi le canal de correction a seulement besoin d'envoyer l'information quant à ces positions. Cela revient à transmettre depuis une source qui produit des chiffres binaires avec une probabilité égale à $p$ pour 1 (incorrecte) et à $q$ pour 0 (correcte). Cela nécessite un canal de capacité
>
> $$-[p \log\, p + q \log\, q]$$
>
> qui est l'équivoque du système original.

Le taux de transmission $R$ peut s'écrire sous deux autres formes du fait des identités notées ci-dessus. On a

$$\begin{aligned} R &= H(x) - H_y(x) \\ &= H(y) - H_x(y) \\ &= H(x) + H(y) - H(x, y). \end{aligned}$$

La première expression de définition a déjà été interprétée comme la quantité d'information envoyée moins l'incertitude sur ce qui a été envoyé. La seconde mesure la quantité reçue moins la partie de cette quantité qui est due au bruit. La troisième est la somme des deux quantités moins l'entropie conjointe et par conséquent, dans un certain sens, c'est le nombre de bits par seconde commun aux deux. Ainsi toutes les expressions ont un certain degré intuitif de signification.

La capacité $C$ d'un canal bruité devrait être le taux maximum possible de transmission, i.e. le taux quand la source est correctement adaptée au canal. On définit donc la capacité du canal par

$$C = \text{Max}(H(x) - H_y(x))$$

où le maximum est calculé par rapport à toutes les sources d'information possibles comme entrées du canal. Si le canal est non bruité, $H_y(x) = 0$. La définition est alors équivalente à celle déjà donnée pour un canal non bruité puisque l'entropie maximum pour le canal est sa capacité.

## 13. Le théorème fondamental pour un canal discret avec bruit

Il peut sembler surprenant de définir une capacité particulière $C$ pour un canal bruité dans la mesure où l'on ne peut jamais envoyer d'information certain dans un tel cas. Il est clair, cependant, qu'en envoyant l'information sous une forme redondante, la probabilité d'erreurs peut être réduite. Par exemple, en répétant le message plusieurs fois et par une étude statistique des différentes versions reçues du message, la probabilité des erreurs peut être rendue très petite. On peut s'attendre, pourtant, à ce que lorsqu'on essaie de faire tendre cette probabilité d'erreurs vers 0, la redondance de l'encodage doive être accrue infiniment, et qu'alors le taux de transmission tende aussi vers zéro. Ceci n'est aucunement vrai. Si ça l'était, il n'y aurait pas une capacité très bien définie, mais simplement une capacité pour une certaine fréquence d'erreurs, ou une certaine équivoque, la capacité baissant au fur et à mesure que les contraintes sur les erreurs sont rendues plus strictes. La capacité $C$ définie ci-dessus a un sens très précisément défini. Il est possible d'envoyer l'information au taux $C$ à travers le canal avec une fréquence d'erreur et d'équivoque aussi petites que souhaitée par un encodage correct. Cet énoncé n'est pas vrai pour n'importe quel taux supérieur à $C$. Si une tentative est effectuée de transmettre à un taux supérieur à $C$, disons $C + R_1$, alors il y aura nécessairement une équivoque égale ou supérieure à l'excès $R_1$. La nature prend son dû en requérant simplement cette incertitude supplémentaire, de telle façon que nous ne puissions pas obtenir un transfert correct de l'information supérieur à $C$.

La situation est présentée dans la Fig. 9. Le taux d'information dans le canal est présenté horizontalement et l'équivoque verticalement. Tout point au-dessus de la ligne épaisse dans la région hachurée peut être atteint et les points en-dessous ne peuvent pas l'être. Les points sur la ligne ne peuvent pas être atteints en général, mais il y aura habituellement deux points sur la ligne qui pourront être atteints.

Ces résultats sont la principale justification de la définition de $C$ et vont être maintenant démontrés.

*Théorème 11 : Soit un canal discret ayant la capacité $C$ et une source discrète d'entropie par seconde $H$, $H \leq C$ ; il existe un système de codage tel que la sortie de la source peut être transmise sur le canal avec une fréquence d'erreur arbitrairement petite (ou une équivoque arbitrairement petite). Si $H > C$, il est possible d'encoder la source de telle façon que l'équivoque*

*soit inférieure à $H - C + \epsilon$ où $\epsilon$ est arbitrairement petit. Il n'y a pas de méthode d'encodage qui donne une équivoque inférieure à $H - C$.*

La méthode pour prouver la première partie de ce théorème ne consiste pas à exhiber une méthode de codage ayant les propriétés souhaitées, mais elle consiste à montrer qu'un tel code devrait exister dans un certain groupe de codes. En fait, on fera la moyenne des erreurs sur ce groupe et on montrera que cette moyenne peut être rendue inférieure à $\epsilon$.

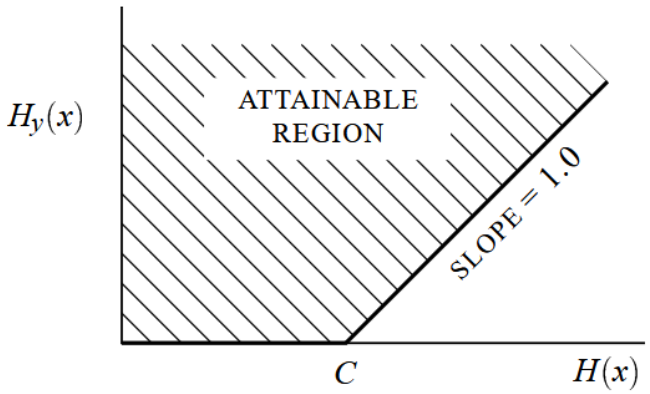



FIG. 9 : The equivocation possible for a given input entropy to a channel.

Si la moyenne d'un ensemble de nombres est inférieure à $\epsilon$, il doit exister au moins un élément de l'ensemble qui est inférieur à $\epsilon$. Cela établira le résultat désiré.

La capacité $C$ d'un canal bruité a été définie comme

$$C = \text{Max}(H(x) - H_y(x))$$

où $x$ est l'entrée et $y$ la sortie. La maximisation s'effectue sur toutes les sources qui pourraient être utilisées comme entrées pour le canal.

Soit $S_0$ une source qui utilise la capacité maximum $C$. Si ce maximum n'est effectivement atteint par aucune source, appelons $S_0$ une source qui l'approche pour donner le taux maximum. Supposons que $S_0$ est utilisée comme entrée pour le canal. On considère les suites possibles transmises et reçues d'une longue durée $T$. Les assertions suivantes sont vraies :

1. Les suites transmises sont de deux sortes, un groupe de forte probabilité contenant environ $2^{TH(x)}$ éléments et le reste des suites de probabilité totale petite.
2. Similairement, les séquences reçues ont une probabilité haute pour environ $2^{TH(y)}$ éléments et une probabilité faible pour les suites restantes.
3. Chaque sortie à forte probabilité devrait être produite par environ $2^{TH_y(x)}$ entrées. La probabilité de tous les autres cas a une probabilité totale faible.

Tous les $\epsilon$ et $\delta$ impliqués par les mots "petit" et "environ" dans ces phrases approchent de zéro lorsqu'on laisse $T$ croître et $S_0$ approcher la source maximum.

La situation est résumée dans la Fig. 10 où les suites en entrée sont les points sur la gauche et les suites en sortie les points sur la droite. La gerbe de lignes qui atteignent la même sortie représentent le domaine des causes possibles pour une sortie type.

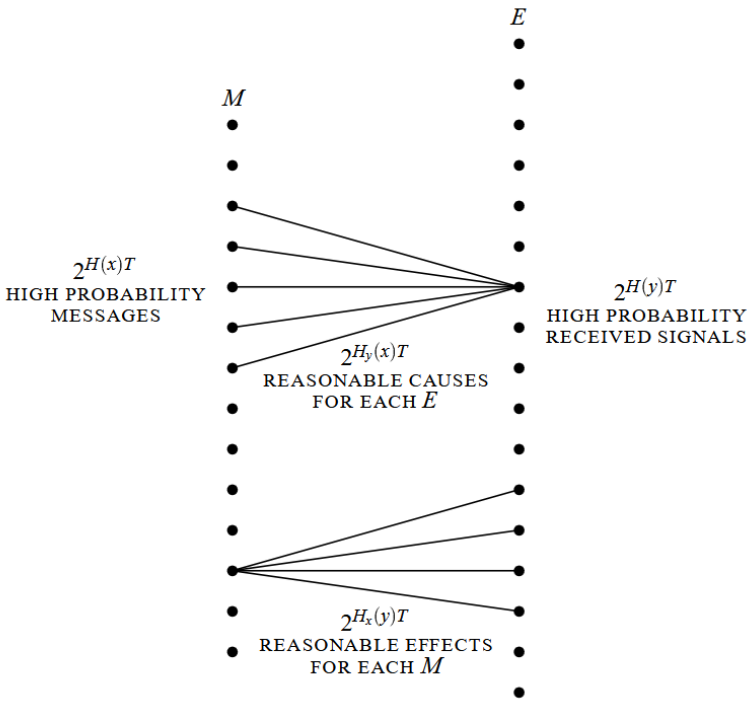



FIG. 10 : Représentation schématique des relations entre les entrées et les sorties dans un canal.

Maintenant supposons qu'on ait une autre source produisant de l'information à un taux $R$ avec $R < C$. Dans la période $T$, cette source aura $2^{TR}$ messages de probabilité haute. On souhaite leur associer une sélection des entrées possibles du canal de telle façon que l'on obtienne une petite fréquence d'erreurs. On effectuera cette association de toutes les façons possibles (en utilisant, pourtant, seulement le groupe à haute probabilité des entrées comme il a été déterminé par la source $S_0$) et on effectuera la moyenne de la fréquence des erreurs pour cette large classe de systèmes de codage possibles. C'est la même chose que de calculer la fréquence des erreurs pour une association aléatoire des messages et des entrées du canal de durée $T$. Supposons qu'une sortie particulière $y_1$ soit observée. Quelle est la probabilité qu'il y ait plus d'un message dans l'ensemble des causes de $y_1$ ? Il y a $2^{TR}$ messages distribués aléatoirement dans $2^{TH(x)}$ points. La probabilité qu'un point particulier soit un message est donc

$$2^{T(R-H(x))}.$$

La probabilité qu'aucun des points dans la gerbe ne soit un message (à part le message original réel) est

$$P = [1 - 2^{T(R-H(x))}]^{2^{TH_y(x)}}.$$

Maintenant, $R < H(x) - H_y(x)$ de telle façon que $R - H(x) = -H_y(x)–\eta$ avec $\eta$ positif. Par conséquent

$$P = [1 - 2^{-TH_y(x)-T\eta}]^{2^{TH_y(x)}}$$

approche (lorsque $T \to \infty$)

$$1 - 2^{-T\eta}$$

Par conséquent, la probabilité qu'il y ait une erreur s'approche de zéro, et la première partie du théorème est démontrée.

On montre aisément la seconde partie du théorème en notant qu'on pourrait simplement envoyer $C$ bits par seconde à partir de la source, en négligeant complètement le reste de l'information générée. Du côté du récepteur, la partie négligée donne une équivoque de $H(x) - C$ et la partie transmise ne nécessite que d'ajouter $\epsilon$. Cette limite peut également être atteinte de plusieurs autres manières, comme cela sera montré lorsqu'on considèrera le cas continu.

Le dernier énoncé du théorème est une simple conséquence de notre définition de $C$. Supposons que l'on puisse encoder une source avec $H(x) = C + a$ de telle façon que l'on obtienne une équivoque $H_y(x) = a - \epsilon$ avec $\epsilon$ positif. Alors $R = H(x) = C + a$ et

$$H(x) = H_y(x) = C + \epsilon$$

avec $\epsilon$ positif. Cela est en contradiction avec la définition de $C$ comme étant le maximum de $H(x) - H_y(x)$.

En fait, on a démontré davantage que ce qui est effectivement énoncé dans le théorème. Si la moyenne d'un ensemble de nombres est séparé d'un écart de $\epsilon$ de leur maximum, une fraction d'au plus $\sqrt{\epsilon}$ peut être supérieure à $\sqrt{\epsilon}$ en-dessous de ce maximum. Puisque $\epsilon$ est arbitrairement petit, on peut dire que presque tous les systèmes sont arbitrairement proches de l'idéal.

## 14. Discussion

La démonstration du théorème 11, bien que ça ne soit pas une démonstration d'existence pure, présente quelques défauts de telles preuves. Une tentative d'obtenir une bonne approximation du codage idéal en suivant la méthode de la preuve est en général impraticable. En fait, à part quelques cas triviaux et certaines situations limites, aucune description explicite d'une suite d'approximations de l'idéeal n'a été trouvée. Probablement que ceci n'est pas accidentel mais ça doit être relié à la difficulté de donner une construction explicite d'une bonne approximation d'une suite aléatoire.

Une approximation de l'idéal devrait avoir la propriété que si le signal est altéré d'une façon raisonnable par le bruit, la suite originale peut encore être retrouvée. En d'autres termes,

l'altération ne rendra en général pas le signal plus proche d'un autre signal raisonnable que du signal original. Ceci est accompli au coût d'une certaine quantité de redondance dans le codage. La redondance doit être introduite d'une façon correcte pour combattre la structure de bruit particulière qui est à l'œuvre. Pourtant, n'importe quelle redondance dans la source aidera si elle est utilisée au point de réception. En particulier, si la source contient déjà une certaine redondance et si aucune tentative n'est faite d'éliminer cette redondance pour s'adapter au canal, la redondance aidera à combattre le bruit. Par exemple, dans un canal de télégraphie sans bruit, on économisera environ 50% du temps en codant correctement les messages. Cela n'est pas fait et la redondance de la langue anglaise reste dans les symboles du canal. Cela a l'avantage, pourtant, d'autoriser un bruit considérable dans le canal. Une portion non négligeable des lettres peut être reçue incorrectement et encore reconstruite par le contexte. En fait, ceci n'est probablement pas une mauvaise approximation de l'idéal dans de nombreux cas, puisque la structure statistique de l'anglais est plutôt importante et pas si éloignée (dans le sens requis par le théorème) d'une sélection aléatoire.

Comme dans le cas non bruité, un délai est en général requis pour approcher l'encodage idéal. Ce délai a comme fonction supplémentaire d'autoriser un large ensemble de bruits d'affecter le signal avant qu'aucun jugement ne soit effectué au point de réception par rapport au message original. Accroître la taille des exemples précisent les assertions statistiques possibles.

Le contenu du théorème 11 et sa preuve peuvent être reformulés d'une manière différente qui montre la connexion avec le cas non bruité plus clairement. Considérons les signaux possibles d'une durée $T$ et supposons qu'un sous-ensemble d'entre eux est sélectionné pour être utilisé. Les éléments du sous-ensemble peuvent être utilisés avec des probabilités égales, et supposons que le récepteur est construit pour sélectionner, comme le signal original, la cause la plus probable dans le sous-ensemble, quand un signal perturbé est reçu. On définit $N(T, q)$ comme le nombre maximum de signaux qu'on peut choisir dans le sous-ensemble et qui soient tels que la probabilité d'une interprétation incorrecte soit inférieure à $q$.

*Théorème 12 :* $\lim_{T\to\infty} \dfrac{\log N(T,q)}{T} = C$*, où* $C$ *est la capacité du canal, en supposant que* $q$ *n'est ni égal à 0 ni égal à 1.*

En d'autres termes, quelle que soit la manière dont on fixe les limites de fiabilité, on peut estimer cette fiabilité dans la durée $T$ si suffisamment de messages correspondent à environ $CT$ bits, quand $T$ est suffisamment grand. Le théorème 12 peut être comparé à la définition de la capacité d'un canal non bruité fournie dans la Section 1.

## 15. Exemple d'un canal discret et de sa capacité

Un exemple simple de canal discret est présenté sur la Fig. 11. Il y a trois symboles possibles. Le premier n'est jamais affecté par le bruit. Le second et le troisième ont chacun pour probabilité $p$ de provenir de l'élément de la paire sans être modifié et $q$ d'être changé en le

second élément de la paire. On a (en notant $\alpha = -[p \log p + q \log q]$ et $P$ et $Q$ les probabilités d'utiliser le premier et le second symboles)

$$H(x) = -P \log P - 2Q \log Q$$
$$H_y(x) = 2Q\alpha$$

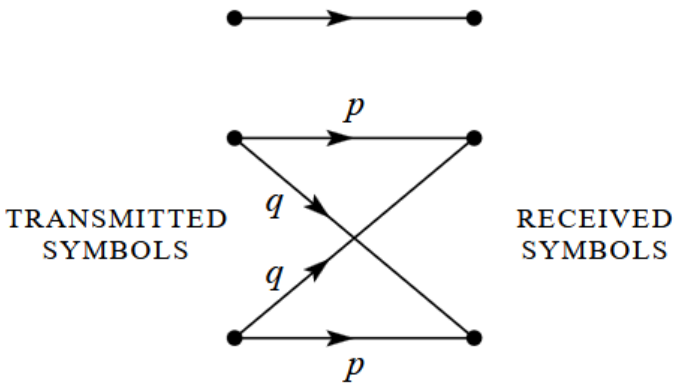



FIG. 11

On souhaite choisir $P$ et $Q$ de telle façon que $H(x) - H_y(x)$ soit maximisé en respectant la contrainte $P + 2Q = 1$. Par conséquent, on considère

$$U = -P \log P - 2Q \log Q - 2Q\alpha + \lambda(P + 2Q)$$

$$\frac{\partial U}{\partial P} = -1 - \log P + \lambda = 0$$

$$\frac{\partial U}{\partial Q} = -2 - 2 \log Q - 2\alpha + 2\lambda = 0.$$

En éliminant $\lambda$

$$\log P = \log Q + \alpha$$

$$P = Qe^{\alpha} = Q\beta$$

$$P = \frac{\beta}{\beta + 2} \qquad Q = \frac{1}{\beta + 2}$$

La capacité du canal est alors

$$C = \log \frac{\beta + 2}{\beta}.$$

Notons comment cela est correctement vérifié par les valeurs triviales dans les cas $p = 1$ et $p = \frac{1}{2}$. Dans le premier cas, $\beta = 1$ et $C = \log 3$, ce qui est correct puisque le canal est alors non bruité avec trois symboles possibles. Si $p = \frac{1}{2}$, $\beta = 2$ et $C = \log 2$, le second et le troisième symboles ne peuvent pas être distingués du tout et agissent ensemble comme un

seul symbole. Le premier symbole est utilisé avec une probabilité $P = \frac{1}{2}$ et le second et le troisième ensemble avec la probabilité $\frac{1}{2}$. Celle-ci peut être distribuée entre eux de n'importe quelle façon souhaitée et cela permettra d'atteindre la capacité maximum.

Pour des valeurs intermédiaires de $p$, la capacité du canal sera une valeur comprise entre log 2 et log 3. La distinction entre le second et le troisième symboles transmet une certaine information mais celle-ci n'est pas aussi grande que dans le cas non bruité. Le premier symbole est utilisé en quelque sorte plus souvent que les autres à cause de sa liberté par rapport au bruit.

## 16. La capacité du canal dans quelques cas particuliers

Si le bruit affecte les symboles successifs du canal indépendamment, il peut être décrit par un ensemble de probabilités de transition $p_{ij}$. $p_{ij}$ est la probabilité, si le symbole $i$ est envoyé, que le symbole $j$ soit reçu. Le taux maximum du canal est alors le maximum de

$$-\sum_{i,j} P_i p_{ij} \log \sum_i P_i p_{ij} + \sum_{i,j} P_i p_{ij} \log P_{ij}$$

où l'on fait varier les $P_i$ en respectant $\sum P_i = 1$. Cela amène par la méthode de Lagrange aux équations,

$$\sum_j p_{sj} \log \frac{p_{sj}}{\sum_i P_i p_{ij}} = \mu \qquad s = 1, 2, \ldots$$

Multiplier par $P_s$ et faire la somme sur $s$ montre que $\mu = C$. Appelons l'inverse de $p_{sj}$ (s'il existe) $h_{st}$ de telle façon que $\sum_s h_{st} p_{sj} = \delta_{tj}$. Alors :

$$\sum_{s,j} h_{st} p_{sj} \log\, p_{sj} - \log \sum_i P_i p_{it} = C \sum_s h_{st}.$$

Par conséquent :

$$\sum_i P_i p_{it} = \exp\left[-C \sum_s h_{st} + \sum_{s,j} h_{st} p_{sj} \log\, p_{sj}\right]$$

ou,

$$P_i = \sum_t h_{it} \exp\left[-C \sum_s h_{st} + \sum_{s,j} h_{st} p_{sj} \log\, p_{sj}\right].$$

Ceci est le système d'équations qui permet de déterminer les valeurs maximales de $P_i$, avec $C$ à déterminer de telle façon que $\sum P_i = 1$. Quand on fait cela, $C$ sera la capacité du canal, et les $P_i$ seront les probabilités correctes des symboles du canal pour atteindre cette capacité.

Si chaque symbole en entrée a le même ensemble de probabilités sur les arêtes du graphe qui en partent, et s'il en est de même de tout symbole de sortie pour les arêtes qui l'atteignent, la capacité peut facilement être calculée. Des exemples sont montrés sur la Fig. 12. Dans un tel

cas, $H_x(y)$ est indépendant de la distribution de probabilités des symboles en entrée, et est égal à $-\sum p_i \log p_i$ où les $p_i$ sont les valeurs des probabilités de transition depuis n'importe quel symbole en entrée. La capacité du canal est

$$\text{Max } [H(y) - H_x(y)] = \text{Max } H(y) + \sum p_i \log p_i.$$

La valeur maximum de $H(y)$ est clairement $\log m$ où $m$ est le nombre de symboles en sortie, puisqu'il est possible de les rendre tous également probables en rendant les symboles en entrée également probables. La capacité du canal est par conséquent

$$C = \log m + \sum p_i \log p_i.$$

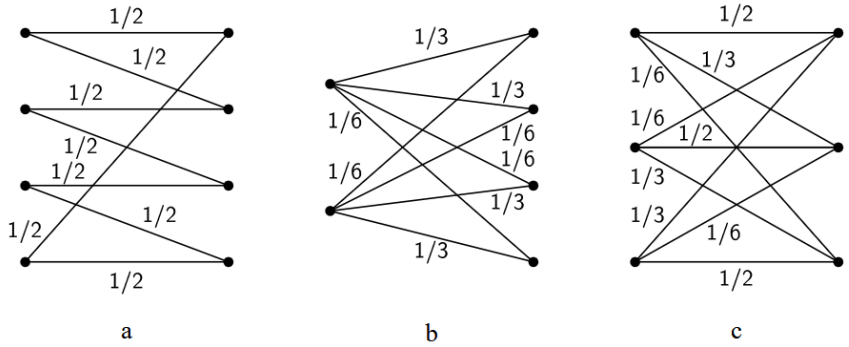



FIG. 12 : Exemples de canaux discrets avec les mêmes probabilités de transition pour chaque entrée et chaque sortie.

Dans la Fig. 12a, la capacité serait égale à

$$C = \log 4 - \log 2 = \log 2.$$

On pourrait obtenir cette capacité en utilisant seulement les premier et troisième symboles. Sur la Fig. 12b

$$\begin{aligned} C &= \log 4 - \frac{2}{3}\log 3 - \frac{1}{3}\log 6 \\ &= \log 4 - \log 3 - \frac{1}{3}\log 2 \\ &= \log \frac{1}{3}\, 2^{\frac{5}{3}}. \end{aligned}$$

Sur la Fig. 12c, on a

$$C = \log 3 - \frac{1}{2}\log 2 - \frac{1}{3}\log 3 - \frac{1}{6}\log 6 = \log \frac{3}{2^{1/2}\, 3^{1/3}\, 6^{1/6}}$$

Supposons que les symboles tombent dans différents groupes tels que le bruit ne permet jamais à un symbole d'un groupe d'être transformé en un symbole d'un autre groupe. Appelons $C_n$

(en bits par seconde) la capacité du $n^{\text{ième}}$ groupe quand on n'utilise que les symboles de ce groupe. Alors, on peut facilement montrer que, pour une meilleure utilisation de l'ensemble entier, la probabilité totale $P_n$ de tous les symboles dans le $n^{\text{ième}}$ groupe devrait être

$$P_n = \frac{2^{C_n}}{\sum 2^{C_n}}.$$

Dans un groupe, la probabilité est distribuée juste comme elle devrait l'être si ces symboles étaient les seuls symboles à être utilisés. La capacité du canal est

$$C = \log \sum 2^{C_n}.$$

## 17. Un exemple de codage efficace

L'exemple suivant, bien qu'un peu irréaliste, est un cas dans lequel l'exacte correspondance vers un canal bruité est possible. Il y a deux symboles qui traversent le canal, 0 et 1, et le bruit les affecte dans des blocs de sept symboles. Un bloc de sept symboles est soit transmis sans erreur, ou bien exactement un seul des sept symboles est incorrect. Ces huit possibilités sont équiprobables. On a

$$\begin{aligned} C &= \text{Max}[H(y) - H_x(y)] \\ &= \frac{1}{7}\left[7 + \frac{8}{8}\log\ \frac{1}{8}\right] \\ &= \frac{4}{7} \text{ bits par symbole.} \end{aligned}$$

Un code efficace, permettant une correction complète des erreurs et une transmission au taux $C$, est le suivant (trouvé par une méthode due à R. Hamming) :

Soit un bloc de sept symboles $X_1, X_2, ..., X_7$. Parmi eux, $X_3, X_5, X_6$ et $X_7$ sont des symboles de message choisis arbitrairement par la source. Les trois autres sont redondants et calculés comme suit :

| | | | | | | |
|---|---|---|---|---|---|---|
| $X_4$ | est | choisi | pour | rendre | $\alpha = X_4 + X_5 + X_6 + X_7$ | pair |
| $X_2$ | 〃 | 〃 | 〃 | 〃 | $\beta = X_2 + X_3 + X_6 + X_7$ | 〃 |
| $X_1$ | 〃 | 〃 | 〃 | 〃 | $\gamma = X_1 + X_3 + X_5 + X_7$ | 〃 |

Quand un bloc de sept symboles est reçu $\alpha, \beta$ et $\gamma$ sont calculés et si un nombre pair d'entre eux est nul, il est appelé 0 ; il est appelé 1 dans le cas d'un nombre impair de symboles nul. Le nombre binaire $\alpha\beta\gamma$ donne alors l'indice du $X_i$ qui est incorrect (s'il est nul, il n'y a pas eu d'erreur).

# APPENDICE 1

## Croissance du nombre de blocs de symboles avec une condition d'état finie

Soit $N_i(L)$ le nombre de blocs de symboles de longueur $L$ se terminant dans l'état $i$. Alors on a

$$N_j(L) = \sum_{i,s} N_i(L - b_{ij}^{(s)})$$

où $b_{ij}^1, b_{ij}^2, ..., b_{ij}^m$ sont les longueurs des symboles qui peuvent être choisis dans l'état $i$ et qui amènent à l'état $j$. Ce sont des équations linéaires et le comportement lorsque $L \to \infty$ doit être du type

$$N_j = A_j W^L.$$

En substituant l'équation aux différences

$$A_j W^L = \sum_{i,s} A_i W^{L - b_{ij}^{(s)}}$$

ou

$$A_j = \sum_{i,s} A_i W^{-b_{ij}^{(s)}}$$

$$\sum_i \left( \sum_s W^{-b_{ij}^{(s)}} - \delta_{ij} \right) A_i = 0.$$

Pour que cela soit possible, le déterminant

$$D(W) = |a_{ij}| = \left| \sum_s W^{-b_{ij}^{(s)}} - \delta_{ij} \right|$$

doit s'évanouir et cela détermine $W$, qui est, bien sûr, la plus grande racine réelle de $D = 0$.

La quantité $C$ est alors donnée par

$$C = \lim_{L \to \infty} \frac{\log \sum A_j W^L}{L} = \log W$$

et on note également que les mêmes propriétés de croissance sont obtenues si on oblige tous les blocs à commencer par le même état (arbitrairement choisi).

## APPENDICE 2

### Dérivation de $H = -\sum p_i \log p_i$

Soit $H\left(\frac{1}{n}, \frac{1}{n}, ..., \frac{1}{n}\right) = A(n)$. À partir de la condition (3), on peut décomposer un choix parmi $s^m$ possibilités de probabilités égales dans une suite de $m$ choix à partir de $s$ possibilités de probabilités égales et obtenir

$$A(s^m) = mA(s)$$

Similairement

$$A(t^n) = nA(t)$$

On peut choisir $n$ arbitrairement grand et trouver un $m$ qui satisfasse

$$s^m \leq t^n < s^{m+1}.$$

Ainsi, en prenant les logarithmes et en divisant par $n \log s$,

$$\frac{m}{n} \leq \frac{\log t}{\log s} \leq \frac{m}{n} + \frac{1}{n} \quad \text{ou} \quad \left|\frac{m}{n} - \frac{\log t}{\log s}\right| < \epsilon$$

où $\epsilon$ est arbitrairement petit. Maintenant, à partir de la propriété de monotonie de $A(n)$,

$$\begin{array}{lll} A(s^m) & \leq A(t^n) & \leq A(s^{m+1}) \\ mA(s) & \leq nA(t) & \leq (m+1)A(s) \end{array}$$

Par conséquent, en divisant par $nA(s)$,

$$\frac{m}{n} \leq \frac{A(t)}{A(s)} \leq \frac{m}{n} + \frac{1}{n} \qquad \text{ou} \qquad \left|\frac{m}{n} - \frac{A(t)}{A(s)}\right| < \epsilon$$

$$\left|\frac{A(t)}{A(s)} - \frac{\log t}{\log s}\right| < 2\epsilon \qquad\qquad A(t) = K \log t.$$

où $K$ doit être positif, pour satisfaire (2).

Maintenant, supposons qu'on ait le choix parmi $n$ possibilités de probabilités commensurables $p_i = \frac{n_i}{\sum n_i}$ où les $n_i$ sont des entiers. On peut décomposer un choix à partir de $\sum n_i$ possibilités en un choix à partir de $n$ possibilités avec des probabilités $p_1, \ldots, p_n$ et alors, si le $i^{\text{ième}}$ choix est effectué, on fait un choix parmi $n_i$ possibilités de probabilités égales. En utilisant la condition (3) à nouveau, on trouve le choix total à partir de $\sum n_i$ en le calculant par deux méthodes

$$K \log \sum n_i = H(p_1, ..., p_n) + K \sum p_i \log n_i.$$

Par conséquent

$$H = K\left[\sum p_i \log \sum n_i - \sum p_i \log n_i\right]$$

$$= -K \sum p_i \log \frac{n_i}{\sum n_i} = -K \sum p_i \log p_i.$$

Si les $p_i$ sont incommensurables, elles peuvent être approchées par des rationnels et la même expression doit être vérifiée par notre hypothèse de continuité. Ainsi, l'expression est vérifiée en général. Le choix du coefficient $K$ est une question de commodité et se résume au choix d'une unité de mesure.

## APPENDICE 3

### Théorèmes sur les sources ergodiques

S'il est possible d'aller de n'importe quel état avec $P > 0$ à n'importe quel autre état le long d'un chemin de probabilité $p > 0$, le système est ergodique et la loi forte des grands nombres peut s'appliquer. Ainsi le nombre de fois où un chemin donné dans $p_{ij}$ (le réseau), est emprunté dans une longue suite de longueur $N$ est environ proportionnel à la probabilité d'être en $i$, disons $P_i$, d'ensuite choisir ce chemin, $P_i p_{ij} N$. Si $N$ est assez grand, la probabilité du pourcentage d'erreur $\pm\delta$ dans ce cas est inférieure à $\epsilon$ de telle façon que pour tous sauf pour un ensemble de petite probabilité, les nombres effectifs appartiennent à un domaine dont les limites sont

$$(P_i p_{ij} \pm \delta)N.$$

Donc, presque toutes les suites ont une probabilité $p$ donnée par

$$p = \prod p_{ij}^{(P_i p_{ij} \pm \delta)N}$$

et $\dfrac{\log p}{N}$ est borné par

$$\frac{\log p}{N} = \sum (P_i p_{ij} \pm \delta) \log p_{ij}$$

ou

$$\left|\frac{\log p}{N} - \sum P_i p_{ij} \log p_{ij}\right| < \eta.$$

Ceci prouve le théorème 3.

Le théorème 4 découle immédiatement de cela en calculant les bornes supérieure et inférieure pour $n(q)$ basées sur les domaines possibles des valeurs de $p$ dans le théorème 3.

Dans le cas mixte (non ergodique), si

$$L = \sum p_i L_i$$

et si les entropies des composantes sont $H_1 \geq H_2 \geq \ldots \geq H_n$, on a le

*Théorème :* $\underset{N\to\infty}{\text{Lim}} \dfrac{\log n(q)}{N} = \varphi(q)$ *est une fonction décroissante en escalier,*

$$\varphi(q) = H_s \quad \textit{dans l'intervalle} \quad \sum_1^{s-1} \alpha_i < q < \sum_1^{s} \alpha_i.$$

Pour prouver le théorème 5 et le théorème 6, notons d'abord que $F_N$ est décroissante monotone parce que $N$ croissant ajoute un indice à une entropie conditionnelle. Une simple substitution pour $p_{B_i}(S_j)$ dans la définition de $F_N$ montre que

$$F_N = NG_N - (N-1)G_{N-1}$$

et ajouter cela pour tous les $N$ donne $G_N = \dfrac{1}{N}\sum F_n$. Par conséquent, $G_N \geq F_N$ et $G_N$ sont décroissantes monotones. Aussi, elles doivent approcher de la même limite. En utilisant le théorème 3, on voit que $\underset{N\to\infty}{\text{Lim}} G_N = H$.

## APPENDICE 4

### Maximiser le taux pour un système de contraintes

Supposons que l'on ait un ensemble de contraintes sur des suites de symboles qui est de type états finis et peut par conséquent être représenté par un graphe linéaire. Soit $\ell_{ij}^{(s)}$ les longueurs des divers symboles qui peuvent être rencontrés en passant de l'état $i$ à l'état $j$. Quelle distribution de probabilités $P_i$ pour les différents états et $p_{ij}^{(s)}$ pour choisir le symbole $s$ dans l'état $i$ et en allant vers l'état $j$ maximise le taux de génération de l'information sous ces contraintes ? Les contraintes définissent un canal discret et le taux maximum doit être inférieur ou égal à la capacité $C$ de ce canal, puisque si tous les blocs de grande longueur étaient équiprobables, ce taux en résulterait, et si possible, ce serait le meilleur taux. On montrera que ce taux peut être obtenu par un choix correct des $P_i$ et des $p_{ij}^{(s)}$.

Le taux en question est

$$\frac{-\sum P_i p_{ij}^{(s)} \log p_{ij}^{(s)}}{\sum P_i p_{ij}^{(s)} \ell_{ij}^{(s)}} = \frac{N}{M}$$

Soit $\ell_{ij} = \sum \ell_{ij}^{(s)}$. De manière évidente, pour un maximum $p_{ij}^{(s)} = k \exp \ell_{ij}^{(s)}$. Les contraintes sur la maximisation sont $\sum P_i = 1, \sum_j p_{ij} = 1, \sum P_i(p_{ij} - \delta_{ij}) = 0$. Par conséquent, on maximise

$$U = \frac{-\sum P_i p_{ij} \log p_{ij}}{\sum P_i p_{ij} \ell_{ij}} + \lambda \sum_i P_i + \sum \mu_i p_{ij} + \sum \eta_j p_i (p_{ij} - \delta_{ij})$$

$$\frac{\partial U}{\partial p_{ij}} = -\frac{MP_i(1 + \log p_{ij}) + NP_i\ell_{ij}}{M^2} + \lambda + \mu_i + \eta_i P_i = 0.$$

En résolvant pour $p_{ij}$

$$p_{ij} = A_i B_j D^{-\ell_{ij}}.$$

Puisque

$$\sum_j p_{ij} = 1, \qquad A_i^{-1} = \sum_j B_j D^{-\ell_{ij}}$$

$$p_{ij} = \frac{B_j D^{-\ell_{ij}}}{\sum_s B_s D^{-\ell_{is}}}.$$

La valeur correcte de $D$ est la capacité $C$ et les $B_j$ sont solutions de

$$B_i = \sum B_j C^{-\ell_{ij}}$$

car alors

$$p_{ij} = \frac{B_j}{B_i} C^{-\ell_{ij}}$$

$$\sum P_i \frac{B_j}{B_i} C^{-\ell_{ij}} = P_j$$

ou

$$\sum P_i \frac{B_j}{B_i} C^{-\ell_{ij}} = \frac{P_j}{B_j}.$$

De telle façon que si $\lambda_i$ satisfait

$$\sum_{P_i} \gamma_i C^{-\ell_{ij}} = \gamma_j$$
$$= B_i \gamma_i$$

à la fois les ensembles d'équations pour $B_i$ et les $\gamma_i$ peuvent être satisfaits puisque $C$ est tel que

$$|C^{-\ell_{ij}} - \delta_{ij}| = 0.$$

Dans ce cas, le taux est

$$-\frac{P_i p_{ij} \log \frac{B_j}{B_i} C^{-\ell_{ij}}}{\sum P_i p_{ij} \ell_{ij}} = C - \frac{\sum P_i p_{ij} \log \frac{B_j}{B_i}}{\sum P_i p_{ij} \ell_{ij}}$$

mais

$$\sum P_i p_{ij} (\log B_j - \log B_i) = \sum_j P_j \log B_j - \sum_i P_i \log B_i = 0.$$

Par conséquent, le taux est $C$ et comme il ne pourrait jamais être excédé, c'est le maximum, ceci justifiant la solution qu'on a supposée.

# PARTIE III : PRÉLIMINAIRES MATHÉMATIQUES

Dans cette dernière section du présent article, on considère le cas où les signaux ou les messages ou les deux sont des variables continues, contrairement au caractère discret supposé jusque-là. Dans une large mesure, le cas continu peut être obtenu comme un processus limite à partir du cas discret en divisant le continuum des messages et des signaux en un nombre grand mais fini de petites régions et en calculant les différents paramètres impliqués sur cette base discrète. Il y a, cependant, quelques nouveaux effets qui apparaissent et également un changement général d'accents dans la direction d'une spécialisation des résultats généraux aux cas particuliers.

Nous n'essaierons pas, dans le cas continu, d'obtenir nos résultats avec la plus grande généralité, ou avec l'extrême rigueur des mathématiques pures, car cela entraînerait beaucoup de théorie abstraite de la mesure et cela obscurcirait les grandes lignes de l'analyse. Une étude préliminaire, pourtant, indique que la théorie peut être formulée d'une façon complètement axiomatique et rigoureuse qui inclut à la fois les cas continus, discrets, et de nombreux autres cas. Les libertés occasionnelles prises avec les processus limites dans la présente analyse peuvent être justifiées dans tous les cas présentant un intérêt pratique.

## 18. Ensembles et ensembles de fonctions

On devra traiter dans le cas continu des ensembles (mot anglais *set*) de fonctions et des ensembles (mot anglais *ensemble*). Un ensemble (*set*) de fonctions, comme son nom l'indique, est simplement une classe ou une collection de fonctions, généralement d'une variable, le temps. Il peut être spécifié en donnant une représentation explicite des différentes fonctions de l'ensemble, ou implicitement en donnant une propriété que les fonctions dans l'ensemble possèdent alors que les autres fonctions ne les possèdent pas. Fournissons quelques exemples d'ensembles (*set*) :

1. L'ensemble des fonctions :
$$f_\theta(t) = \sin(t + \theta).$$
Chaque valeur particulière de $\theta$ détermine une fonction particulière dans l'ensemble.
2. L'ensemble des fonctions du temps ne contenant pas de fréquences supérieures à $W$ cycles par seconde.
3. L'ensemble de toutes les fonctions limitées en bande par $W$ et en amplitude par $A$.
4. L'ensemble des signaux parlés anglais comme des fonctions du temps.

Un ensemble (*ensemble*) de fonctions est un ensemble (*set*) de fonctions auquel est associée une mesure de probabilité tel qu'on peut déterminer la probabilité d'une fonction de l'ensemble (*set*) ayant certaines propriétés [10]. Par exemple, avec l'ensemble (*set*)

$$f_\theta(t) = \sin(t + \theta),$$

[10] Dans la terminologie mathématique, les fonctions appartiennent à un espace mesuré dont la mesure totale est l'unité.

on peut donner la distribution de probabilité pour $\theta, P(\theta)$. L'ensemble (*set*) devient un ensemble (*ensemble*). D'autres exemples d'ensembles (*ensemble*) de fonctions sont :

1. Un ensemble fini de fonctions $f_k(t)$ $(k = 1, 2, ..., n)$ dont les probabilités $f_k$ sont $p_k$.
2. Une famille finie-dimensionnelle de fonctions

   $$f(\alpha_1, \alpha_2, ..., \alpha_n; t)$$

   avec une distribution de probabilité sur les paramètres $\alpha_i$ :

   $$p(\alpha_1, ..., \alpha_n).$$

   Par exemple, on pourrait considérer l'ensemble (*ensemble*) défini par

   $$f(a_1, \ldots, a_n, \theta_1, \ldots, \theta_n; t) = \sum_{i=1}^{n} a_i \sin i(\omega t + \theta_i)$$

   avec les amplitudes $a_i$ distribuées normalement et indépendamment, et les phases $\theta_i$ distribuées uniformément (de 0 à $2\pi$) et indépendamment.
3. L'ensemble (*ensemble*)

   $$f(a_i, t) = \sum_{n=-\infty}^{\infty} a_n \frac{\sin \pi(2W_t - n)}{\pi(2W_t - n)}$$

   avec les $a_i$ normaux et indépendants ayant tous la même déviation standard $\sqrt{N}$. C'est une représentation du bruit "blanc", limité en bande à la bande de 0 à $W$ cycles par seconde et de puissance moyenne $N$ [11].
4. Soient des points distribués sur l'axe temporel selon une distribution de Poisson. À chaque point sélectionné, la fonction $f(t)$ est placée et les différentes fonctions sont ajoutées, donnant l'ensemble (*ensemble*)

   $$\sum_{k=-\infty}^{\infty} f(t + t_k)$$

   où les $t_k$ sont les points de la distribution de Poisson. Cet ensemble (*ensemble*) peut être considéré comme un type d'impulsion ou bruit de tir, où toutes les impulsions sont identiques.
5. L'ensemble des fonctions du discours anglais avec une mesure de probabilité donnée par la fréquence d'occurrence dans le langage courant.

[11] Cette représentation peut être utilisée comme une définition du bruit blanc à bande limitée. Cela présente certains avantages en ce que cela implique moins d'opérations pour le limiter que les définitions qu'on avait utilisées par le passé. Le nom "bruit blanc", déjà fermement ancré dans la littérature, est peut-être quelque peu malvenu. En optique, la lumière blanche signifie soit un spectre continu quelconque, soit un spectre qui est plat en terme de longueur d'onde (ce qui n'est pas la même chose qu'un spectre plat en fréquence).

Un ensemble (*ensemble*) de fonctions $f_\alpha(t)$ est stationnaire si on obtient le même ensemble quand toutes les fonctions sont décalées d'une certaine durée temporelle. L'ensemble (*ensemble*)

$$f_\theta(t) = \sin(t + \theta)$$

est stationnaire si $\theta$ est distribuée uniformément de 0 à $2\pi$. Si l'on décale chaque fonction de $t_1$, on obtient

$$\begin{aligned} f_\theta(t + t_1) &= \sin(t + t_1 + \theta) \\ &= \sin(t + \varphi) \end{aligned}$$

avec $\varphi$ distribuée uniformément de 0 à $2\pi$. Chaque fonction a changé mais l'ensemble comme un tout est invariant par la translation. Les autres exemples donnés ci-dessus sont également stationnaires.

Un ensemble (*ensemble*) est ergodique s'il est stationnaire, et s'il ne contient pas de sous-ensemble de fonctions avec une probabilité différente de 0 et de 1 qui soit stationnaire. L'ensemble (*ensemble*)

$$\sin(t + \theta)$$

est ergodique. Aucun sous-ensemble de ces fonctions de probabilité $\neq 0$, 1 n'est transformé en lui-même par toute translation temporelle. D'un autre côté, l'ensemble

$$a \sin(t + \theta)$$

avec $a$ normalement distribué et $\theta$ uniforme est stationnaire mais non ergodique. Le sous-ensemble de ces fonctions avec $a$ entre 0 et 1 par exemple est stationnaire.

Parmi les exemples donnés, le 3 et le 4 sont ergodiques, et le 5 peut peut-être considéré comme l'étant également. Si un ensemble est ergodique, on peut grossièrement dire que chaque fonction dans l'ensemble est typique de l'ensemble. Plus précisément, on sait qu'avec un ensemble ergodique, une moyenne de n'importe quelle statistique sur l'ensemble est égale (avec probabilité 1) à une moyenne sur les translations temporelles d'une fonction particulière de l'ensemble [12]. Pour le dire rapidement, on peut s'attendre à ce que chaque fonction, lorsque le temps progresse, avec la fréquence correcte, passe par toutes les convolutions de n'importe quelle fonction de l'ensemble.

De la même façon que l'on peut effectuer plusieurs opérations sur les nombres ou les fonctions pour obtenir d'autres nombres ou d'autres fonctions, on peut effectuer des opérations sur

[12] C'est le célèbre théorème d'ergodicité ou plutôt l'un des aspects de ce théorème qui a été démontré selon des formulations quelque peu différentes par Birkoff, von Neumann, et Koopman, et ensuite généralisé par Wiener, Hopf, Hurewicz et d'autres. La littérature concernant la théorie ergodique est assez conséquente et le lecteur peut se référer aux articles de ces auteurs pour des formulations précises et générales ; par exemple E. Hopf, "Ergodentheorie", Ergebnisse der Mathematik und ihrer Grenzgebiete, v. 5 ; "On Causality Statistics and Probability", *Journal of Mathematics and Physics*, v. XIII, No. 1, 1934 ; N. Wiener, "The Ergodic Theorem", Duke Mathematical Journal, v. 5, 1939.

les ensembles pour obtenir de nouveaux ensembles. Supposons par exemple qu'on ait un ensemble de fonctions $f_\alpha(t)$ et un opérateur $T$ qui donne pour chaque fonction $f_\alpha(t)$ une fonction résultante $g_\alpha(t)$ :

$$g_\alpha(t) = Tf_\alpha(t).$$

Une mesure de probabilité est définie pour l'ensemble $g_\alpha(t)$ à partir de celle pour l'ensemble $f_\alpha(t)$. La probabilité d'un certain sous-ensemble des fonctions $g_\alpha(t)$ est égale à celle du sous-ensemble des $f_\alpha(t)$ qui fournissent les éléments du sous-ensemble donné de $g$ selon l'opération $T$. Physiquement, cela correspond à faire passer l'ensemble à travers une sorte d'appareil physique, par exemple un filtre, un rectificateur, ou un modulateur. Les fonctions en sortie de l'appareil forment l'ensemble $g_\alpha(t)$.

Un appareil ou opérateur $T$ sera dit invariant si décaler l'entrée décale simplement la sortie, i.e. si

$$g_\alpha(t) = Tf_\alpha(t)$$

implique

$$g_\alpha(t + t_1) = Tf_\alpha(t + t_1)$$

pour toute $f_\alpha(t)$ et toute $t_1$. On montre facilement (voir Appendice 5) que si $T$ est invariant et si l'ensemble en entrée est stationnaire alors l'ensemble en sortie est stationnaire. De même, si l'entrée est ergodique alors la sortie sera également ergodique.

Un filtre ou un rectificateur est invariant selon toute translation temporelle. L'opération de modulation ne l'est pas puisque la phase porteuse donne une certaine structure temporelle. Pourtant, la modulation est invariante selon toute translation qui est multiple de la période de la phase.

Wiener a remarqué la relation profonde existant entre l'invariance d'appareils physiques selon des translations temporelles et la théorie de Fourier [13]. Il a montré, en fait, que si un appareil est linéaire ainsi qu'invariant, l'analyse de Fourier est alors l'outil mathématique adéquat pour gérer ce problème.

Un ensemble de fonctions est la représentation mathématique adéquate des signaux produits par l'émetteur (i.e. une source continue de production de messages) - par exemple le discours - et du bruit perturbant le signal. La théorie de la communication a pour objet principal, comme l'a souligné Wiener, non pas les opérations sur des fonctions particulières, mais les opérations sur les ensembles de fonctions. Un système de communication est conçu non pas

[13] La théorie de la communication doit beaucoup à Wiener pour de nombreux éléments de sa philosophie de base et de sa théorie. Son rapport classique NDRC, *The Interpolation, Extrapolation and Smoothing of Stationary Time Series* (Wiley, 1949), contient la première formulation claire de la théorie de la communication comme problème statistique, l'étude des opérations sur les suites temporelles. Ce travail, bien que principalement concerné par la prédiction linéaire et les problèmes de filtrage, est une référence collatérale importante en connexion avec le présent article. On doit aussi faire référence ici au livre de Wiener *Cybernetics* (Wiley, 1948), qui traite de problèmes généraux de communication et contrôle.

pour une fonction particulière du discours, et encore moins pour une onde sinusoïdale, mais pour l'ensemble des fonctions du discours.

## 19. Ensembles de fonctions à bande limitée

Si une fonction temporelle $f(t)$ est limitée à la bande s'étendant de 0 à $W$ cycles par seconde, elle est complètement déterminée par la donnée de ses ordonnées sur une suite de points discrets espacés de $\frac{1}{2W}$ secondes sauf dans la manière indiquée par le résultat suivant [14].

*Théorème 13 : Soit $f(t)$ ne contenant pas de fréquences au-dessus de $W$. Alors*

$$f(t) = \sum_{-\infty}^{\infty} X_n \frac{\sin \pi(2W_t - n)}{\pi(2W_t - n)}$$

*où*

$$X_n = f\left(\frac{n}{2W}\right).$$

Dans le développement, $f(t)$ est représentée comme une somme de fonctions orthogonales. Les coefficients $X_i$ des différents termes peuvent être considérés comme les coordonnées d'un "espace fonctionnel" infini-dimensionnel. Dans cet espace, toute fonction correspond précisément à un point et tout point à une fonction.

Une fonction peut être considérée comme étant substantiellement limitée à une durée $T$ si toutes les ordonnées $X_n$ en dehors de cet intervalle de temps sont nulles. Dans ce cas, toutes les coordonnées sauf $2TW$ d'entre elles seront nulles. Ainsi, les fonctions limitées à une bande $W$ et une durée $T$ correspondent aux points dans un espace à $2TW$ dimensions.

Un sous-ensemble des fonctions de bande $W$ et de durée $T$ correspond à une région dans cet espace. Par exemple, les fonctions dont l'énergie totale est inférieure ou égale à $E$ correspondent aux points dans une sphère $2TW$-dimensionnelle de rayon $r = \sqrt{2WE}$.

Un ensemble de fonctions de durée et de bande limitées sera représentée par une distribution de probabilité $p(x_1, ..., x_n)$ dans l'espace correspondant $n$-dimensionnel. Si l'ensemble n'est pas limité en temps, on peut considérer les $2TW$ coordonnées dans un intervalle donné $T$ pour représenter substantiellement la partie de la fonction dans l'intervalle $T$ et la distribution de probabilité $p(x_1, ..., x_n)$ pour donner la structure statistique de l'ensemble pour les intervalles de cette durée.

[14] Pour une preuve de ce théorème et la discussion qui suit, voir l'article de l'auteur "Communication in the Presence of Noise" publié dans les *Proceedings of the Institute of Radio Engineers*, v. 37, No. 1, Jan., 1949, pp. 10-21.

## 20. Entropie d'une distribution continue

L'entropie d'un ensemble discret de probabilités $p_1, \ldots, p_n$ a été défini par :

$$H = -\sum p_i \log p_i$$

De manière analogue, on définit l'entropie d'une distribution continue avec la fonction de distribution de la densité $p(x)$ par :

$$H = -\int_{-\infty}^{\infty} p(x) \log\, p(x) dx.$$

Avec une distribution $n$-dimensionnelle $p(x_1, ..., x_n)$, on a

$$H = -\int ... \int p(x_1, ..., x_n) \log\, p(x_1, ..., x_n) dx_1 \ldots dx_n.$$

Si on a deux arguments $x$ et $y$ (qui peuvent eux-mêmes être multi-dimensionnels), les entropies conjointes et conditionnelles de $p(x, y)$ sont données par

$$H(x, y) = -\iint p(x, y) \log\, p(x, y) dx dy$$

et

$$\begin{aligned} H_x(y) &= -\iint p(x, y) \log \frac{p(x, y)}{p(x)} dx dy \\ H_y(x) &= -\iint p(x, y) \log \frac{p(x, y)}{p(y)} dx dy \end{aligned}$$

où

$$\begin{aligned} p(x) &= \int p(x, y) dy \\ p(y) &= \int p(x, y) dx. \end{aligned}$$

Les entropies des distributions continues ont la plupart (mais pas toutes) les propriétés du cas discret. En particulier, on a les éléments suivants :

1. Si $x$ est limité à un certain volume $\nu$ dans son espace, alors $H(x)$ est un maximum et est égal à $\log \nu$ quand $p(x)$ est constant $(1/\nu)$ dans le volume.
2. Pour n'importe quelles variables $x, y$ on a

   $$H(x, y) \leq H(x) + H(y)$$

   avec égalité si (et seulement si) $x$ et $y$ sont indépendantes, i.e. $p(x, y) = p(x)p(y)$ (à part potentiellement pour un ensemble de points de probabilité nulle).

3. Considérons une opération de calcul de la moyenne généralisée du type suivant :

$$p'(y) = \int a(x,y)p(x)dx$$

avec

$$\int a(x,y)dx = \int a(x,y)dy = 1, \qquad a(x,y) \geq 0.$$

Alors l'entropie de la distribution moyennée $p'(y)$ est supérieure ou égale à celle de la distribution originale $p(x)$.

4. On a

$$H(x,y) = H(x) + H_x(y) = H(y) + H_y(x)$$

et

$$H_x(y) \leq H(y).$$

5. Soit $p(x)$ une distribution uni-dimensionnelle. La forme de $p(x)$ d'entropie maximum qui respecte la condition que la déviation standard de $x$ soit fixée à $\sigma$ est gaussienne. Pour montrer cela, on doit maximiser

$$H(x) = -\int p(x) \log\, p(x)dx$$

avec les contraintes

$$\sigma^2 = \int p(x)x^2dx \quad \text{et} \quad 1 = \int p(x)dx$$

Cela nécessite, par le calcul des variations, de maximiser

$$\int [-p(x) \log\, p(x) + \lambda p(x)x^2 + \mu p(x)]dx$$

La condition pour cela est

$$-1 - \log\, p(x) + \lambda x^2 + \mu = 0$$

et par conséquent (en ajustant les constantes pour satisfaire les contraintes)

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-x^2/2\sigma^2}$$

De façon similaire, en $n$ dimensions, supposons que les moments du second ordre de $p(x_1, ..., x_n)$ soient fixés à $A_{ij}$ :

$$A_{ij} = \int \ldots \int x_i x_j p(x_1, \ldots, x_n)dx_1 \ldots dx_n.$$

Alors l'entropie maximum a lieu (par un calcul similaire) quand $p(x_1, ..., x_n)$ est la distribution gaussienne $n$-dimensionnelle des moments du second ordre $A_{ij}$.

6. L'entropie d'une distribution gaussienne uni-dimensionnelle dont la déviation standard $\sigma$ est donnée par

$$H(x) = \log \sqrt{2\pi e}\sigma.$$

Elle se calcule comme suit :

$$\begin{aligned} p(x) &= \frac{1}{\sqrt{2\pi}\sigma} e^{-(x^2/2\sigma^2)} \\ -\log\, p(x) &= \log \sqrt{2\pi}\sigma + \frac{x^2}{2\sigma^2} \\ H(x) &= -\int p(x) \log\, p(x) dx \\ &= \int p(x) \log\, \sqrt{2\pi}\sigma dx + \int p(x) \frac{x^2}{2\sigma^2} dx \\ &= \log\, \sqrt{2\pi}\sigma \frac{\sigma^2}{2\sigma^2} \\ &= \log\, \sqrt{2\pi}\sigma + \log \sqrt{e} \\ &= \log\, \sqrt{2\pi e}\sigma. \end{aligned}$$

Similairement, la distribution gaussienne $n$-dimensionnelle de forme quadratique associée $a_{ij}$ est donnée par

$$p(x_1, ..., x_n) = \frac{|a_{ij}|^{\frac{1}{2}}}{(2\pi)^{n/2}} \exp\left(-\frac{1}{2} \sum a_{ij} x_i x_j\right)$$

et l'entropie peut être calculée comme

$$H = \log(2\pi e)^{n/2} |a_{ij}|^{-\frac{1}{2}}$$

où $|a_{ij}|$ est le déterminant dont les éléments sont les $a_{ij}$.

7. Si $x$ est limitée à une demi-droite ($p(x) = 0$ pour $x \leq 0$) et si le premier moment de $x$ est fixé à $a$ :

$$a = \int_0^\infty p(x) x dx,$$

alors l'entropie maximum a lieu quand

$$p(x) = \frac{1}{a} e^{-(x/a)}$$

et est égale à $\log ea$.

8. Il y a une différence importante entre les entropies continue et discrète. Dans le cas discret, l'entropie mesure de façon absolue le caractère aléatoire de la variable. Dans le cas continu, la mesure est relative au système de coordonnées. Si on change les coordonnées, l'entropie changera en général. En fait, si on change les coordonnées $y_1 \dots y_n$, la nouvelle entropie est donnée par

$$H(y) = \int \dots \int p(x_1, ..., x_n) J\left(\frac{x}{y}\right) \log p(x_1, ..., x_n) J\left(\frac{x}{y}\right) dy_1 \dots dy_n$$

où $J\left(\frac{x}{y}\right)$ est le jacobien de la transformation des coordonnées. En développant le logarithme et en changeant les variables en $x_1 \dots x_n$, on obtient :

$$H(y) = H(x) - \int \dots \int p(x_1, ..., x_n) \log\, J\left(\frac{x}{y}\right) dx_1 ... dx_n.$$

Ainsi, la nouvelle entropie est l'ancienne entropie moins le logarithme attendu du jacobien. Dans le cas continu, l'entropie peut être considérée comme une mesure du caractère aléatoire relativement à un standard supposé, notamment le système de coordonnées choisi, avec un poids identique affecté à chaque petit élément de volume $dx_1 \dots dx_n$. Quand on change le système de coordonnées, l'entropie du nouveau système mesure le caractère aléatoire quand les éléments de volume égaux $dy_1 \dots dy_n$ dans le nouveau système se voient affectés un même poids donné.

Malgré cette dépendance au système de coordonnées, le concept d'entropie est aussi important dans le cas continu que dans le cas discret. Cela est dû au fait que les concepts de taux d'information et de capacité du canal qui en découlent dépendent de la différence entre les deux entropies et cette différence ne dépend pas du modèle de coordonnées, chacun des deux termes étant changé d'une même quantité.

L'entropie d'une distribution continue peut être négative. L'échelle des mesures affecte un zéro arbitraire correspondant à une distribution uniforme sur un volume unité. Une distribution qui est plus confinée que cela a une entropie inférieure qui sera négative. Les taux et les capacités seront, pourtant, toujours non négatifs.

9. Un cas particulier de changement de coordonnées est le cas d'une transformation linéaire

$$y_j = \sum_i a_{ij} x_i.$$

Dans ce cas, le jacobien est simplement le déterminant $|a_{ij}|^{-1}$ et

$$H(y) = H(x) + \log |a_{ij}|.$$

Dans le cas d'une rotation des coordonnées (ou de n'importe quelle mesure préservant la transformation), $J = 1$ et $H(y) = H(x)$.

## 21. Entropie d'un ensemble de fonctions

Considérons un ensemble ergodique de fonctions limitées à une certaine bande de largeur $W$ cycles par seconde. Soient

$$p(x_1, ..., x_n)$$

la fonction de distribution de la densité pour les amplitudes $x_1, ..., x_n$ en $n$ points d'échantillon successifs. On définit l'entropie de l'ensemble par degré de liberté par

$$H' = -\operatorname*{Lim}_{n\to\infty} \frac{1}{n} \int \dots \int p(x_1, \dots, x_n) \log p(x_1, \dots, x_n) dx_1 \dots dx_n.$$

On peut aussi définir une entropie $H$ par seconde en divisant, non pas par $n$, mais par la durée $T$ en secondes pour $n$ exemples. Puisque $n = 2TW, H = 2W H'$.

Avec un bruit blanc thermique, $p$ est gaussienne et on a

$$\begin{aligned} H' &= \log \sqrt{2\pi e N}, \\ H &= W \log 2\pi e N. \end{aligned}$$

Pour une puissance moyenne donnée $N$, le bruit blanc a l'entropie maximum possible. Cela découle des propriétés de maximisation de la distribution gaussienne notées ci-dessus.

L'entropie d'un processus stochastique continu a de nombreuses propriétés analogues à celles des processus discrets. Dans le cas discret, l'entropie était liée au logarithme de la probabilité de longues suites, et au nombre de suites longues raisonnablement probables. Dans le cas continu, l'entropie est liée de façon similaire au logarithme de la densité de probabilité pour une longue suite d'exemples, et le volume de probabilité raisonnablement élevé dans l'espace de fonction.

Plus précisément, si l'on suppose $p(x_1, ..., x_n)$ continu selon tous les $x_i$ pour tout $n$, alors, pour $n$ suffisamment grand

$$\left| \frac{\log p}{n} - H' \right| < \epsilon$$

pour tous les choix de $(x_1, ..., x_n)$ sauf pour un ensemble dont la probabilité totale est inférieure à $\delta$, avec $\delta$ et $\epsilon$ arbitrairement petits. Cela découle de la propriété d'ergodicité si on divise l'espace en un grand nombre de petites cellules.

La relation de $H$ au volume peut s'énoncer comme suit : sous les mêmes hypothèses, considérons l'espace $n$-dimensionnel correspondant à $p(x_1, ..., x_n)$. Soit $V_n(q)$ le plus petit volume dans cet espace qui contient en son intérieur la probabilité totale $q$. Alors

$$\operatorname*{Lim}_{n\to\infty} \frac{\log V_n(q)}{n} = H'$$

à la condition que $q$ ne soit égal ni à 0 ni à 1.

Ces résultats montrent que pour $n$ grand, il y a un volume plutôt bien défini (au moins au sens logarithmique) de probabilité élevée, et que dans ce volume, la densité de probabilité est relativement uniforme (à nouveau au sens logarithmique). Dans le cas du bruit blanc, la distribution est donnée par

$$p(x_1, ..., x_n) = \frac{1}{(2\pi N)^{n/2}} \exp\left(-\frac{1}{2N}\sum x_i^2\right)$$

Puisqu'elle ne dépend que de $\sum x_i^2$, les surfaces de densité de probabilité égale sont des sphères et la distribution complète présente une symétrie sphérique. La région de probabilité forte est une sphère de rayon $\sqrt{nN}$. Lorsque $n \to \infty$, la probabilité d'être à l'extérieur d'une sphère de rayon $\sqrt{n(N+\epsilon)}$ approche de zéro et $\frac{1}{n}$ fois le logarithme du volume de la sphère approche de $\log \sqrt{2\pi eN}$.

Dans le cas continu, il est pratique de travailler avec l'entropie $H$ d'un ensemble mais avec une quantité dérivée qu'on appelle la puissance d'entropie. Celle-ci est définie comme la puissance d'un bruit blanc limité à la même bande que l'ensemble original et ayant la même entropie. En d'autres termes, si $H'$ est l'entropie d'un ensemble, la puissance de son entropie est

$$N_1 = \frac{1}{2\pi e} \exp 2H'.$$

D'un point de vue géométrique, cela revient à mesurer le volume de grande probabilité en élevant au carré le rayon d'une sphère ayant le même volume. Puisque le bruit blanc a l'entropie maximum pour une puissance donnée, la puissance d'entropie de n'importe quel bruit est inférieure ou égal à sa puissance effective.

## 22. Perte d'entropie dans les filtres linéaires

*Théorème 14 : Si un ensemble ayant l'entropie $H_1$ par degré de liberté dans la bande $W$ passe à travers un filtre de caractéristique $Y(f)$, l'ensemble en sortie a une entropie*

$$H_2 = H_1 + \frac{1}{W}\int_W \log |Y(f)|^2 df.$$

L'opération du filtre consiste essentiellement en une transformation linéaire des coordonnées. Si on considère les différentes composantes de fréquence comme système original de coordonnées, les nouvelles composantes de fréquence sont simplement les anciennes multipliées par certains facteurs. La matrice de transformation des coordonnées est ainsi essentiellement diagonalisée en fonction de ces coordonnées. Le jacobien de la transformation est (pour $n$ composantes sinus et $n$ composantes cosinus)

$$J = \prod_{i=1}^{n} |Y(f_i)|^2$$

où les $f_i$ sont espacés à écart fixe dans la bande $W$. Cela devient dans la limite

$$\exp \frac{1}{W} \int_W \log |Y(f)|^2 \, df.$$

Puisque $J$ est constante, sa valeur moyenne est la même quantité et en appliquant le théorème sur le changement d'entropie par changement de coordonnées, le résultat peut être déduit. On peut également l'exprimer en fonction de la puissance d'entropie. Ainsi, si la puissance d'entropie du premier ensemble est $N_1$, celle du second est

$$N_1 \exp \frac{1}{W} \int_W \log |Y(f)|^2 \, df.$$

L'entropie finale est l'entropie initiale multipliée par le gain moyen géométrique du filtre. Si le gain est mesuré en *db*, alors la puissance d'entropie en sortie sera augmentée du gain de la moyenne arithmétique *db* sur $W$.

Dans la Table, la puissance d'entropie perdue a été calculée (et également exprimée en *db*) pour un certain nombre de caractéristiques de gain idéal. Les réponses en impulsion de ces filtres sont également fournies pour $W = 2\pi$ avec une phase supposée nulle.

La perte d'entropie dans de nombreux autres cas peut être obtenue à partir de ces résultats. Par exemple, le facteur de la puissance d'entropie $1/e^2$ dans le premier cas s'applique également à n'importe quelle caractéristique de gain obtenu à partir de $1 - \omega$ par une mesure préservant la transformation de l'axe $W$. En particulier, un gain d'accroissement linéaire $G(\omega) = \omega$, ou une caractéristique en "dents de scie" entre 0 et 1 ont la même perte d'entropie. Le gain réciproque a un facteur réciproque. Ainsi $1/\omega$ a le facteur $e^2$. Élever le gain à n'importe quelle puissance élève le facteur à cette puissance.

TABLE I

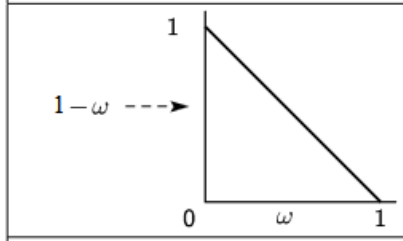
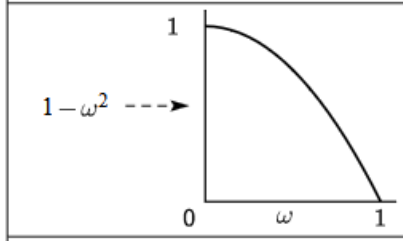
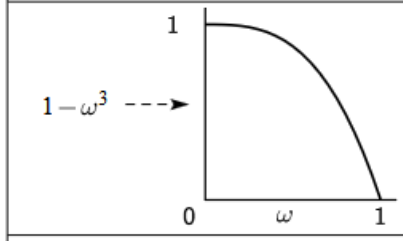
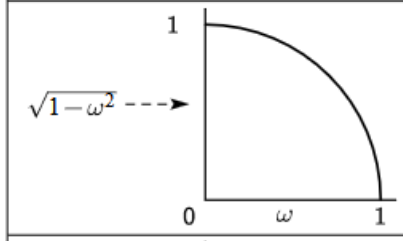
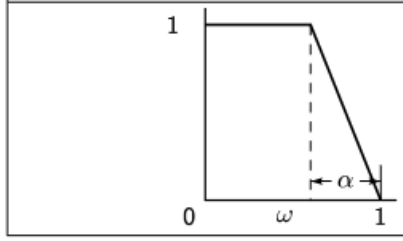
| GAIN | ENTROPY POWER FACTOR | ENTROPY POWER GAIN IN DECIBELS | IMPULSE RESPONSE |
|---|---|---|---|
|   | $\frac{1}{e^2}$ | −8.69 | $\frac{\sin^2(t/2)}{t^2/2}$ |
|   | $\left(\frac{2}{e}\right)^4$ | −5.33 | $2\left[\frac{\sin t}{t^3}-\frac{\cos t}{t^2}\right]$ |
|   | 0.411 | −3.87 | $6\left[\frac{\cos t-1}{t^4}-\frac{\cos t}{2t^2}+\frac{\sin t}{t^3}\right]$ |
|   | $\left(\frac{2}{e}\right)^2$ | −2.67 | $\frac{\pi}{2}\frac{J_1(t)}{t}$ |
|   | $\frac{1}{e^{2\alpha}}$ | $-8.69\alpha$ | $\frac{1}{\alpha t^2}\left[\cos(1-\alpha)t-\cos t\right]$ |

FIG. 13

## 23. ENTROPIE D'UNE SOMME DE DEUX ENSEMBLES

Si on a deux ensembles de fonctions $f_\alpha(t)$ et $g_\beta(t)$, on peut former un nouvel ensemble par "addition". Supposons que le premier ensemble ait la fonction de densité de probabilité $p(x_1, ..., x_n)$ et que le second ait $q(x_1, ..., x_n)$. Alors la fonction de densité pour la somme est donnée par la convolution :

$$r(x1, \ldots, x_n) = \int \ldots \int p(y_1, \ldots, y_n) q(x_1 - y_1, \ldots x_n - y_n) dy_1 \ldots dy_n.$$

Physiquement, cela correspond à ajouter les bruits ou les signaux représentés par les ensembles originaux de fonctions.

Le résultat suivant découle de l'Appendice 6.

*Théorème 15 : Soient les puissances moyennes de deux ensembles $N_1$ et $N_2$ et soient les puissances de leurs entropies $\overline{N}_1$ et $\overline{N}_2$. Alors, la puissance d'entropie de leur somme, $\overline{N}_3$, est bornée par*

$$\overline{N}_1 + \overline{N}_2 \leq \overline{N}_3 \leq N_1 + N_2.$$

Le bruit blanc gaussien a la propriété particulière de pouvoir absorber n'importe quel autre bruit ou ensemble de signaux qui peuvent lui être ajoutés avec une puissance d'entropie résultante environ égale à la somme de la puissance du bruit blanc et de la puissance du signal (mesurée à partie d'une valeur moyenne du signal, qui est normalement nulle), si la puissance du signal est petite, dans un certain sens, comparée au bruit.

Considérons un espace de fonctions associé à ces ensembles ayant $n$ dimensions. Le bruit blanc correspond à la distribution sphérique gaussienne dans cet espace. L'ensemble du signal correspond à une autre distribution de probabilités, non nécessairement gaussienne ou sphérique. Appelons les seconds moments de cette distribution par rapport à son centre de gravité $\alpha_j$. C'est-à-dire que si $p(x_1, ..., x_n)$ est la fonction de distribution de la densité

$$a_{ij} = \int \dots \int p(x_i - \alpha_i)(x_j - \alpha_j) dx_1 .... dx_n$$

où les $\alpha_i$ sont les coordonnées du centre de gravité. Maintenant $a_{ij}$ est une forme quadratique définie positive, et on peut faire tourner le système de coordonnées pour l'aligner avec les directions principales de cette forme. $a_{ij}$ se réduit alors à la forme diagonale $b_{ii}$. Cela nécessite que chaque $b_{ii}$ soit petit comparé à $N$, le carré du rayon de la distribution sphérique.

Dans ce cas, la convolution du bruit et du signal produit approximativement une distribution gaussienne dont la forme quadratique correspondante est

$$N + b_{ii}$$

La puissance d'entropie de cette distribution est

$$\left[\prod (N + b_{ii})\right]^{1/n}$$

ou environ. Le dernier terme est la puissance du signal, alors que le premier terme est la puissance du bruit.

$$= \left[(N)^n + \sum b_{ii} (N)^{n-1}\right]^{1/n}$$

$$\doteq N + \frac{1}{n} \sum b_{ii}.$$

# PARTIE IV : LE CANAL CONTINU

## 24. La capacité d'un canal continu

Dans un canal continu, l'entrée ou les signaux transmis seront des fonctions continues du temps $f(t)$ appartenant à un certain ensemble, et la sortie ou les signaux reçus seront des versions perturbées de ceux-ci. On considèrera seulement le cas où à la fois les signaux transmis et les signaux reçus sont limités dans une certaine bande $W$. Ils peuvent alors être spécifiés, pour une durée $T$, par $2TW$ nombres, et leur structure statistique peut être spécifiée par des fonctions de distribution de dimension finie. Ainsi, les statistiques du signal transmis seront déterminées par

$$P(x_1, ..., x_n) = P(x)$$

et celles du bruit le seront par la distribution de probabilité conditionnelle

$$P_{x_1,...,x_n} = P_x(y).$$

Le taux de transmission de l'information pour un canal continu est défini de manière analogue à celle qu'on a utilisée pour un canal discret, notamment

$$R = H(x) - H_y(x)$$

où $H(x)$ est l'entropie de l'entrée et où $H_y(x)$ est l'équivoque. La capacité du canal $C$ est définie comme le $R$ maximum, quand on fait varier l'entrée sur tous les ensembles possibles. Cela signifie que dans une approximation de dimension finie, on peut faire varier $P(x) = P(x_1, \ldots, x_n)$ et maximiser

$$-\int P(x) \log\, P(x)dx + \iint P(x,y) \log \frac{P(x,y)}{P(y)} dxdy.$$

Ceci peut s'écrire

$$\iint P(x,y) \log \frac{P(x,y)}{P(x)P(y)} dxdy$$

en utilisant le fait que $\iint P(x,y) \log P(x)dxdy = \int P(x) \log P(x)dx$. La capacité du canal s'exprime alors comme suit

$$C = \operatorname*{Lim}_{T\to\infty} \operatorname*{Max}_{P(x)} \frac{1}{T} \iint P(x,y) \log \frac{P(x,y)}{P(x)P(y)} dxdy.$$

Il est évident sous cette forme que $R$ et $C$ sont indépendants du système de coordonnées puisque le numérateur et le dénominateur dans $\log \dfrac{P(x,y)}{P(x)P(y)}$ sont multipliés par le même facteur quand $x$ et $y$ sont transformés de manière bijective. L'expression intégrale pour $C$ est plus générale que $H(x) - H_y(x)$. Correctement interprétée (voir l'appendice 7), elle existera toujours si l'on suppose que $H(x) - H_y(x)$ peut être une forme indéterminée $\infty - \infty$ dans

certains cas. Cela arrive, par exemple, si $x$ est limitée à une surface ayant moins de dimensions que $n$ dans son approximation $n$-dimensionnelle.

Si la base logarithmique utilisée pour le calcul de $H(x)$ et $H_y(x)$ est 2, alors $C$ est le nombre maximum de chiffres binaires qui peuvent être envoyés par seconde à travers le canal avec une équivoque arbitrairement petite, exactement comme dans le cas discret. Cela peut se constater physiquement en divisant l'espace des signaux en un grand nombre de petites cellules, suffisamment petites pour que la densité de probabilité $P_x(y)$ du signal $x$ étant perturbé au point $y$ soit substantiellement constante sur une cellule (soit $x$ soit $y$). Si les cellules sont considérées comme des points, la situation est essentiellement la même que dans le cas d'un canal discret et les preuves utilisées alors s'appliquent. Mais il est clair physiquement que cette quantification du volume en points individuels ne peut pas dans des situations pratiques altérer la réponse finale de façon significative, en supposant que les régions sont suffisamment petites. Ainsi la capacité sera la limite des capacités pour les subdivisions discrètes et ceci est exactement la capacité continue définie ci-dessus.

D'un point de vue mathématique, on peut d'abord démontrer (voir Appendice 7) que si $u$ est le message, $x$ est le signal, $y$ est le signal reçu (perturbé par le bruit) et $\nu$ est le message reconstitué alors

$$H(x) - H_y(x) \geq H(u) - H_\nu(u)$$

indépendamment des opérations qui sont effectuées sur $u$ pour obtenir $x$ ou sur $y$ pour obtenir $\nu$. Ainsi la manière dont on encode les chiffres binaires pour obtenir le signal n'a pas d'importance, ainsi que la manière dont on décode le signal reçu pour retrouver le message, le taux discret des chiffres binaires n'excède pas la capacité du canal que l'on a définie. D'un autre côté, il est possible selon des conditions très générales de trouver un système de codage pour transmettre des chiffres binaires au taux $C$ avec une équivoque ou une fréquence d'erreurs aussi petite que souhaitée. Cela est vrai, par exemple, si, quand on prend un espace de dimension approximativement finie pour les fonctions de signaux, $P(x, y)$ est continu à la fois en $x$ et en $y$ excepté pour un ensemble de points de probabilité nulle.

Un cas particulier a lieu quand le bruit est ajouté au signal et est indépendant de lui (au sens probabiliste). Alors $P_x(y)$ est une fonction de la différence $n = y - x$,

$$P_x(y) = Q(y - x)$$

et on peut assigner une entropie définie au bruit (indépendante des statistiques du signal), notamment l'entropie de la distribution $Q(n)$. Cette entropie sera notée $H(n)$.

*Théorème 16 : si le signal et le bruit sont indépendants et si le signal reçu est la somme du signal transmis et du bruit alors le taux de transmission est*

$$R = H(y) - H(n),$$

*i.e. l'entropie du signal reçu moins l'entropie du bruit. La capacité du canal est*

$$C = \operatorname*{Max}_{P(x)} H(y) - H(n).$$

On a, puisque $y = x + n$ :

$$H(x, y) = H(x, n).$$

En développant le côté gauche et en utilisant le fait que $x$ et $n$ sont indépendants

$$H(y) + H_y(x) = H(x) + H(n).$$

Par conséquent

$$R = H(x) - H_y(x) = H(y) - H(n).$$

Puisque $H(n)$ est indépendant de $P(x)$, maximiser $R$ nécessite de maximiser $H(y)$, l'entropie du signal reçu. S'il y a certaines contraintes sur l'ensemble des signaux transmis, l'entropie du signal reçu doit être maximisée en respectant ces contraintes.

## 25. Capacité d'un canal avec limitation de puissance moyenne

Une application simple du théorème 16 est le cas où le bruit est un bruit blanc thermique et où les signaux transmis sont limités par une certaine puissance moyenne $P$. Alors les signaux reçus ont une puissance moyenne $P + N$ où $N$ est la puissance moyenne du bruit. L'entropie maximum pour les signaux reçus a lieu quand ils forment également un ensemble de bruit blanc puisque c'est la plus grande entropie possible pour une puissance $P+N$ et elle peut être obtenue par un choix adéquat des signaux transmis, notamment s'ils forment un ensemble de bruit blanc de puissance $P$. L'entropie (par seconde) de l'ensemble reçu est alors

$$H(y) = W \log 2\pi e(P + N),$$

et l'entropie du bruit est

$$H(n) = W \log 2\pi e.$$

La capacité du canal est

$$C = H(y) - H(n) = W \log \frac{P + N}{N}.$$

Pour résumer, on a le théorème suivant :

*Théorème 17 : la capacité d'un canal de bande $W$ perturbé par un bruit blanc thermique de puissance $N$ quand la puissance moyenne de l'émetteur est limitée par $P$ est donnée par*

$$C = W \log \frac{P + N}{N}.$$

Cela signifie que par des systèmes suffisamment impliqués d'encodage, on peut transmettre des chiffres binaires au taux de $W \log_2 \frac{P + N}{N}$ bits par seconde, avec une fréquence d'erreur arbitrairement petite. Il n'est pas possible de transmettre à un niveau supérieur $N$ par un système d'encodage sans une fréquence définie positive d'erreurs.

Pour approximer ce taux limitant la transmission, les signaux transmis doivent approximer, dans leurs propriétés statistiques, un bruit blanc [15]. Un système qui approche le taux idéal peut être décrit comme suit : soient $M = 2^s$ exemples de bruit blanc construits, chacun étant de durée $T$. On leur assigne des nombres binaires de 0 à $M - 1$. Au niveau de l'émetteur, les suites de messages sont scindées en groupes de $s$ et pour chaque groupe, l'exemple de bruit correspondant est transmis comme signal. Au niveau du récepteur, les $M$ exemples sont connus et le signal effectif reçu (perturbé par le bruit) est comparé à chacun d'entre eux. L'exemple qui a la plus petite divergence de la R.M.S. (i.e. valeur moyenne réelle) [16] du signal reçu est choisi comme signal transmis et le nombre binaire correspondant est calculé. Ce processus revient à choisir le signal le plus probable (a posteriori). Le nombre $M$ des exemples de bruit utilisé dépend de la fréquence tolérable d'erreur $\epsilon$, mais pour presque tous les choix d'exemples, on a

$$\lim_{\epsilon \to 0} \lim_{T \to \infty} \frac{\log M(\epsilon, T)}{T} = W \log \frac{P+N}{N},$$

de telle façon que la petitesse du $\epsilon$ choisi n'a pas d'importance, et on peut, en prenant $T$ suffisamment grand, transmettre un nombre aussi proche que souhaité de $TW \log \frac{P+N}{N}$ chiffres binaires pendant la durée $T$.

Des formules similaires à $C = W \log \frac{P+N}{N}$ pour le bruit blanc ont pu être développées indépendamment de $N$ par plusieurs autres auteurs, bien que selon des interprétations quelque peu différentes. On peut mentionner les travaux de N. Wiener [17], W. G. Tuller [18], et H. Sullivan en connexion avec la section présente.

Dans le cas d'un bruit perturbateur arbitraire (non nécessairement un bruit blanc thermique), il ne semble pas que le problème de la maximisation pour déterminer la capacité du canal $C$ puisse être résolu explicitement. Pourtant on peut trouver des bornes supérieure et inférieure pour $C$ en fonction de la puissance moyenne du bruit $N$, et de la puissance d'entropie du bruit $N_1$. Ces bornes sont suffisamment proches l'une de l'autre dans la plupart des cas pratiques pour fournir une solution satisfaisante au problème.

*Théorème 18 : la capacité du canal de bande $W$ perturbé par un bruit arbitraire est bornée par les inégalités*

$$W \log \frac{P+N_1}{N_1} \leq C \leq W \log \frac{P+N}{N_1}$$

[15] Cette propriété ainsi que d'autres propriétés du cas du bruit blanc sont discutées du point de vue géométrique dans "Communication in the Presence of Noise", loc. cit.

[16] *Note de la traductrice : ou bien quadratique ?*

[17] *Cybernetics*, loc. cit.

[18] "Theoretical Limitations on the Rate of Transmission of Information", *Proceedings of the Institute of Radio Engineers*, v. 37, No. 5, May, 1949, pp. 468-78.

où

$$\begin{aligned} P &= \text{puissance moyenne de l'émetteur} \\ N &= \text{puissance moyenne du bruit} \\ N_1 &= \text{puissance d'entropie du bruit.} \end{aligned}$$

Ici aussi, la puissance moyenne des signaux perturbés serait $P + N$. L'entropie maximum pour cette puissance aurait lieu si les signaux reçus étaient du bruit blanc et elle serait égale à $W \log 2\pi e(P + N)$. Il peut ne pas être possible de réaliser cela ; i.e. il peut n'y avoir aucun ensemble de signaux transmis qui, ajouté à un bruit perturbateur, produise un bruit blanc thermique du côté du récepteur, mais au moins cela fournit une borne supérieure à $H(y)$. On a, par conséquent

$$\begin{aligned} C &= \text{Max } H(y) - H(n) \\ &\leq W \log 2\pi e(P + N) - W \log 2\pi e_1. \end{aligned}$$

Ceci est la limite supérieure fournie par le théorème. La borne inférieure peut être obtenue en considérant le taux si on rend le signal transmis avec un bruit blanc de puissance $P$. Dans ce cas, la puissance d'entropie du signal reçu doit être au moins aussi grande que celle d'un bruit blanc de puissance $P + N_1$ puisqu'on a montré dans un théorème précédent que la puissance d'entropie de la somme de deux ensembles est supérieure ou égale à la somme des puissances des entropies individuelles. Par conséquent

$$\text{Max } H(y) \geq W \log 2\pi e(P + N_1)$$

et

$$\begin{aligned} C &\geq W \log 2\pi e(P + N_1) - W \log 2\pi e N_1 \\ &= W \log \frac{P + N_1}{N_1}. \end{aligned}$$

Lorsque $P$ croît, les limites supérieure et inférieure s'approchent l'une de l'autre, de telle façon qu'on a le taux asymptotique

$$W \log \frac{P + N}{N_1}.$$

Si le bruit est lui-même blanc, $N = N_1$ et le résultat se réduit à la formule démontrée précédemment :

$$C = W \log \left(1 + \frac{P}{N}\right)$$

Si le bruit est gaussien mais avec un spectre qui n'est pas nécessairement plat, $N_1$ est la moyenne géométrique de la puissance du bruit sur les différentes fréquences dans la bande $W$. Ainsi

$$N_1 = \exp \frac{1}{W} \int_W \log N(f) df$$

où $N(f)$ est la puissance du bruit à la fréquence $f$.

*Théorème 19 : Si l'on définit la capacité pour la puissance donnée d'un émetteur $P$ comme étant égale à*

$$C = W \log \frac{P + N - \eta}{N_1}$$

*alors $\eta$ est décroissante monotone lorsque $P$ croît et approche 0 à la limite.*

Supposons que pour une puissance donnée $P_1$, la capacité du canal soit

$$W \log \frac{P_1 + N - \eta_1}{N_1}.$$

Cela signifie que la meilleure distribution du signal, disons $p(x)$, quand on l'ajoute à la distribution du bruit $q(x)$, donne une distribution reçue $r(y)$ dont la puissance d'entropie est $P_1 + N - \eta_1$. Faisons s'accroître la puissance jusqu'à $P_1 + \Delta P$ en ajoutant un bruit blanc de puissance $\Delta P$ au signal. L'entropie du signal reçu est maintenant au moins

$$H(y) = W \log 2\pi e(P_1 + N - \eta_1 + \Delta P)$$

par application du théorème sur la puissance d'entropie minimum d'une somme. Par conséquent, on peut atteindre le $H$ indiqué, l'entropie de la distribution maximisante doit être au moins aussi grande et $\eta$ doit être décroissante monotone. Pour montrer que $\eta \to 0$ lorsque $P \to \infty$, considérons un signal qui est un bruit blanc avec $P$ grand. Quel que soit le bruit perturbateur, le signal reçu sera approximativement un bruit blanc, si $P$ est suffisamment grand, au sens où il aura une puissance d'entropie approchant $P + N$.

## 26. La capacité d'un canal avec limitation de la puissance pic

Dans certaines applications, l'émetteur est limité non pas par la puissance moyenne possible pour la sortie mais par le pic de puissance instantanée. Le problème de calculer la capacité du canal est alors de maximiser (en faisant varier l'ensemble des symboles transmis)

$$H(y) - H(n)$$

en respectant la contrainte que toutes les fonctions $f(t)$ dans l'ensemble soient inférieures ou égales à $\sqrt{S}$, disons, pour tout $t$. Une contrainte de ce type ne marche pas mathématiquement aussi bien que la limitation de la puissance moyenne. Le seul résultat que nous ayons obtenu pour ce cas est une borne inférieure valide pour tout $\frac{S}{N}$, une borne supérieure "asymptotique" (valide pour $\frac{S}{N}$ grand) et une valeur asymptotique de $C$ pour $\frac{S}{N}$ petit.

*Théorème 20 : la capacité du canal $C$ pour une bande $W$ perturbé par un bruit blanc thermique de puissance $N$ est bornée par*

$$C \geq W \log \frac{2}{\pi e^3} \frac{S}{N},$$

*où $S$ est la puissance pic autorisée pour l'émetteur. Pour $\frac{S}{N}$ suffisamment grand*

$$C \leq W \log \frac{\frac{2}{\pi e} S + N}{N} (1 + \epsilon)$$

*où $\epsilon$ est arbitrairement petit. Lorsque $\frac{S}{N} \to 0$ (et à la condition que la bande $W$ commence en 0)*

$$C \Big/ W \log\left(1 + \frac{S}{N}\right) \to 1$$

On souhaite maximiser l'entropie du signal reçu. Si $\frac{S}{N}$ est grand, cela arrivera très près de l'endroit qui maximise l'entropie de l'ensemble transmis.

La borne supérieure asymptotique est obtenue en relaxant les conditions sur l'ensemble. Supposons que la puissance soit limitée à $S$ non pas à tout instant, mais seulement à des points échantillonés. L'entropie maximum de l'ensemble transmis sous ces conditions affaiblies est certainement plus grande ou égale à celle sous les conditions originales. Ce problème altéré peut être résolu aisément. L'entropie maximum a lieu quand les différents exemples sont indépendants et a une fonction de distribution qui est constante $-\sqrt{S}$ to $\sqrt{S}$. L'entropie est égale à

$$W \log 4S.$$

Le signal reçu aura alors une entropie inférieure à

$$W \log(4S + 2\pi eN)(1 + \epsilon)$$

avec $\epsilon \to 0$ lorsque $\frac{S}{N} \to \infty$ et la capacité du canal est obtenue en soustrayant l'entropie du bruit blanc, $W \log 2\pi eN$ :

$$W \log(4S + 2\pi eN)(1 + \epsilon) - W \log(2\pi eN) = W \log \frac{\frac{2}{\pi e}S + N}{N}(1 + \epsilon)$$

Ceci est la borne supérieure souhaitée pour la capacité du canal.

Pour obtenir une borne inférieure, considérons le même ensemble de fonctions. Laissons passer ces fonctions à travers un filtre idéal avec une caractéristique de transfert triangulaire. Le gain doit être l'unité à la fréquence 0 et doit décroître linéairement vers un gain de 0 à la fréquence $W$. On montre d'abord que les fonctions de sortie du filtre ont une limitation du pic de puissance $S$ à tous les instants (et non pas seulement aux points échantillonés). D'abord, on note qu'une pulsation $\frac{\sin 2\pi Wt}{2\pi Wt}$ entrant dans le filtre produit

$$\frac{1}{2}\frac{\sin^2 \pi Wt}{(\pi Wt)^2}$$

dans l'entrée. Cette fonction n'est jamais négative. On peut penser à la fonction de l'entrée (dans le cas général) comme à la somme d'une suite de fonctions décalées

$$a\frac{\sin 2\pi Wt}{2\pi Wt}$$

où $a$, l'amplitude de l'échantillon, n'est pas plus grande que $\sqrt{S}$. Par conséquent, la sortie est la somme des fonctions décalées de la forme non négative ci-dessus avec les mêmes coefficients. Ces fonctions étant non négatives, la valeur positive la plus grande pour n'importe quel $t$ est obtenue quand tous les coefficients $a$ ont leurs valeurs positives maximum, i.e. $\sqrt{S}$. Dans ce cas, la fonction en entrée était une constante d'amplitude $\sqrt{S}$ et puisque le filtre a un gain unité pour un courant continu, la sortie est la même. Par conséquent, l'ensemble de sortie a pour pic de puissance $S$.

L'entropie de l'ensemble de sortie peut être calculée à partir de la partie de l'ensemble d'entrée en utilisant le théorème traitant une telle situation. L'entropie de sortie est égale à l'entropie de l'entrée plus le gain géométrique moyen du filtre :

$$\int_0^W \log G^2 df = \int_0^W \log \left(\frac{W-f}{W}\right)^2 df = -2W.$$

Par conséquent, l'entropie de sortie est

$$W \log 4S - 2W = W \log \frac{4S}{e^2}$$

et la capacité du canal est supérieure à

$$W \log \frac{2}{\pi e^3} \frac{S}{N}.$$

On voudrait maintenant montrer que, pour de petites valeurs de $\frac{S}{N}$ (le pic de la puissance du signal sur la puissance moyenne du bruit blanc), la capacité du canal est approximativement

$$C = W \log \left(1 + \frac{S}{N}\right)$$

Plus précisément, $C \Big/ W \log \left(1 + \frac{S}{N}\right) \to 1$ lorsque $\frac{S}{N} \to 0$. Puisque la puissance moyenne du signal $P$ est inférieure ou égale au pic $S$, il s'ensuit que pour tout $\frac{S}{N}$,

$$C \leq W \log \left(1 + \frac{P}{N}\right) \leq W \log \left(1 + \frac{S}{N}\right)$$

Par conséquent, si on peut trouver un ensemble de fonctions tel qu'elles correspondent à un taux proche de $W \log \left(1 + \frac{S}{N}\right)$ et soient limitées à la bande $W$ et au pic $S$, le résultat sera démontré. Considérons l'ensemble de fonctions du type suivant. Une suite de $t$ échantillons ont la même valeur, soit $+\sqrt{S}$ soit $-\sqrt{S}$, alors les $t$ prochains échantillons ont la même valeur. La valeur pour une suite est choisie aléatoirement, de probabilité $\frac{1}{2}$ pour $+\sqrt{S}$ et $\frac{1}{2}$ pour $-\sqrt{S}$. Si cet ensemble passe à travers un filtre avec caractéristique de gain triangulaire (le gain unité

pour un courant continu), la sortie a son pic limité par $\pm S$. De plus, la puissance moyenne est presque $S$ et peut approcher cela en prenant $t$ suffisamment grand. L'entropie de la somme de cela et du bruit thermique peut être trouvée en appliquant le théorème sur la somme d'un bruit et d'un petit signal. Ce théorème s'appliquera si

$$\sqrt{t}\frac{S}{N}$$

est suffisamment petit. Cela peut être assuré en prenant $\dfrac{S}{N}$ suffisamment petit (après que $t$ ait été choisi). La puissance d'entropie sera égale à $S+N$ aussi proche d'une approximation que souhaité, et par conséquent, le taux de transmission est aussi proche qu'on le souhaite de

$$W \log \left( \frac{S+N}{N} \right).$$

## PARTIE V : TAUX POUR UNE SOURCE CONTINUE

### 27. Fonctions d'évaluation de la fidélité

Dans le cas d'une source discrète d'information, on a été capable de déterminer un taux défini de génération de l'information, notamment l'entropie du processus stochastique la sous-tendant. Avec une source continue, la situation est considérablement moins maîtrisée. En premier lieu, une quantité variant continument peut avoir un nombre infini de valeurs et requiert, de ce fait, un nombre infini de chiffres binaires pour être complètement spécifiée. Cela signifie que transmettre la sortie d'une source continue avec récupération exacte au point de réception nécessite, en général, un canal de capacité infinie (en bits par seconde). Puisque, ordinairement, les canaux ont un certain nombre de bruit, et donc une capacité finie, la transmission exacte est impossible.

Ceci, cependant, élude la question principale. Pratiquement, on n'est pas intéressé par une transmission exacte quand on a une source continue, mais seulement par une transmission avec un certain degré de tolérance. La question est, peut-on assigner un taux fini à une source continue quand on requiert seulement une certain fidélité du message reçu, mesurée d'une manière adéquate. Bien sûr, comme les contraintes de fidélité augmentent, le taux augmentera. On montrera qu'on peut, dans des cas très généraux, définir un tel taux, ayant la propriété qu'il est possible, par un encodage adéquat de l'information, de la transmettre sur un canal dont la capacité est égale au taux en question, et satisfait les contraintes de fidélité. Un canal de capacité inférieure est insuffisant.

Il est d'abord nécessaire de donner la formulation mathématique de l'idée de fidélité de la transmission. Considérons l'ensemble des messages d'une durée longue, disons $T$ secondes. La source est décrite en donnant la densité de probabilité, dans l'espace associé, qui gouverne la façon dont elle sélectionnera le message en question $P(x)$. Un système donné de communication est décrit (d'un point de vue externe) en donnant la probabilité conditionnelle $P_x(y)$ que si le message $x$ est produit par la source, le message reconstruit au point de réception

sera $y$. Le système comme un tout (incluant la source et le système de transmission) est décrit par la fonction de probabilité $P(x, y)$ d'avoir un message $x$ en entrée et un message $y$ en sortie finale. Si cette fonction est connue, les caractéristiques complètes du système sont connues du point de vue de la fidélité. Toute évaluation de la fidélité doit correspondre mathématiquement à une opération appliquée à $P(x, y)$. Cette opération doit au moins avoir les propriétés d'un simple ordonnancement des systèmes ; i.e. il doit être possible de dire de deux systèmes représentés par $P_1(x, y)$ et $P_2(x, y)$ que, selon notre critère de fidélité, soit (1) le premier est plus fidèle, soit (2) le second est plus fidèle, soit (3) les deux systèmes sont de même fidélité. Cela signifie qu'un critère de fidélité peut être représenté par une fonction évaluées numériquement,

$$\nu(P(x, y))$$

dont les arguments couvrent les différentes fonctions de probabilité possibles $P(x, y)$.

On va maintenant montrer que sous ces hypothèses très générales et raisonnables, la fonction $\nu(P(x, y))$ peut être écrite sous une forme qui semble beaucoup plus spécialisée, notamment comme une moyenne d'une fonction $\rho(x, y)$ sur l'ensemble des valeurs possibles de $x$ et $y$ :

$$\nu(P(x, y)) = \iint P(x, y)\rho(x, y)dxdy.$$

Pour obtenir cela, on a seulement besoin de supposer (1) que la source et le système sont ergodiques de telle façon qu'un très long exemple sera, avec une probabilité proche de 1, typique de l'ensemble, et (2) que l'évaluation est "raisonnable" au sens où il est possible, en observant une entrée et une sortie types, $x_1$ et $y_1$, de former une évaluation provisoire sur la base des exemples ; et si ces exemples voient leur durée augmenter, l'évaluation provisoire sera, avec la probabilité 1, une approche de l'évaluation exacte basée sur une connaissance complète de $P(x, y)$. Soit l'évaluation provisoire $\rho(x, y)$. Alors la fonction $\rho(x, y)$ approche (lorsque $T \to \infty$) une constante pour presque tous les $(x, y)$ qui sont dans la région de forte probabilité correspondant au système

$$\rho(x, y) \to \nu(P(x, y))$$

et on peut également écrire

$$\rho(x, y) \to \iint P(x, y)\rho(x, y)dxdy$$

puisque

$$\iint P(x, y)dxdy = 1.$$

Cela établit le résultat souhaité.

La fonction $\rho(x, y)$ a le type général d'une "distance" entre $x$ et $y$ [19]. Elle mesure combien il est indésirable (selon notre critère de fidélité) de recevoir $y$ lorsque $x$ est transmis. Le résultat

[19] Ce n'est pas une "métrique" au sens strict du terme, cependant, puisqu'en général, elle ne satisfait ni $\rho(x, y) = \rho(y, x)$ ni $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$.

général donné ci-dessus peut être énoncé comme suit : toute évaluation raisonnable peut être représentée comme une moyenne d'une fonction de distance sur l'ensemble des messages et des messages reconstitués $x$ et $y$ pondérés selon la probabilité $P(x, y)$ d'obtenir les paires en question, si la contrainte que la durée $T$ des messages soit suffisamment grande est respectée.

Ci-dessous sont fournis des exemples simples de fonctions d'évaluation :

1. critère R.M.S.
$$\nu = \overline{(x(t) - y(t))^2}.$$
Dans cette mesure très communément utilisée de la fidélité, la fonction distance $\rho(x, y)$ est (à un facteur constant près) le carré de la distance euclidienne ordinaire entre les points $x$ et $y$ dans l'espace de fonctions associé.
$$\rho(x, y) = \frac{1}{T} \int_0^T [x(t) - y(t)]^2 dt$$

2. Critère R.M.S. pondéré de distance. Plus généralement, on peut appliquer différents poids aux différentes composantes fréquentielles avant d'utiliser la mesure de fidélité R.M.S. Ceci est équivalent à faire passer la différence $x(t) - y(t)$ à travers un filtre de forme et à déterminer la puissance moyenne dans la sortie. Donc soit
$$e(t) = x(t) - y(t)$$
et
$$f(t) = \int_{-\infty}^{\infty} e(\tau) k(t - \tau) d\tau$$
alors
$$\rho(x, y) = \frac{1}{T} \int_0^T f(t)^2 dt.$$

3. Critère d'erreur absolue.
$$\rho(x, y) = \frac{1}{T} \int_0^T |x(t) - y(t)| dt$$

4. La structure de l'oreille et du cerveau déterminent implicitement une évaluation, ou plutôt un certain nombre d'évaluations, appropriées dans les cas du discours et de la transmission musicale. Il y a, par exemple, un critère d'"intelligibilité" selon lequel $\rho(x, y)$ est égale à la fréquence relative de mots incorrectement interprétés quand le message $x(t)$ est reçu comme $y(t)$. Bien qu'on ne puisse pas donner une représentation explicite de $\rho(x, y)$ dans ces cas, ils pourraient, en principe, être déterminés par des expérimentations suffisantes. Certaines de ces propriétés découlent de résultats expérimentaux bien connus sur l'audition, par exemple l'oreille est relativement insensible à la phase, et la sensibitilié à l'amplitude et à la fréquence sont à peu près logarithmiques.
5. Le cas discret peut être considéré comme un cas particulier dans lequel on a tacitement supposé une évaluation basée sur la fréquence des erreurs. La fonction $\rho(x, y)$ est alors définie comme le nombre de symboles dans la séquence $y$ qui diffèrent de leur correspondant dans $x$, divisé par le nombre total de symboles de $x$.

## 28. Le taux pour une source par rapport à une évaluation de la fidélité

On est maintenant dans la capacité de définir un taux de génération de l'information pour une source continue. Sont donnés $P(x)$ pour la source et une évaluation $\nu$ déterminée par une fonction de distance $\rho(x, y)$ qui sera supposée continue à la fois en $x$ et en $y$. Avec un système particulier $P(x, y)$, la qualité est mesurée par

$$\nu = \iint \rho(x, y)P(x, y)dxdy.$$

De plus, le taux du flux de chiffres binaires correspondant à $P(x, y)$ est

$$R = \iint P(x, y) \log \frac{P(x, y)}{P(x)P(y)} dxdy.$$

On définit le taux $R_1$ de génération de l'information pour une qualité donnée $\nu_1$ de reproduction comme étant le $R$ minimum quand on garde $\nu$ fixé en $\nu_1$ et quand on fait varier $P_x(y)$. On obtient :

$$R_1 = \underset{P_x(y)}{\text{Min}} \iint P(x, y) \log \frac{P(x, y)}{P(x)P(y)} dxdy$$

en respectant la contrainte :

$$\nu_1 = \iint P(x, y)\rho(x, y)dxdy.$$

Cela signifie qu'on considère, en effet, tous les systèmes de communication qui peuvent être utilisés et qui transmettent avec la fidélité requise. Le taux de transmission en bits par seconde est calculé pour chacun et on choisit celui qui a le taux le plus faible. Ce dernier taux est le taux que l'on assigne à la source pour la fidélité en question.

La justification de cette définition repose sur le résultat suivant :

*Théorème 21 : Si une source a un taux $R_1$ pour une valuation $\nu_1$, il est possible d'encoder la sortie de la source et de la transmettre via un canal de capacité $C$ avec une fidélité aussi proche de $\nu_1$ que souhaité en supposant $R_1 \leq C$. Cela n'est pas possible si $R_1 > C$.*

Le dernier énoncé du théorème découle immédiatement de la définition de $R_1$ et des résultats précédents. Si ce n'était pas vrai, on pourrait transmettre plus de $C$ bits par seconde sur un canal de capacité $C$. La première partie du théorème est démontrée par une méthode analogue à celle qui a été utilisée pour le théorème 11. On peut, en premier lieu, diviser l'espace $(x, y)$ en un grand nombre de petites cellules et représenter la situation comme dans le cas discret. Cela ne changera pas la fonction d'évaluation de plus d'une quantité arbitrairement petite (quand les cellules sont très petites) à cause de la continuité supposée de $\rho(x, y)$. Supposons que $P_1(x, y)$ est le système particulier qui minimise le taux et donne $R_1$. On choisit aléatoirement parmi des $y$ de fortes probabilités un ensemble d'entre eux contenant

$$2^{(R_1+\epsilon)T}$$

des éléments pour lesquels $\epsilon \to 0$ lorsque $T \to \infty$. Avec de grandes valeurs de $T$, chaque point choisi sera relié par une arête de forte probabilité (comme dans la Fig. 10) à un ensemble de $x$. Un calcul similaire à celui utilisé pour prouver le théorème 11 montre que si $T$ est grand, presque tous les $x$ sont couverts par les gerbes sortant des points $y$ choisis pour presque tous les choix des $y$. Le système de communication à utiliser fonctionne comme suit : les points choisis se voient affecter des nombres binaires. Quand un message $x$ est initié, il apparaitra (avec une probabilité approchant 1 lorsque $T \to \infty$) dans au moins l'une des gerbes. Le nombre binaire correspondant est transmis (ou bien l'un d'eux choisi arbitrairement s'il y en a plusieurs) via le canal par des moyens de codage adéquats pour que la probabilité d'erreur soit petite. Puisque $R_1 \leq C$, il est possible de faire cela. Au point de réception, le $y$ correspondant est reconstruit et utilisé comme message entrant.

L'évaluation $\nu_1'$ pour ce système peut être rendue arbitrairement proche de $\nu_1$ en prenant $T$ suffisamment grand. Cela est dû au fait que pour chaque exemple long de message $x(t)$ et de message reconstruit $y(t)$, l'évaluation approche de $\nu_1$ (avec une probabilité 1).

Il est intéressant de noter que, dans ce système, le bruit dans le message reconstruit est effectivement produit par une sorte de quantification générale dans l'émetteur et n'est pas reproduite par le bruit dans le canal. Cela est plus ou moins analogue au bruit quantifiant dans la modulation MIC.

## 29. Le calcul des taux

La définition du taux est similaire par bien des aspects à la définition de la capacité d'un canal. Dans la première

$$R = \underset{P_x(y)}{\text{Min}} \iint P(x,y) \log \frac{P(x,y)}{P(x)P(y)} dxdy$$

avec $P(x)$ et $\nu_1 = \iint P(x,y)\rho(x,y)dxdy$ fixés. Dans la seconde,

$$C = \underset{P(x)}{\text{Max}} \iint P(x,y) \log \frac{P(x,y)}{P(x)P(y)} dxdy$$

avec $P_x(y)$ fixés et potentiellement, une ou plusieurs contraintes (par exemple, une limitation de la puissance moyenne) de la forme $K = \iint P(x,y)\lambda(x,y)dxdy$.

Une solution partielle du problème général de maximisation pour déterminer le taux d'une source peut être donnée. En utilisant la méthode de Lagrange, on considère

$$\iint \left[ P(x,y) \log \frac{P(x,y}{P(x)P(y)} + \mu P(x,y)\rho(x,y) + \nu(x)P(x,y) \right] dxdy.$$

L'équation variationnelle (quand on prend la première variation sur $P(x,y)$ ) amène à

$$P_y(x) = B(x)e^{-\lambda\rho(x,y)}$$

où $\lambda$ est déterminé pour donner la fidélité requise et $B(x)$ est choisi pour satisfaire

$$\int B(x)e^{-\lambda\rho(x,y)}dx = 1$$

Cela montre que, avec un meilleur encodage, la probabilité conditionnelle d'une certaine cause pour plusieurs $y$ reçus, $P_y(x)$ diminuera exponentiellement avec la fonction de distance $\rho(x,y)$ entre le $x$ et le $y$ en question.

Dans le cas particulier où la fonction de distance $\rho(x,y)$ dépend seulement de la différence (vectorielle) entre $x$ et $y$,

$$\rho(x,y) = \rho(x-y)$$

on a

$$\int B(x)e^{-\lambda\rho(x-y)}dx = 1$$

Par conséquent, $B(x)$ est constant, disons égal à $\alpha$, et

$$P_y(x) = \alpha e^{-\lambda\rho(x-y)}.$$

Malheureusement, ces solutions formelles sont difficiles à évaluer dans les cas particuliers et semblent être de peu de valeur. En fait, le calcul effectif des taux a été mené seulement dans un très petit nombre de cas simples.

Si la fonction de distance $\rho(x,y)$ est la divergence de carré moyen entre $x$ et $y$ et si l'ensemble du message est du bruit blanc, le taux peut être déterminé. Dans ce cas, on a

$$R = \text{Min}[H(x) - H_y(x)] = H(x) - \text{Max}H_y(x)$$

avec $N = \overline{(x-y)^2}$. Mais le Max $H_y(x)$ a lieu quand $y-x$ est un bruit blanc, et est égal à $W_1 \log 2\pi eN$ où $W_1$ est la largeur de bande de l'ensemble du message. Par conséquent

$$\begin{aligned} R &= W_1 \log 2\pi eQ - W_1 \log 2\pi eN \\ &= W_1 \log \frac{Q}{N} \end{aligned}$$

où $Q$ est la puissance moyenne du message. Cela prouve le théorème suivant :

*Théorème 22 : Le taux pour une source de bruit blanc de puissance $Q$ et de bande $W_1$ relative à une mesure de fidélité R.M.S. est*

$$R = W_1 \log \frac{Q}{N}$$

*où $N$ est l'erreur moyenne sur les moindres carrés autorisée entre les messages original et reconstruit.*

Plus généralement, avec n'importe quel message source, on peut obtenir des inégalités bornant le taux relatif à un critère d'erreur des moindres carrés moyen.

*Théorème 23 : Le taux de n'importe quelle source de bande $W_1$ est bornée par*

$$W_1 \log \frac{Q_1}{N} \leq R \leq W_1 \log \frac{Q}{N}$$

*où $Q$ est la puissance moyenne de la source, $Q_1$ sa puissance d'entropie et $N$ l'erreur des moindres carrés moyenne autorisée.*

La borne inférieure découle du fait que le Max $H_y(x)$ pour un $\overline{(x-y)^2} = N$ donné a lieu dans le cas du bruit blanc. La borne supérieure résulte d'un placement de points (utilisé dans la preuve du théorème 21) non pas de la meilleure manière mais aléatoirement dans une sphère de rayon $\sqrt{Q-N}$.


## Remerciements

L'auteur remercie ses collaborateurs aux Laboratoires, en particulier Ms. les Dr. H. W. Bode, Dr. J. R. Pierce, Dr. B. McMillan, et Dr. B. M. Oliver pour de nombreuses suggestions utiles et critiques tout au long de ce travail. Il exprime sa reconnaissance à M. le Professeur N. Wiener, dont l'élégante solution au problème du filtrage et de la prédiction d'ensembles stationnaires a considérablement influencé la pensée de l'auteur dans ce domaine.


## APPENDICE 5

Soit $S_1$ un sous-ensemble mesurable quelconque de l'ensemble $g$, et $S_2$ le sous-ensemble de l'ensemble $f$ qui donne $S_1$ selon l'opération $T$. Alors

$$S_1 = TS_2.$$

Soit $H^\lambda$ l'opérateur qui décale toutes les fonctions d'un ensemble de la durée $\lambda$. Alors

$$H^\lambda S_1 = H^\lambda T S_2 = T H^\lambda S_2$$

puisque $T$ est invariant et, par conséquent, commute avec $H^\lambda$. Par conséquent, si $m[S]$ est la mesure de probabilité de l'ensemble $S$,

$$\begin{aligned} m[H^\lambda S_1] &= m[T H^\lambda S_2] = m[H^\lambda S_2] \\ &= m[S_2] = m[S_1] \end{aligned}$$

où la seconde égalité provient de la définition de la mesure dans l'espace $g$, la troisième égalité puisque l'ensemble $f$ est stationnaire, et la dernière, du fait de la définition de la mesure de $g$ à nouveau.

Pour prouver que la propriété ergodique est préservée par les opérations invariantes, soit $S_1$ un sous-ensemble de l'ensemble $g$ qui est invariant par $H^\lambda$, et soit $S_2$ l'ensemble de toutes les fonctions $f$ qui se transforment dans $S_1$. Alors

$$H^\lambda S_1 = H^\lambda T S_2 = T H^\lambda S_2 = S_1$$

de telle manière que $H^\lambda S_2$ est inclus dans $S_2$ pour tout $\lambda$. Maintenant, puisque

$$m[H^\lambda S_2] = m[S_1]$$

cela implique

$$H^\lambda S_2 = S_2$$

pour tout $\lambda$ avec $m[S_2] \neq 0, 1$. Cette contradiction montre que $S_1$ n'existe pas.

## APPENDICE 6

La borne supérieure, $\overline{N}_3 \leq N_1 + N_2$, est due au fait que l'entropie maximum possible pour une puissance $N_1 + N_2$ a lieu quand on a un bruit blanc dans la puissance. Dans ce cas, la puissance d'entropie est $N_1 + N_2$.

Pour obtenir la borne inférieure, supposons qu'on ait deux distributions en $n$ dimensions $p(x_i)$ et $q(x_i)$ de puissances d'entropie $\overline{N}_1$ et $\overline{N}_2$. Quelle forme devraient prendre $p$ et $q$ pour minimiser la puissance d'entropie $\overline{N}_3$ de leur convolution $r(x_i)$ :

$$r(x_i) = \int p(y_i) q(x_i - y_i) dy_i.$$

L'entropie $H_3$ de $r$ est donnée par

$$H_3 = -\int r(x_i) \log r(x_i) dx_i.$$

On souhaite minimiser ceci en respectant les contraintes

$$\begin{aligned} H_1 &= -p(x_i) \log p(x_i) dx_i, \\ H_2 &= -q(x_i) \log q(x_i) dx_i. \end{aligned}$$

On considère alors

$$\begin{aligned} U &= -\int [r(x) \log\, r(x) + \lambda p(x) \log\, p(x) + \mu q(x) \log\, q(x)] dx \\ \delta U &= -\int [[1 + \log\, r(x)] \delta r(x) + \lambda [1 + \log\, p(x)] \delta p(x) + \mu [1 + \log\, q(x)] \delta q(x)]\, dx. \end{aligned}$$

Si $p(x)$ varie selon un argument particulier $x_i = s_i$, la variation dans $r(x)$ est

$$\delta r(x) = q(x_i - s_i)$$

et

$$\delta U = -\int q(x_i - s_i) \log\, r(x_i) dx_i - \lambda \log\, p(s_i) = 0$$

et similairement quand on fait varier $q$. Par conséquent, les conditions pour un minimum sont

$$\int q(x_i - s_i) \log\, r(x_i) dx_i = -\lambda \log\, p(s_i)$$

$$\int p(x_i - s_l) \log\, r(x_i) dx_i = -\mu \log\, q(s_i).$$

Si on multiplie la première équation par $p(s_i)$ et la seconde par $q(s_i)$ et qu'on intègre par rapport à $s_i$, on obtient

$$H_3 = -\lambda H_1$$

$$H_3 = -\mu H_2$$

ou en résolvant pour $\lambda$ et $\mu$ et en remplaçant dans les équations

$$H_1 \int q(x_i - s_i) \log\, r(x_i)) dx_i = -H_3 \log\, p(s_i)$$

$$H_2 \int p(x_i - s_i) \log\, r(x_i)) dx_i = -H_3 \log\, q(s_i).$$

Maintenant supposons que $p(x_i)$ et $q(x_i)$ sont normaux

$$p(x_i) = \frac{|A_{ij}|^{n/2}}{(2\pi)^{n/2}} \exp\left(-\frac{1}{2} \sum A_{ij} x_i x_j\right)$$

$$q(x_i) = \frac{|B_{ij}|^{n/2}}{(2\pi)^{n/2}} \exp\left(-\frac{1}{2} \sum B_{ij} x_i x_j\right).$$

Alors $r(x_i)$ sera aussi normal de forme quadratique $C_{ij}$. Si les inverses de ces formes sont $a_{ij}, b_{ij}, c_{ij}$ alors

$$c_{ij} = a_{ij} + b_{ij}$$

On souhaite montrer que ces fonctions satisfont les conditions de minimisation si et seulement si $a_{ij} = K b_{ij}$ et ainsi, donnent le minimum $H_3$ respectant les contraintes. D'abord on a

$$\log\, r(x_i) \;\; = \frac{n}{2} \log \frac{1}{2\pi} |C_{ij}| - \frac{1}{2} \sum C_{ij} x_i x_j$$

$$\int q(x_i - s_i) \log\, r(x_i) dx_i \;\; = \frac{n}{2} \log \frac{1}{2\pi} |C_{ij}| - \frac{1}{2} \sum C_{ij} s_i s_j - \frac{1}{2} \sum C_{ij} b_{ij}.$$

Cela devrait être égal à

$$\frac{H_3}{H_1}\left[\frac{n}{2}\log\frac{1}{2\pi}|A_{ij}| - \frac{1}{2}\sum A_{ij}s_i s_j\right]$$

ce qui nécessite que $A_{ij} = \frac{H_1}{H_3}C_{ij}$. Dans ce cas, $A_{ij} = \frac{H_1}{H_2}B_{ij}$ et les deux équations se réduisent à des identités.

## APPENDICE 7

Cette appendice indiquera une approche plus générale et plus rigoureuse des définitions centrales de la théorie de la communication. Considérons un espace de mesure de probabilités dont les éléments sont des paires ordonnées $(x, y)$. Les variables $x, y$ doivent être identifiées comme les signaux transmis et reçus possibles d'une certaine durée $T$. Appelons bande au-dessus de $S_1$ l'ensemble de tous les points dont la première coordonnée $x$ appartient à un sous-ensemble contenant $x$, et similairement, bande au-dessus de $S_2$, l'ensemble dont les $y$ appartiennent à $S_2$. On divise $x$ et $y$ en une collection de sous-ensembles mesurables ne se chevauchant pas $X_i$ et $Y_i$ proches du taux de transmission $R$ par

$$R_1 = \frac{1}{T}\sum_i P(X_i, Y_i)\log\frac{P(X_i, Y_i)}{P(X_i)P(Y_i)}$$

où

| | |
|---|---|
| $P(X_i)$ | est la mesure de probabilité de la bande au-dessus de $X_i$ |
| $P(Y_i)$ | est la mesure de probabilité de la bande au-dessus de $Y_i$ |
| $P(X_i, Y_i)$ | est la mesure de probabilité de l'intersection des bandes. |

Une sous-division supplémentaire ne peut jamais faire décroître $R_1$. Car si $X_1$ est divisé en $X_1 = X_1' + X_1''$ et si on a

$$\begin{array}{cc} P(Y_1) = a & P(X_1) = b + c \\ P(X_1') = b & P(X_1', Y_1) = d \\ P(X_1'') = c & P(X_1'', Y_1) = e \end{array}$$
$$P(X_1, Y_1) = d + e$$

Alors dans la somme, on remplace (pour l'intersection $X_1, Y_1$)

$$(d+e)\log\frac{d+e}{a(b+c)} \quad \text{par} \quad d\log\frac{d}{ab} + e\log\frac{e}{ac}.$$

On montre aisément qu'avec la limitation, on a sur $b, c, d, e$,

$$\left[\frac{d+e}{b+c}\right]^{d+e} \leq \frac{d^d e^e}{b^d c^e}$$

et par conséquent, la somme est augmentée. Ainsi les différentes subdivisions possibles forment un ensemble orienté, avec $R$ croissante monotone selon le granularité de la subdivision.

On peut définir $R$ de façon non ambigue comme la plus petite borne supérieure pour $R_1$ et l'écrire

$$R = \frac{1}{T} \iint P(x,y) \log \frac{P(x,y)}{P(x)P(y)} dxdy.$$

Cette intégrale, comprise au sens ci-dessus, inclut à la fois des cas discrets et des cas continus et bien sûr, de nombreux autres qui ne peuvent être représentés ni par une forme ni par l'autre. Il est trivial dans cette formulation que si $x$ et $u$ sont en bijection, le taux de $u$ vers $y$ est égal à celui de $x$ vers $y$. Si $\nu$ est n'importe quelle fonction de $y$ (n'ayant pas nécessairement une fonction inverse) alors le taux de $x$ vers $y$ n'est plus supérieur ou égal à celui de $x$ vers $\nu$ puisque, dans le calcul des approximations, les sous-divisions de $y$ sont principalement plus fines que celles pour $\nu$. Plus généralement, si $y$ et $\nu$ sont liées non pas fonctionnellement mais statistiquement, i.e. si on a un espace de mesure de probabilité $(y, \nu)$, alors $R(x,\nu) \leq R(x,y)$. Cela signifie que n'importe quelle opération appliquée au signal reçu, même si elle ne fait pas intervenir de statistiques, n'accroîtra pas $R$.

Une autre notion qui devrait être définie précisément par une formulation abstraite de la théorie est celle de "'taux de dimension", qui est le nombre moyen de dimensions requises par seconde pour spécifier un élément d'un ensemble. Dans le cas de la bande limitée, $2W$ nombres par seconde sont suffisants. Une définition générale peut être esquissée comme suit. Soit $f_\alpha(t)$ un ensemble de fonctions et soit $\rho_T[f_\alpha(t), f_\beta(t)]$ une métrique mesurant la "distance" de $f_\alpha$ à $f_\beta$ sur la durée $T$ (par exemple, la divergence R.M.S. sur cet intervalle). Soit $N(\epsilon, \delta, T)$ le plus petit nombre d'éléments $f$ qui peuvent être choisis de telle façon que tous les éléments de l'ensemble sauf un ensemble de mesure $\delta$ sont à distance $\epsilon$ d'au moins un de ceux choisis. Ainsi, on couvre l'espace de $\epsilon$ sauf un ensemble de petite mesure $\delta$. On définit le taux de dimension $\lambda$ pour l'ensemble par la triple limite

$$\lambda = \operatorname*{Lim}_{\delta \to 0} \operatorname*{Lim}_{\epsilon \to 0} \operatorname*{Lim}_{T \to \infty} \frac{\log N(\epsilon, \delta, T)}{T \log \epsilon}.$$

Ceci est une généralisation des définitions de type mesure de la dimension en topologie, et c'est en accord avec le taux intuitif de dimension pour des ensembles simples sur lesquels le résultat souhaité est évident.