www.polytechniquebruxelles.be
G Square
#14 | mars 2015

G²

Le magazine
de l'École polytechnique
de Bruxelles
et de ses Alumni

PLONGÉE DANS LA NANOSPHÈRE

L'INVISIBLE EN QUESTION

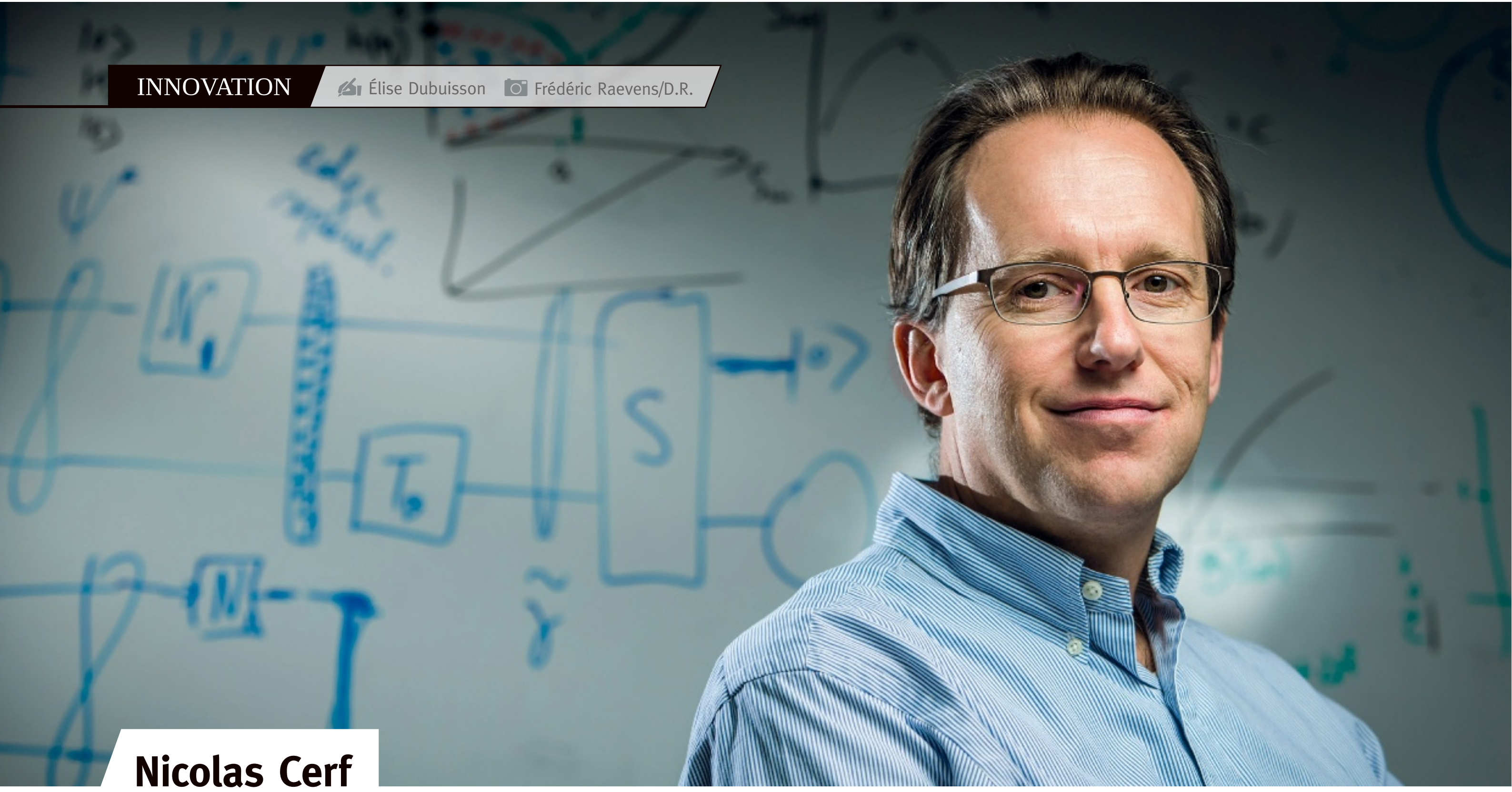
Céline Kermisch (ICEM 2000) et Philippe Busquin nous présentent le Cycle de Conférences 2015

ET AUSSI

Trimestriel - Bureau de dépôt: Anvers X - N° d'agréation: P 701323

ULB

Élise Dubuisson Frédéric Raevens/D.R.



Nicolas Cerf

La limite quantique des télécommunications

Domaine en pleine expansion, les télécommunications par fibres optiques sont partout aujourd'hui. Mais quelle est la limite ultime de nos canaux de télécommunication? La réponse de **Nicolas Cerf** et **Raul García-Patrón**.

Nous l'entendons tous les jours: nous vivons dans une société de l'information. Mais que recouvre exactement le terme d'information, et comment peut-on quantifier celle-ci? Par ailleurs, les réseaux de télécommunications sont de plus en plus performants, mais quelle est leur limite? Quel est le débit maximum d'un canal de communication?

SHANNON: LES BASES D'UNE THÉORIE

Cette question intéresse de nombreux chercheurs depuis déjà près d'un siècle, mais c'est généralement à Claude Shannon qu'est attribuée la paternité de la théorie de l'information. Cet ingénieur américain a joué un rôle clé, avec notamment le célèbre mathématicien anglais Alan Turing, dans le déchiffrage des codes secrets des nazis durant la seconde guerre mondiale. En 1948, il est le premier à avoir formalisé mathématiquement la notion d'information en termes d'entropie, révélant un lien profond avec la thermodynamique. «Sa théorie est à la base, cinquante ans plus tard, de nombreuses applications comme les codes correcteurs d'erreurs utilisés pour combattre les parasites dans nos téléphones cellulaires ou encore les techniques de compression de données permettant le streaming sur Internet», explique Nicolas Cerf, directeur du service Quantum Information and Communication (QuIC).

UNE FORMULE UNIVERSELLE

Shannon établit notamment une formule célèbre qui décrit la capacité d'un canal de communication à bruit blanc gaussien. C'est-à-dire le taux de transmission maximum qui peut idéalement être atteint par encodage dans un canal où le signal est entaché d'un bruit statistiquement distribué suivant une loi de Gauss et dont le spectre en fréquence est «plat» dans une bande donnée. Plus précisément, la formule de Shannon s'énonce $C = B \log_2(1 + P/N)$.

- C est la **capacité** (exprimée en bits/sec)
- B est la **largeur de bande** (en Hz)
- P/N est le **rapport de la puissance du signal sur la puissance du bruit**.

«Cette formule est universelle, et c'est tout son intérêt: elle ne dépend pas du procédé physique utilisé pour la communication, qu'il s'agisse d'impulsions électriques circulant dans un fil, d'ondes radio se propageant dans un câble coaxial ou en espace libre, etc.», détaille Nicolas Cerf. Sauf que Shannon considérait les communications dans le cadre de la physique classique, ignorant implicitement les porteurs microscopiques de l'information – par exemple les électrons formant le courant électrique. Autant cette approximation était justifiée pour les communications qui occupaient Shannon à son époque, autant ceci pose aujourd'hui question d'un point de vue fondamental.

LIMITE QUANTIQUE DE LA THÉORIE DE SHANNON

«Actuellement, les réseaux de télécommunications reposent en grande partie sur la fibre optique et l'envoi de messages sous forme d'impulsions lumineuses. Il est donc important aussi de connaître les limites de ce type de communications.» Et c'est là que la physique quantique entre en piste: «Vu les très hauts débits que permettent aujourd'hui ces réseaux optiques, on est amené à traiter des impulsions lumineuses de plus en plus courtes, dont la puissance en bout de ligne devient excessivement faible pour de longues portées. On tend donc progressivement vers un régime où l'on ne peut plus négliger les particules composant ces impulsions: les photons. Ce qui nous fait basculer du cadre de la physique classique vers celui de la physique quantique».

Les premiers travaux dans ce domaine sont attribués au physicien américain James Gordon et datent de 1962. Cependant, il faudra attendre les années 90 et la naissance des sciences de l'information quantique pour que des chercheurs développent les outils appropriés permettant d'aborder ce problème.

LES CANAUX BOSONIQUES GAUSSIENS

Le chercheur russe Alexander Holevo formalise alors dans un cadre quantique le calcul de la capacité de ce qu'on nomme les canaux bosoniques gaussiens – les photons appartenant à la famille de particules appelées bosons. «Le cas limite d'un canal optique idéal, sans aucune atténuation ni bruit, permet d'appréhender simplement le problème», affirme Raul García-Patrón, chercheur au QuIC.

SUITE EN PAGE 12

L'ENTROPIE D'UN MESSAGE

C'est de ses travaux visant à casser les codes nazis que Claude Shannon tira son inspiration sur ce qu'il appelle l'entropie d'un message, mesure statistique de la quantité d'information qu'il contient. Supposons que nous ayons M messages possibles et que la probabilité d'émission du $i^{\text{ème}}$ message soit p_i. D'après Shannon, la «surprise» qui survient lors de l'observation du $i^{\text{ème}}$ message peut se mesurer par $-\log_2 p_i$. Plus le message est rare, plus on est surpris de l'observer. Pour un flot de messages successifs, la valeur moyenne de la «surprise» devient:

$$H = -\sum_{i=1}^{N} p_i \log_2 p_i$$

Cette expression est appelée entropie de Shannon et son unité est le «bit». On peut voir H comme l'incertitude moyenne ou, à l'inverse, comme l'information contenue dans un message: c'est le nombre moyen de questions auxquelles il faut répondre par un bit – «oui» ou «non» – pour réduire le champ des possibles et identifier le message. Si les M messages ont tous la même probabilité $1/M$, on trouve simplement $H = \log_2 M$. Par exemple, l'annonce de la carte tirée au hasard dans un jeu de cartes apporte une information de $\log_2 32 = 5$ (il faut bien 5 bits pour coder le numéro de la carte en binaire).

UNE RECHERCHE À 4 MAINS

Pour parvenir à ces résultats, Raul García-Patrón et Nicolas Cerf ont travaillé de concert tantôt à l'ULB, tantôt à l'étranger.

2007
Après une thèse au QuIC dans le domaine de la cryptographie quantique, Raul García-Patrón part en postdoc au MIT de Boston. Il y rencontre des spécialistes des communications optiques quantiques travaillant sur la limite quantique de la théorie de Shannon.

2009 ET 2010
Sa curiosité piquée, Nicolas Cerf prend deux congés sabbatiques au MIT pour s'attaquer également à ce problème avec son ancien étudiant.

2013
Fort des connaissances acquises et des contacts scientifiques noués à l'étranger, Raul García-Patrón revient à l'ULB et y termine ses travaux avec Nicolas Cerf.

2014
Nicolas Cerf et Raul García-Patrón publient l'article «Ultimate classical communication rates of quantum optical channels» dans la revue Nature Photonics[1] (article cosigné avec Vittorio Giovannetti et Alexander Holevo).

Nicolas Cerf voit en ce sujet une occasion unique d'associer la physique quantique fondamentale et l'ingénierie des télécommunications.

«Si nous abordons ce canal par le biais de la théorie de Shannon, nous faisons vite face à une aberration puisque celle-ci indique que la capacité serait infinie (pour N=0). Or, physiquement, c'est inexact car le canal reste inévitablement entaché par un bruit d'origine quantique appelé bruit de photons.» Tenant compte de ce bruit de photons, Holevo ébauche une formule quantique de la capacité, mais il reste une grosse ombre au tableau: une conjecture mathématique non démontrée.

UN OBSTACLE DÉJOUÉ

Cette conjecture était considérée comme l'un des problèmes ouverts les plus difficiles de ce domaine. C'est dire si les travaux de Nicolas Cerf et Raul García-Patrón sont significatifs! Il s'agissait de prouver que, parmi tous les encodages quantiques possibles, c'est l'encodage gaussien qui est optimal. «Nous avons pris le problème sous son angle le plus élémentaire possible, en le ramenant à la tâche de minimiser l'entropie de sortie du canal gaussien», commente Nicolas Cerf. «Le défi était de montrer que c'est l'état du vide quantique à l'entrée du canal qui réalise ce minimum. Même si cela s'énonce simplement, c'était loin d'être simple à démontrer, et c'est grâce à un raisonnement reposant sur des notions avancées de physique quantique que nous sommes arrivés à bout de ce problème.»

L'état du vide quantique étant gaussien, l'encodage optimal était gaussien également, et la boucle était bouclée. Nicolas Cerf et Raul García-Patrón ont alors pu résoudre ce problème énoncé par Gordon il y a plus d'un demi-siècle, et valider la forme «quantiquement compatible» de la capacité de Shannon.

À côté de son intérêt conceptuel, cette version parachevée de la formule de Shannon ouvre la perspective d'accroître les performances des réseaux de télécommunications optiques grâce aux possibilités offertes par les technologies quantiques. Sur un ton plus futuriste, certains scientifiques osent même rêver tout haut de l'avènement, un jour, d'un véritable «Internet quantique»[2].

[1] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo, «Ultimate classical communication rates of quantum optical channels», Nature Photonics 8, 796 (2014).

[2] H. J. Kimble, «The quantum internet», insight in Nature 453, 1023 (2008).

NICOLAS CERF

1987 Ingénieur civil électro-mécanicien (ULB) /
Depuis 1998 Professeur à l'EPB où il dirige actuellement le service Quantum Information and Communication (QuIC)

RAUL GARCÍA-PATRÓN

2003 Ingénieur civil physicien (ULB) / **Actuellement** chercheur titulaire d'un mandat de retour de la Politique scientifique fédérale (BELSPO) au sein du service QuIC

CAP SUR L'ENCODAGE GAUSSIEN

De la formule de Shannon...

Shannon démontre que le taux de transmission maximum (la capacité) pouvant être atteint dans un canal s'obtient en maximisant la différence $H_{\rm out} - H_{\rm noise}$, où $H_{\rm noise}$ est l'entropie du signal de sortie obtenu lorsque le signal d'entrée est mis à zéro (entropie du bruit seul), tandis que $H_{\rm out}$ est l'entropie de la sortie entachée de bruit. La formule emblématique de Shannon décrit la capacité d'un canal affecté par un bruit gaussien et blanc dans une bande spectrale B. Un tel bruit est omniprésent car il résulte naturellement, en vertu d'un théorème statistique, de l'addition de perturbations indépendantes. Shannon montre que $H_{\rm noise} = Bf(N/u)$, où N est la puissance de bruit, u est une unité de puissance arbitraire, et $f(x) = \log_2 x$. De même, si P est la puissance d'entrée, la sortie bruyante aura la puissance $P + N$ et son entropie sera $H_{\rm out} = B\, f(P/u + N/u)$. En exprimant la différence d'entropies (en fait d'entropies par seconde), nous trouvons la capacité $C = B\,\log_2(1 + P/N)$, fonction du rapport P/N de la puissance du signal sur celle du bruit. À noter que seul le terme $H_{\rm out}$ doit être maximisé pour atteindre la capacité, alors que $H_{\rm noise}$ n'intervient pas.

...à sa version quantique

Les choses sont tout autres dans le cas quantique! La capacité du canal bosonique gaussien s'écrit également comme une différence d'entropies (quantiques), mais il ne suffit plus de maximiser le terme $H_{\rm out}$ seul car le principe d'incertitude de Heisenberg exclut de mettre à zéro un signal quantique! Grâce à la preuve de la conjecture, qui implique que $H_{\rm noise}$ est minimum si l'entrée est le vide quantique, les chercheurs ont montré qu'il faut remplacer la fonction $f(x)$ par $g(x) = (x+1)\log_2(x+1) - x\log_2 x$, où x devient un nombre moyen de photons. En effet, l'énergie d'une impulsion (puissance intégrée sur la durée de l'impulsion) vaut le nombre de photons qu'elle contient multiplié par le quantum d'énergie $h\nu$, où h est la constante de Planck et ν est la fréquence. La capacité s'exprime donc comme $C = B\,g(P+N) - B\,g(N)$, où P et N décrivent ici le nombre moyen de photons reçus contribuant respectivement au signal et au bruit. On vérifie que la divergence $f(0) \to -\infty$ responsable de tous les maux de la formule de Shannon a disparu ici, puisque $g(0) \simeq 0$. D'autre part, on retrouve bien la formule de Shannon à la limite classique puisque $g(x) \simeq f(x)$ quand $x \to \infty$, c'est-à-dire quand le nombre de photons de signal et de bruit est énhaurme dans chaque impulsion.

LA FONDATION ULB annonce la création du

FONDS PRIX NOBEL FRANCOIS ENGLERT

dédié à la recherche d'excellence en sciences exactes et naturelles

Faites un don **avec la communication « FONDS PRIX NOBEL FRANCOIS ENGLERT»**

Exonération fiscale à partir de 40€

par virement IBAN : BE95 3630 4292 4358 BIC : BBRUBEBB

www.fondation.ulb.ac.be