REAL ACADEMIA GALEGA DE CIENCIAS

A DERRADEIRA ADIVIÑA DE SHANNON

DISCURSO DO ACADÉMICO NUMERARIO ELECTO

SR. D. FERNANDO PÉREZ GONZÁLEZ

LEÍDO NO ACTO DA SÚA TOMA DE POSESIÓN
O DÍA 2 DE XULLO DE 2014

REAL ACADEMIA
GALEGA DE CIENCIAS

Cando emprendas a túa viaxe cara a Ítaca,
debes pregar que o camiño sexa longo,
cheo de peripecias, cheo de experiencias.
Constantino Kavafis, Ítaca

Excelentísimo Señor Presidente,
Excelentísimo Reitor Magnífico da Universidade de Vigo,
Excelentísimos Señores Académicos,
Autoridades, colegas e amigos,

I

O pasado 12 de setembro de 2013, a NASA anunciaba que a sonda Voyager 1 atravesara a heliopausa e entrara no espazo interestelar o 25 de agosto de 2012, converténdose no primeiro obxecto fabricado pola humanidade en aproximarse aos confíns do Sistema Solar. Semellante logro non era senón un fito máis dun periplo iniciado 36 anos antes e que incluíra etapas como os seus achegamentos a Xúpiter e Saturno en 1979 e 1980, respectivamente, dende onde enviara unhas aínda fascinantes e detalladas imaxes dos devanditos planetas, ata entón só ao alcance dos telescopios. Pero para moitos espectadores outra proeza probablemente pasou desapercibida: dende a heliopausa, a 18.000 millóns de quilómetros do Sol, a súa branca antena parabólica seguía transmitindo os datos obtidos polos poucos instrumentos de medida que aínda continuaban operativos.

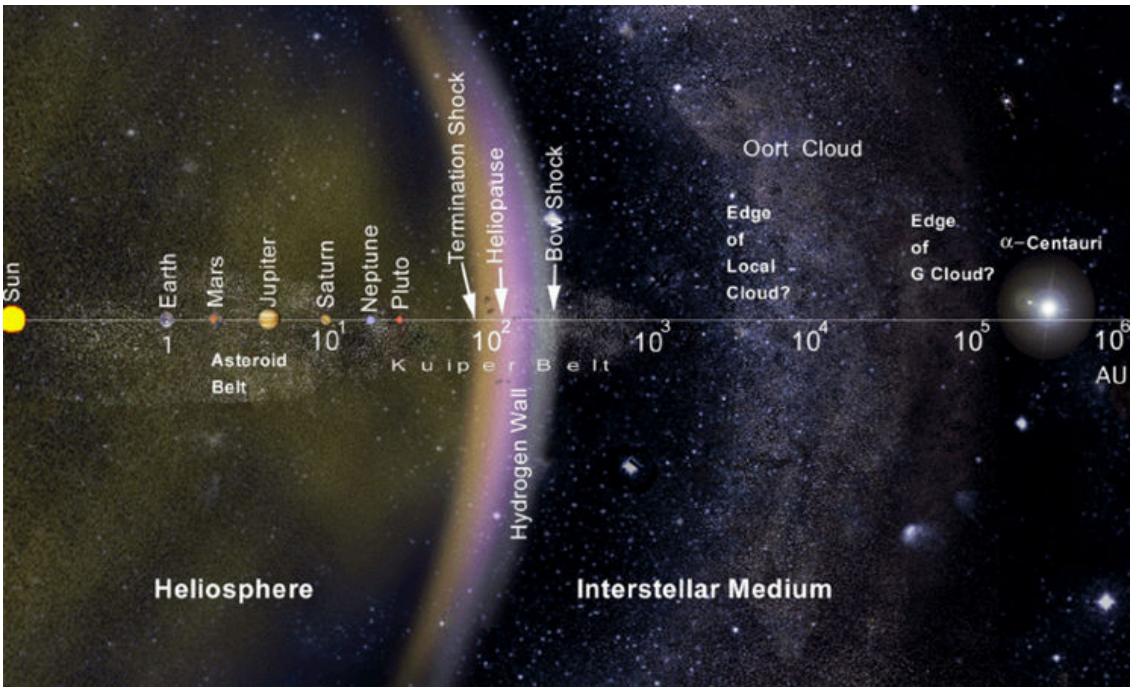

Figura 1: Situación da heliopausa e o espazo interestelar. Imaxe NASA.

Conseguir transmitir medidas dun modo fiable a unha distancia máis de 125 veces superior á que nos separa do Sol é parte doutra viaxe, tamén inconclusa, na que enxeñeiros e científicos foron capaces de resolver, con moito enxeño e un chisco de sorte, un problema que, case como unha adiviña, formulara unha das mentes máis sobresaíntes do século XX, Claude Shannon, en 1948. Propóñolles que repitamos esa viaxe a toda velocidade, deténdonos a observar algúns fitos de especial relevancia.

Figura 2: Un graffiti adicado a Claude Shannon. Fotografía: Thierry Ehrmann, Creative Commons 2.0

Calquera intento de definir a poliédrica personalidade de Shannon está condenado a fracasar. É preferible contentarse con dicir que era unha desas rara avis que encontra pracer tanto na abstracción matemática coma fedellando. Disto último, dan mostra as súas construcións dun robot capaz de emular a un malabarista ou un rato mecánico capaz de atopar a saída dun labirinto. Afeccionado aos xogos malabares, Shannon adoitaba pasearse polos lendarios laboratorios Bell, onde desenvolveu boa parte da súa carreira profesional, montado en monociclo.

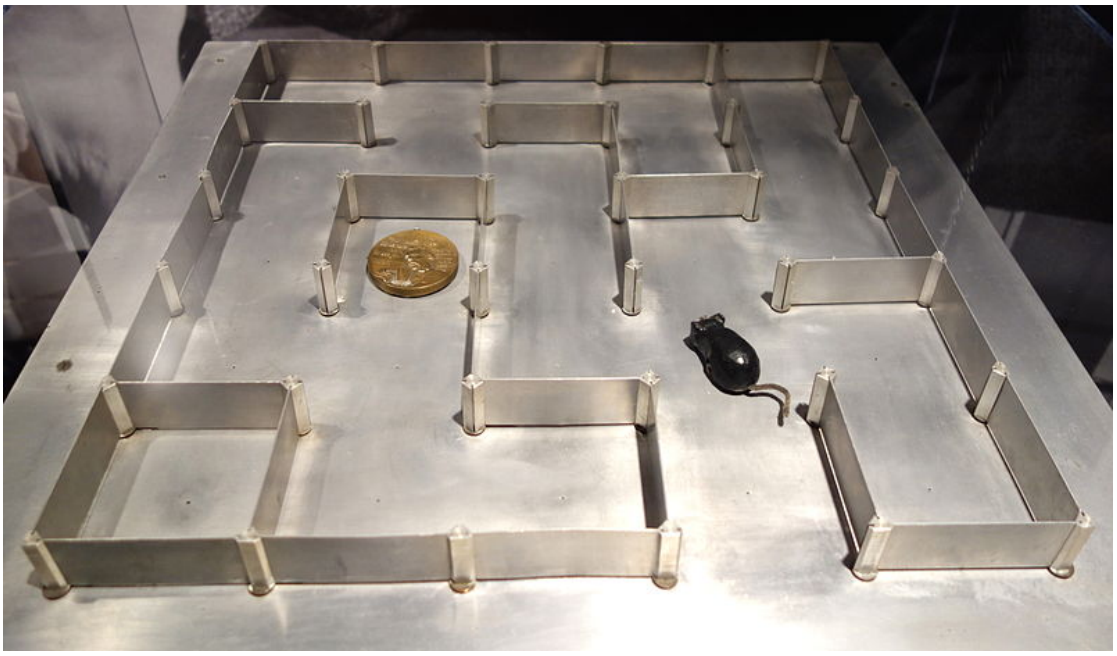

Figura 3: O rato mecánico de Shannon no Museo do MIT. Creative Commons 1.0

Pero Shannon pasou á historia polo seu artigo, publicado en 1948 na revista dos Laboratorios Bell, titulado *Unha teoría matemática da comunicación*. Robert Gallager, a quen volveremos encontrar máis adiante, xustamente dixo deste artigo que "contén os planos da era dixital". É tal a clarividencia que derrama o traballo de Shannon que resulta imposible valoralo sen equiparalo ás contribucións de Newton ou Einstein. Shannon define dun modo tan preciso o concepto de "información" que tropezarse por vez primeira no seu artigo co agora ubicuo termo *bit*[1] é case un simpático corolario. Shannon foxe dunha interpretación semántica, e polo tanto, subxectiva, de "información" e, en cambio, obxectívaa ao relacionala co concepto de "entropía"[2], que mide estatisticamente a desorde, e que importou el dende a Física neste contexto.

[1]A Tukey, outro curioso personaxe, debemos a invención de termo, que é acrónimo de *binary digit* (díxito binario).

[2]Shannon pensaba en chamala "incerteza", pero foi Von Neumann quen lle suxeriu que usase o termo "entropía", porque en mecánica estatística xa se empregaba con ese nome, e porque "ninguén sabía o que era realmente a entropía, así que nunha discusión sempre tería esa vantaxe".

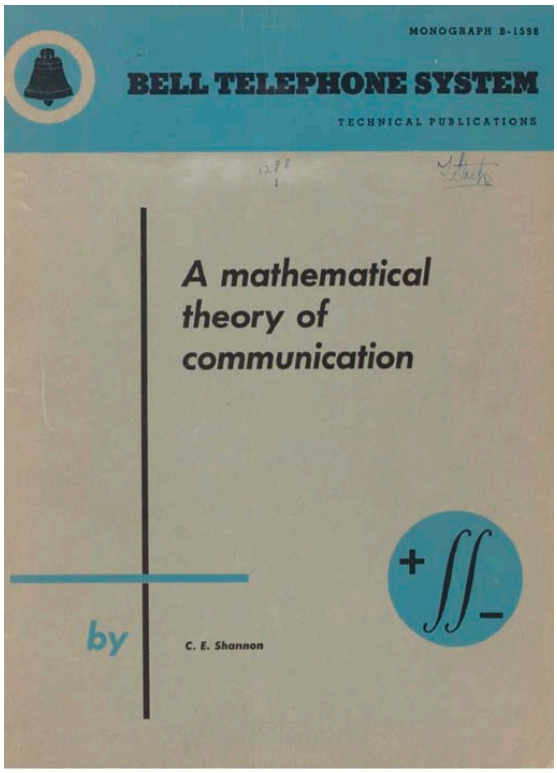

Figura 4: A portada da monografía dos Laboratorios Bell co artigo de Shannon

Se Shannon tivese sido investigador nos nosos días, os do "publica ou morre", posiblemente tería sucumbido á presión por filetear as súas ideas nunha lista inacabable e inabordable de artigos[3]. En cambio, *Unha teoría matemática da información*, coas suas 55 saborosas páxinas, adhírese á divisa gaussiana de "pauca sed matura" (poucos pero maduros) e aborda dous problemas esencialmente distintos, pero maxistralmente enlazados a través do concepto de "información". O primeiro é coñecido como o problema da "codificación de fonte". Un código de fonte é un método para representar a información co menor número de bits posible. Cando comprimimos un ficheiro nos coñecidos formatos "ZIP" ou "RAR" estamos a empregar un codificador de fonte; os populares formatos de compresión "JPEG" para imaxes ou "MPEG" para vídeos están baseados en códigos de fonte eficientes. Shannon enunciou e demostrou un teorema que cuantifica ata que punto se pode codificar unha fonte cando se impón unha restrición de fidelidade na reconstrución. Por exemplo, no caso de vídeos comprimidos, esta fidelidade mide en que grao o vídeo descomprimido se parece ao orixinal antes de

[3]A Shannon non lle gustaba escribir artigos. Nunha entrevista que lle fixo Robert Price en 1982 (véxase bibliografía), Shannon falaba de caixas enteiras de artigos inacabados no faiado.

comprimir. A maior distorsión permitida, maior compresión alcanzable. Pero o resultado de Shannon vai máis alá: se a fonte ten redundancia, entón pódese comprimir mesmo sen incorrer en distorsión na reconstrución. Isto sábeno ben os nosos mozos, que reinventaron un código de fonte para aforrar carácteres ao intercambiarse mensaxes de texto, aproveitándose da redundancia da linguaxe. Digo reinventado, porque se poden encontrar numerosos exemplos similares ao longo da Historia sempre que houbo un incentivo para iso; dende aproveitar o espazo ao tallar un obelisco ata pagar menos ao enviar un telegrama.

O segundo problema abordado por Shannon no seu prodixioso artigo é o da "codificación de canle". Neste caso pártese da existencia dunha canle de comunicacións a través da cal se quere transmitir información. As canles de comunicacións adoitan estar caracterizadas polo denominado "ancho de banda", que mide o tamaño do rango de frecuencias que se poden--por limitacións de natureza física ou legal--empregar para transmitir sinais. O outro parámetro esencial da canle é a potencia do ruído medida sobre ese ancho de banda. O ruído é o "inimigo a bater", porque deteriora as formas de onda transmitidas, ata o punto de poder facer confundir unhas con outras. A máis sinxela e mellor coñecida das canles de comunicacións é a chamada "canle gaussiana", así chamada porque o único efecto da canle é engadir ruído cuxa distribución estatística segue unha campá de Gauss. Para este tipo de canle, Shannon encontrou unha fórmula que determina a súa "capacidade" como unha función do ancho de banda, a potencia do ruído e a potencia transmitida. A capacidade é un parámetro esencial da canle que se pode interpretar como a velocidade binaria (en bits por segundo) á que se pode transmitir sobre a canle de forma "fiable".

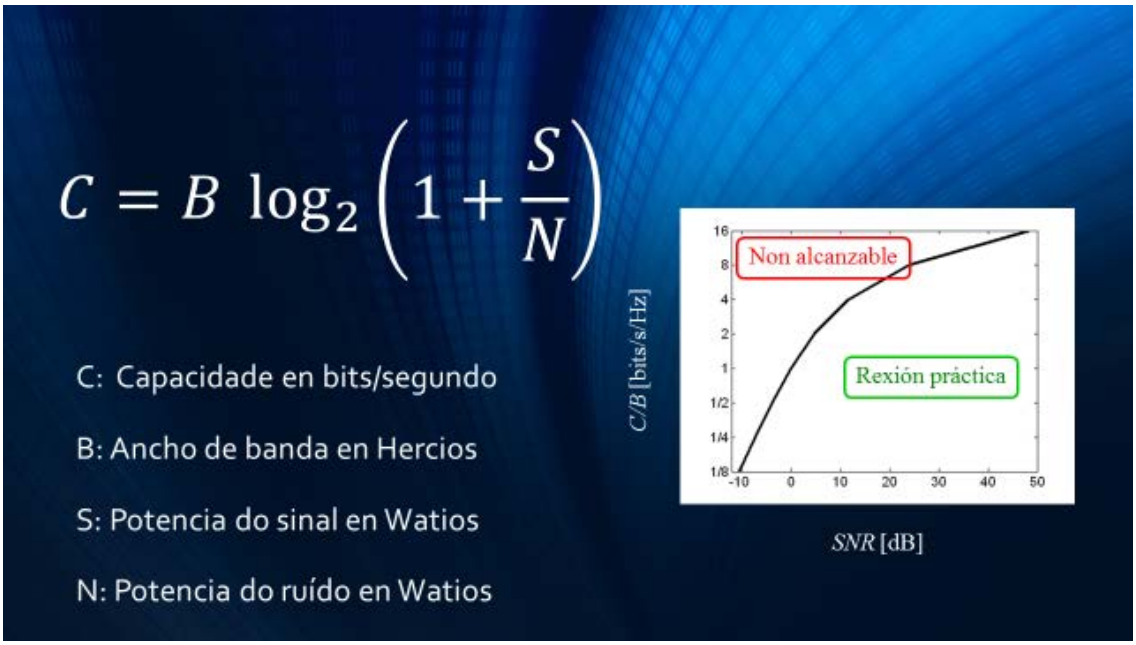

Figura 5: A célebre fórmula da capacidade de Shannon.

A fascinación que exerce o resultado de Shannon provén de que a capacidade se converte nunha barreira infranqueable, similar ao cono de luz relativista: para velocidades binarias superiores á capacidade, non é posible conseguir unha transmisión fiable; para velocidades inferiores, a teoría de Shannon demostra que é posible. Un "código de canle" é un método para converter a información en formas de onda que resistan do mellor modo posible o paso pola canle. Por ilustralo cun exemplo, cando ao deletrear por teléfono dicimos "pe de Pamplona" ou "te de Teruel" estamos a empregar un código de canle que trata de remediar o feito de que a canle telefónica distorsiona os fonemas "p" e "t" ata o punto de que resulta doado confundilos.

Cal é a diferenza entre codificación de fonte e de canle? Para explicalo, regresemos a 1980, no momento en que o Voyager 1 acaba de tomar unha imaxe de Saturno e se dispón a enviala á Terra. Para tratar de minimizar a cantidade de información a enviar e, polo tanto, o tempo total da transmisión, a fotografía comprímese utilizando un algoritmo de codificación de fonte. Para transmitir a imaxe comprimida de modo que o ruído da canle non produza erros, emprégase un código de canle. A codificación de fonte e de canle actúan con obxectivos aparentemente contrapostos: a codificación de fonte elimina a redundancia existente na fonte para representala dun xeito eficiente; a codificación de canle introduce redundancia para evitar que se produzan erros de transmisión. Sendo así, por que eliminar a

redundancia se se volve engadir despois? A resposta é que se trata de diferentes tipos de redundancia.

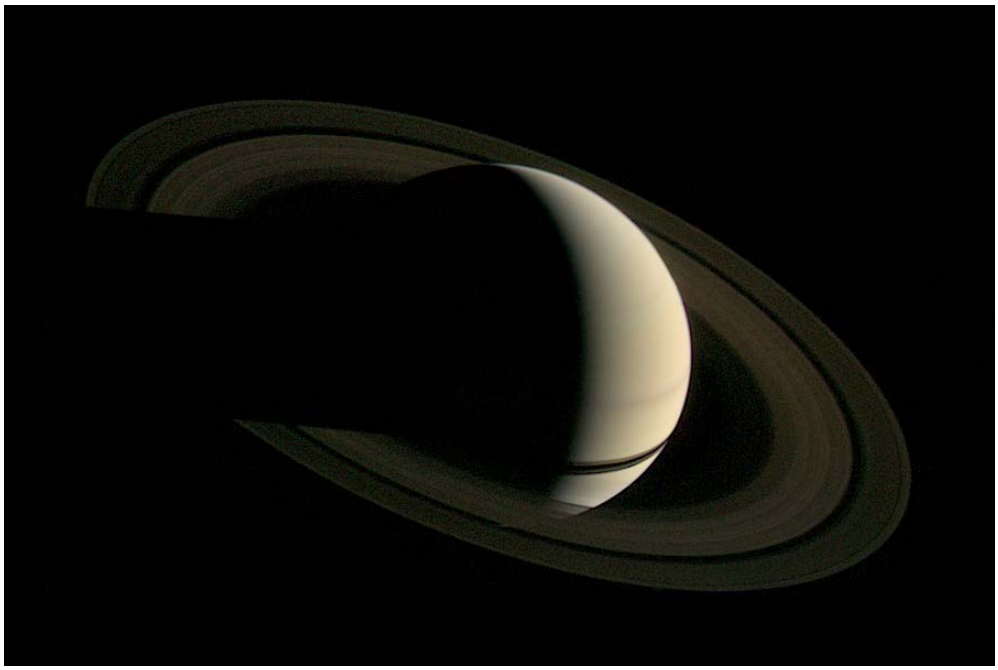

Figura 6: Unha das imaxes de Saturno tomadas polo Voyager 1. Fotografía NASA.

Agora que o Voyager 1 se encontra no espazo interestelar e xa non ten que enviar grandes volumes de datos podemos entender que o milagre da comunicación fiable non se encontra tanto na codificación de fonte coma na de canle. É por iso que aquí só abordarei a segunda. En particular, cando se fala de codificación de canle, adóitanse distinguir dous tipos de códigos: os que permiten detectar que houbo erros e os que non só son capaces de detectalos, senón de corrixilos. Os códigos de detección de erros son factibles naqueles casos en que se pode pedir a retransmisión da información que se recibiu con erros. O primeiro código coñecido, inventado no século II A.C polos escribas xudeus encargados de copiar a biblia incluía como elementos de control o número de palabras por liña ou a palabra central dunha páxina, o que permitía ao copista detectar erros, en cuxo caso tiraba a páxina mal copiada. Unha estratexia similar, loxicamente con códigos moito máis sofisticados, emprégase hoxe na maior parte dos protocolos de Internet.

Figura 7: Páxina do Códice de Alepo (s. X) coas anotacións "masoréticas" nos marxes. Fotografía: Ardon Bar Hama.

Non obstante, en moitos casos a retransmisión non é posible: por exemplo, na televisión dixital que recibimos nos nosos fogares non existe forma de comunicar ao transmisor que un paquete de datos se recibiu con erros. E aínda que a houbese, non sería práctica, porque seguramente en cada receptor os erros acontecerían en paquetes de datos diferentes, o que conduciría a miúdo a ter que retransmitir toda a información. No caso do Voyager 1, aínda que pode recibir sinais dende terra, tampouco é práctico pedir retransmisións, porque ademais de malgastar enerxía, á distancia que se encontra, o sinal propagándose á velocidade da luz tardaría máis de 17 horas. É por iso que os códigos correctores de erros revisten maior importancia e constitúen de feito o obxecto da análise de Shannon.

A Shannon, de carácter xovial e chistoso, apaixonábanlle os xogos lóxicos e as adiviñas. Lendo *O escaravello dourado* de Poe adquirira unha afección, que acabou sendo unha ocupación durante a Segunda Guerra Mundial, pola criptografía. Tomando unha idea do pai da intelixencia artificial, Marvin Minsky, construíu "a máquina definitiva", tamén coñecida como a máquina "déixenme en paz".

Imposible mellorar a descrición do artefacto que Arthur C. Clarke fixo no seu libro *Voice across the sea*:

"*Nada podería ser máis simple. Trátase simplemente dun pequeno cofre de madeira, do tamaño e a forma dunha caixa de cigarros, cun só interruptor nunha cara. Cando un empurra o interruptor, escóitase un zunido enfadado. A tapa levántase lentamente, e dende debaixo dela emerxe unha man. A man esténdese cara a abaixo, apaga o interruptor e refúxiase na caixa. Coa mesma finalidade dun ataúde pechado, a tapa se pecha de golpe, o zunido cesa e a paz reina de novo. O efecto psicolóxico, se un non sabe que esperar, é devastador. Hai algo indescritiblemente sinistro nunha máquina que non fai nada - absolutamente nada - agás apagarse.* "

Figura 8: A "máquina definitiva" no Museo do MIT a piques de autoapagarse. Creative Commons 2.0.

II

No seu famoso artigo Shannon deixou implícita unha adiviña aínda maior: a demostración do seu teorema da codificación de canle era, como dirían os matemáticos, non construtiva. Isto quere dicir que se ben establecía o límite fundamental (a capacidade) á velocidade binaria sobre a que se pode transmitir sobre unha canle, non dicía como podería deseñarse un bo código. Non parecía que coubese sequera buscar pistas sobre como facelo na construción usada por Shannon na súa demostración, porque se valía de códigos aleatorios de lonxitude non acoutada, o que en termos máis chairos quere dicir que, para poder comunicarse, transmisor e receptor deberían de compartir de antemán unha cantidade de información infinita. Aínda que a publicación do artigo de Shannon tivo un impacto inmediato na comunidade científica, haberíanse de necesitar uns 50 anos para resolver a súa adiviña: como construír códigos prácticos que se acheguen ao límite da capacidade? Non era tarefa doada; tanto contrastaba a sinxeleza dos quiméricos códigos de Shannon coas prestacións dos códigos prácticos que os expertos deseguida acuñaron un dito: "todos os códigos son bos, agás os que coñecemos".

Os primeiros intentos de deseñar códigos prácticos, que abranguen as primeiras décadas da investigación nesta materia, céntranse nos chamados "códigos alxébricos". O primeiro exemplo de código alxébrico coñecido, mesmo citado por Shannon no seu artigo, son os códigos Hamming, así chamados en honor ao seu inventor. A explicación do código Hamming (7,4) pódenos axudar a entender como funcionan. Este código toma un bloque de 4 bits de información e convérteo nun bloque de 7 bits engadindo redundancia. É doado ver que das 2 ^ 7 =128 combinacións de 7 bits en principio posibles, só se empregan 2 ^ 4 =16, que se denominan "palabras código". En transmisión envíase unha desas palabras código de 7 bits. Os erros producidos na canle poden cambiar o valor dalgúns deses bits, polo que o receptor busca aquela palabra código que teña menos diferenzas cos bits recibidos. Un pode entender que un bo código será aquel en que as palabras estean afastadas entre si. De feito, o código Hamming (7,4) ten a propiedade de que as 16 palabras código de 7 bits difiren unhas doutras en, polo menos, 3 bits. Polo tanto, se nun dos 7 bits se produce un erro, é posible corrixilo. O prezo é que agora temos que enviar 7 bits en lugar de 4. Puidera parecer entón que se require máis enerxía para transmitir cada bit de información, pero non é así, porque sen

codificación necesitariamos transmitir con máis potencia cada bit para que fose distinguible do ruído.

En xeral, os códigos (e os alxébricos son un bo exemplo) deséñanse para que a xeración da palabra código a partir dos bits de información sexa sinxela e, sobre todo, para que a descodificación sexa alcanzable en termos do número de operacións necesarias. Unha das familias de códigos alxébricos máis populares é a proposta por Reed e Solomon en 1960, que ofrece unhas prestacións excelentes cando se producen refachos de erros, razón pola que aínda se utilizan para corrixir erros como os producidos por rabuños nos discos compactos, ou os ocasionados por esvaecementos temporais do sinal de televisión dixital terrestre. A popularidade dos códigos Reed-Solomon ten moito que ver coa dispoñibilidade dun algoritmo de descodificación eficiente proposto por Berlekamp e perfeccionado por Massey.

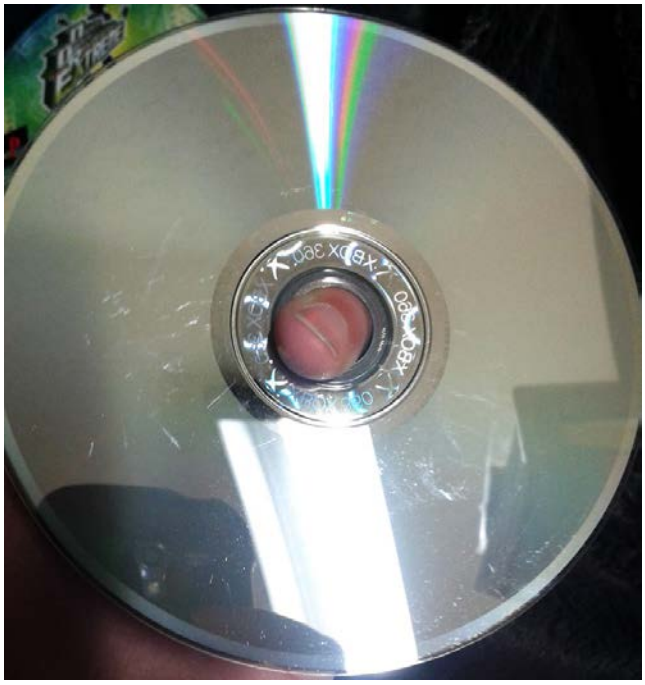

Figura 9: Un disco compacto con rabuños. Creative commons 3.0.

Un dos fitos da disciplina que comezou a chamarse neses anos "Teoría da Información" é a proposta en 1955 por parte de Peter Elias dunha familia de códigos alxébricos denominados "convolucionais". Conceptualmente máis complexos que os códigos que operan con simples bloques, os convolucionais constrúen unha reixa de interdependencias entre os bits que axudan a crear palabras código moi longas. Intuitivamente, cantos máis bits teñen as palabras código, maior é a dimensión do espazo matemático no que se poden representar,

polo que máis doado é conseguir separar unhas doutras. O problema dos códigos convolucionais naqueles momentos era a complexidade da descodificación, que facía prohibitivo o seu uso práctico. Recoñecendo o potencial que encerraban os códigos convolucionais, na década dos 60 iniciouse unha frenética actividade no MIT para buscar descodificadores eficientes. En 1961, Wozencraft foi o primeiro en propoñer un algoritmo de descodificación secuencial que aproveitaba a estrutura en reixa do código.

Xusto nesa mesma época, a NASA, que comezaba a enviar as primeiras sondas ao espazo, chegou á conclusión de que se se desexaba unha transmisión fiable e enerxeticamente eficiente da información, era necesario empregar codificación de canle. Pensando no código que se ía incorporar nas sondas Mariner que se lanzarían en 1969, os famosos Laboratorios de Propulsión a Chorro (JPL) optaron por un código bloque, porque o método de descodificación de Wozencraft seguía sen ser práctico. Paradoxalmente, en 1963, cando a decisión xa estaba tomada, Robert Fano no MIT propuxo un método que, en palabras de Massey moitos anos despois, era "o algoritmo máis sutil" que xamais vira. Fano é un dos grandes nomes da codificación de canle. Nacido en Turín, e emigrado a Estados Unidos coa súa familia cando tiña 22 anos, escapando da persecución de Mussolini aos xudeus, a Fano tamén debemos o terse decatado de que non é boa idea tirar información no receptor usando só un bit por cada bit transmitido; se non se empregan máis bits para tomar a decisión é imposible alcanzar o límite de Shannon. Esta observación xenial poñía os códigos convolucionais en franca vantaxe, porque se prestaban mellor ao que os enxeñeiros denominamos "decodificación branda".

Figura 10: Unha fotografía recente de Robert Fano. Creative commons 3.0.

O algoritmo de Fano para descodificar códigos convolucionais era tan eficiente que a NASA decidiu incluír un convolucional na sonda Pioneer 9, cuxo lanzamento estaba previsto para 1968. Para saltarse os longos procedementos de certificación, os circuítos que realizaban o codificador convolucional instaláronse como un "experimento de abordo", manténdose o sistema de comunicacións primario, que non levaba codificación algunha. En canto a sonda se lanzou, activouse o codificador convolucional para non o apagar xamais. Polo tanto, a Pioneer 9 ten a honra de ser a primeira sonda que incluíu codificadores de canle, antes das Mariner de 1969, ás que prexudicou ter discorrido pola canle oficial.

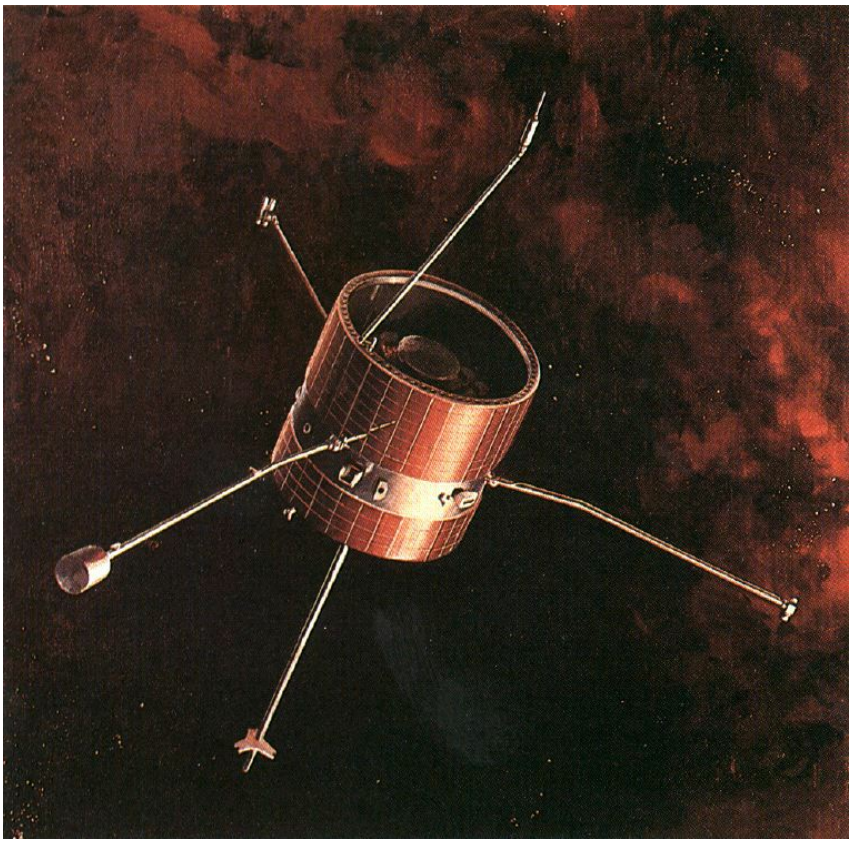

Figura 11: A sonda Pioneer 9. Fotografía NASA.

En 1967, Andrew Viterbi, que simultaneaba o seu traballo de profesor na Universidade de California en Los Angeles co de investigador nos JPL, publicou un arquifamoso método de descodificación secuencial que aínda se emprega. Ao igual que a de Fano, a familia de Viterbi emigrara en 1939 dende Italia fuxindo de Mussolini. Para aqueles dos meus colegas investigadores que renegan da docencia, a historia do algoritmo de Viterbi é un aldabonazo; Viterbi concibiuno buscando unha forma de explicar aos seus alumnos os principios da descodificación secuencial:

"*Comecei seguindo o que se fixera e explicándoo. Esa foi unha grande experiencia de aprendizaxe, e foi aí cando desenvolvín o chamado algoritmo de Viterbi para códigos convolucionais. Chegou a partir da miña docencia. Estaba ensinando unha cousa que resultaba bastante difícil, e particularmente difícil de ensinar. Cando un investiga entra nun estado mental no que se converte en algo secundario, pero chegado o momento de explicarllo a alguén é cando se fai patente se un o entende de verdade. A teoría da información parecíame difícil de explicar, así que comecei a desenvolver algunhas ferramentas. Este algoritmo vén de aí*".

Figura 12: Andrew Viterbi en 2007. Fotografía: Alberto D'Ottavi, Creative commons 2.0.

Viterbi inventara un algoritmo que logo se demostrou era óptimo e que, se a memoria do codificador non era moi grande, se podía implementar cos circuítos dispoñibles na época. De feito, a NASA elixiu para as sondas Voyager un codificador convolucional máis sinxelo que o da Pioneer 9, de tal forma que a descodificación se puidese realizar empregando o algoritmo de Viterbi.

En 1971, nun *workshop* sobre teoría da comunicación celebrado en Florida, Ned Weldon pronunciou a que se acabou coñecendo como a conferencia de "a codificación está morta". A esa visión pesimista que, ao cabo, resultou equivocada, contribuíu sen dúbida o feito de que para entón moitos dos grandes nomes da codificación de canle no MIT abandonaran este tema de investigación. Un dos que seguían ao pé do canón, Irwin Jacobs, que se trasladara a California e con Viterbi fundara unha empresa chamada Linkabit, respondeu tras a intervención de Weldon mostrando á audiencia un circuíto integrado feito á medida e exclamando: "este é o futuro da codificación!". Vaia se era o futuro! En 1985 Viterbi e Jacobs abandonaron Linkabit e fundaron a empresa Qualcomm, que deseña circuítos integrados para comunicacións, cotiza no Nasdaq, ten 31.000 empregados e unha facturación en 2013 de 25.000 millóns de dólares.

Figura 13: Irwin Jacobs en 2005. Fotografía Dan Anderson.

En todo caso, é certo que a principios dos 70 os avances en codificación atravesaban un período de estancamento. Podemos preguntarnos que lonxe se estaba da capacidade de Shannon en 1973, transcorridos 25 anos do seu revolucionario artigo. Neste punto é importante sinalar a existencia de dous réximes distintos derivados do ancho de banda dispoñible. O caso das comunicacións de espazo profundo coñécese como "limitado en potencia", porque o ancho de banda é virtualmente ilimitado, pero a enerxía consumida se traduce nunha menor vida útil da batería de abordo. En moitos outros casos, como na difusión de sinais de televisión, ou nas comunicacións móbiles, fálase de canles "limitadas en ancho de banda". As estratexias que se deben empregar fronte a limitacións en potencia ou en ancho de banda difiren considerablemente; como vimos, o interese polas comunicacións coas sondas espaciais fixo que a meirande parte da investigación se dirixise inicialmente ás canles limitadas en potencia.

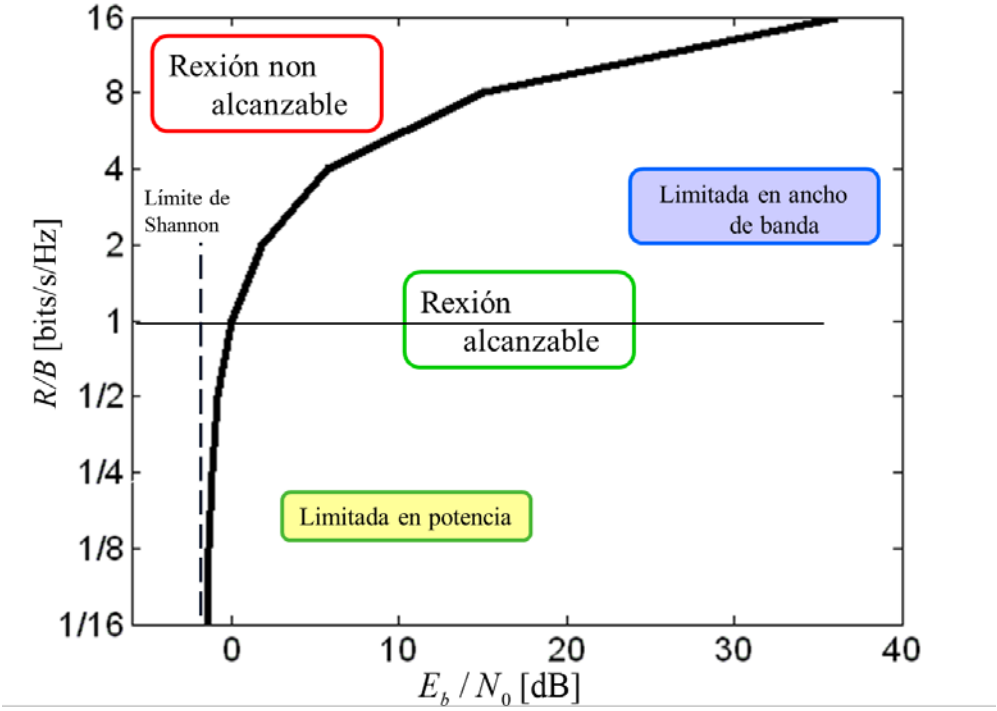

Figura 14: Réximes limitados en potencia e ancho de banda e a fronteira da capacidade.

Para medir a que distancia se estaba do límite de Shannon pódese utilizar a enerxía por bit, isto é cantos xulios custa poñer un bit de información (non de redundancia) para que se reciba no receptor cunha probabilidade de erro baixa (xeralmente, adóptase a regra de 1 bit erróneo cada 100.000 transmitidos). Normalmente, a distancia mídese nesa unidade que tanto nos gusta aos enxeñeiros: o decibelio. Pois ben, se non se emprega codificación de canle, a distancia ao límite de Shannon[4] é de 11,2 decibelios. Como podemos interpretar esta cantidade? Como en unidades naturais é 13,2, isto quere dicir que se alcanzásemos a capacidade de canle poderiamos reducir a enerxía necesaria para enviar cada bit de información en máis de 13 veces ou, posto doutro modo, para transmitir a mesma cantidade de información, a batería podería durar 13 veces máis.

[4]Para o caso en que a eficiencia espectral se vai asintoticamente a 0. Os 11,2 decibelios son, polo tanto, un límite ideal alcanzable cando o ancho de banda tende a infinito, ou cando a información transmitida tende a cero. En canles limitadas en ancho de banda, a distancia co límite de Shannon mídese fixando a eficiencia espectral.

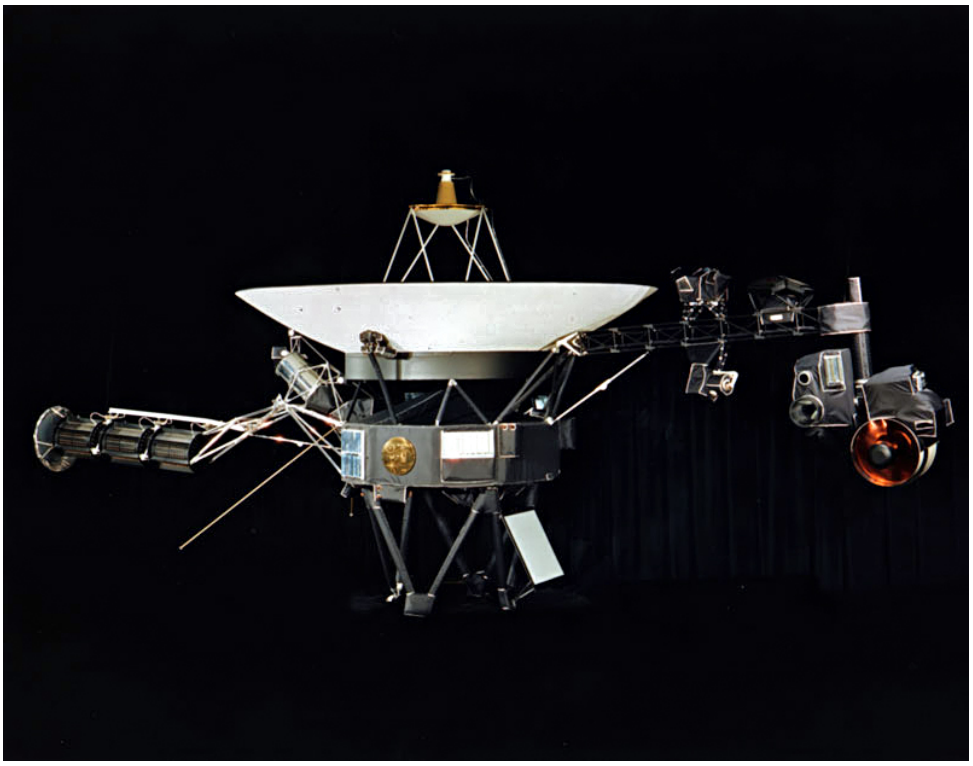

Figura 15: A sonda espacial Voyager 1. Fotografía NASA.

Nos anos 60 dicíase que cada decibelio gañado producía un aforro de 1 millón de dólares no custo do equipamento necesario para transmitir e recibir. O código das Mariner gañaba 2,2 decibelios e o da Pioneer 9, 3,3 decibelios. Gañar 3 decibelios supoñía reducir a aproximadamente a metade a enerxía necesaria e que a misión puidese viaxar decenas de millóns de quilómetros máis. O emprego dun código convolucional co descodificador de Viterbi supoñía unha gañancia duns 6 decibelios; en realidade, as Voyager beneficiáronse dunha idea adicional de Forney que consistía en "concatenar" dous códigos, un bloque e outro convolucional, para que o primeiro corrixise os erros remanentes do descodificador de Viterbi. Con este descodificador, a gañancia eran uns asombrosos 7,3 decibelios, malia que aínda quedaban 3,9 ata o límite de Shannon para canles limitadas en potencia e uns 2,5 considerando a canle limitada en ancho de banda.

Figura 16: Modem telefónico a 14400 bits por segundo. Fotografía: W.R. de Carvalho Machado, Creative Commons 3.0

Como vimos, ata principios dos 80 practicamente toda a investigación en codificación se centrara en como aforrar potencia con velocidades binarias relativamente baixas. Unha razón para iso é que ninguén dera con códigos que producisen gañancias aceptables para canles limitadas en ancho de banda. A partir de finais dos anos 60 había un interese crecente polos chamados "módems" para transmitir e recibir información sobre a liña telefónica. Ata que comezaron a popularizarse os módems ADSL, os módems telefónicos eran a única forma de conectarmos a Internet dende casa. A canle telefónica tiña unha forte limitación en ancho de banda, xa que dispoñía soamente duns 3,1 quilohercios. Empregando técnicas similares ás utilizadas en comunicacións de espazo profundo, as velocidades binarias alcanzables eran tan baixas que hoxe nos farían sorrir—aos meus fillos, rosmar—. Por exemplo, a mediados dos 80 os módems estándar permitían unha conexión a un máximo de 1.200 bits por segundo. Nas sondas, o xeito máis sinxelo de aumentar a velocidade era utilizar un maior ancho de banda, pero na canle telefónica isto era fisicamente imposible[5]. O único modo de incrementar a velocidade era aumentar o número de niveis de amplitude posibles nos sinais transmitidos, posto que ata entón só se empregaban dous niveis (correspondentes aos valores binarios 0 e 1). Parecía sinxelo, pero non o era: ao

[5]Polos filtros aplicados na central telefónica, adaptados ao sinal de voz. Prescindindo destes filtros, como fai ADSL, poderíanse alcanzar anchos de banda moi superiores.

aumentar o número de niveis, estes podían confundirse máis doadamente a causa do ruído. Xa o dixera Shannon…

E entón, en 1982, un enxeñeiro austríaco traballando para IBM en Zürich, Gottfried Ungerboeck, publicou unha idea xenial, dunha sinxeleza insultante, que permitía combinar os códigos convolucionais coa utilización de moitos niveis de amplitude. Os códigos resultantes, denominados "códigos en reixa" convertéronse no ingrediente fundamental para todos os módems telefónicos que viñeron despois. Non sería a última vez que un investigador da periferia desfaría o nó gordiano. Ungerboeck explicábao así:

"*...mais eu non estaba dentro, así que os meus pensamentos non estaban contaminados polo que estes tipos fixeran. Eles quedaron atascados na codificación alxébrica. Quero dicir que tiñan cousas marabillosas, pero con certa estreiteza de miras.* "

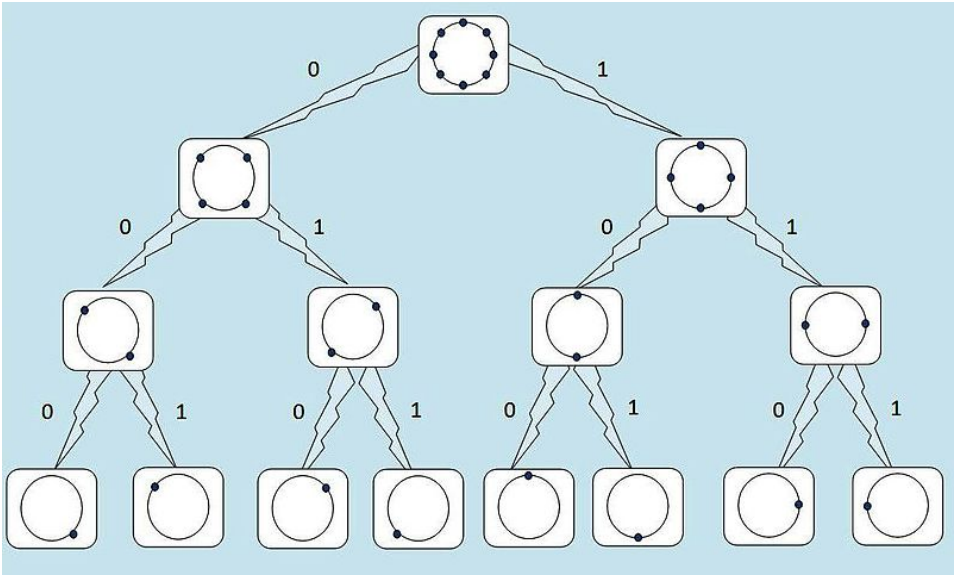

Figura 17: O esquema de particións sistemáticas sucesivas que forma o núcleo da idea de Ungerboeck. Creative commons 3.0.

A idea de Ungerboeck permitiu aos módems telefónicos multiplicar por 4 a velocidade ata 9,6 quilobits por segundo usando 8 niveis de amplitude. Combinando os niveis de varias transmisións sucesivas nun vector definido sobre o que denominamos "constelación multidimensional", e usando unha técnica adicional coñecida como "moldeado" para que os elementos da constelación se distribúan de forma uniforme sobre unha esfera (de catro dimensións), a codificación en reixa posibilitou chegar a finais dos anos 90 transmitir a 33.600 bits por segundo sobre o

par de fíos de cobre telefónico. Os codificadores da época conseguían unha gañancia de 4,52 decibelios, o que parece modesto comparado coas obtidas polos códigos empregados nas sondas espaciais, pero hai que pensar que as gañancias dos codificadores en reixa non se facían a custa de ningún aumento de ancho de banda. De feito, antes de Ungerboeck moitos pensaban que non era posible conseguir gañancia ningunha sen incrementar o ancho de banda. Aínda que os módems telefónicos apenas sobreviven nalgúns hoteis caducos, as ideas de Ungerboeck seguen vixentes nos módems ADSL, onde a limitación en ancho de banda segue presente.

En 1993, cando menos ninguén llo esperaba, chegou a sorpresa maiúscula. Dous franceses, Berrou e Glavieux, presentaban no congreso internacional de referencia un novo tipo de códigos, que bautizaron como "códigos turbo" e que, supostamente, se achegaban a menos de 1 decibelio do límite de Shannon. Nunha comunidade tan pechada como a de codificación de canle, onde calquera avance precisaba cada vez máis de profundos coñecementos alxébricos, Berrou e Glavieux eran uns completos descoñecidos sen tan sequera un doutorado. Como me confesaba Sergio Benedetto, un dos investigadores que máis fixo por axudar a entender os códigos turbo:

"*Ninguén os creu; todos estabamos seguros de que cometeran un erro nos cálculos. Pero cando regresamos á casa, cada un pediu aos seus doutorandos que repetisen as simulacións. E alí estaba. Tiñan razón!* "

A contribución clave de Berrou e Glavieux non estaba tanto na codificación coma na descodificación. Poderiamos dicir que ata entón os códigos concatenados se descodificaban por orde: primeiro, o chamado código interno; despois o externo, e aí remataba o proceso. Salvo algúns casos de escasa relevancia, a ninguén se lle ocorrera antes volver repetir a descodificación do código interno e así iterar o bucle unhas cantas veces. O concepto, aínda que sinxelo, non era trivial. En primeiro lugar, para poder regresar ao principio do bucle, era necesario retroalimentar ao primeiro descodificador non só os bits descodificados polo segundo, senón información da "fiabilidade" (poderiamos dicir, a "credibilidade") de cada bit. O algoritmo de Viterbi non serve para tal propósito, pero Glavieux e Berrou rescataron un algoritmo denominado BCJR (o acrónimo correspóndese coas letras dos seus inventores) publicado en 1974 e do que non se coñecía ningunha utilidade práctica. En segundo lugar, era necesario utilizar un tipo particular de codificadores convolucionais chamados recursivos e, especialmente, un elemento denominado "barallador" que desordena os bits de entrada. O barallador é aleatorio (mellor dito,

pseudoaleatorio[6]) e ten unha lonxitude de miles de bits, de modo que as palabras código que efectivamente utiliza un turbo código teñen dúas propiedades: 1) son dunha lonxitude enorme; 2) teñen aparencia aleatoria. Estas eran precisamente as dúas propiedades que tiñan os códigos que Shannon empregara na súa demostración; a diferenza era que por vez primeira alguén era capaz de construír un método práctico para xerar as devanditas palabras código e descodificalas de xeito eficiente. O propio código orixinalmente proposto por Berrou e Glavieux achegábase a só 0,5 decibelios do límite de Shannon. O teléfono móbil que vostedes levan consigo emprega códigos turbo para corrixir erros na transmisión da información.

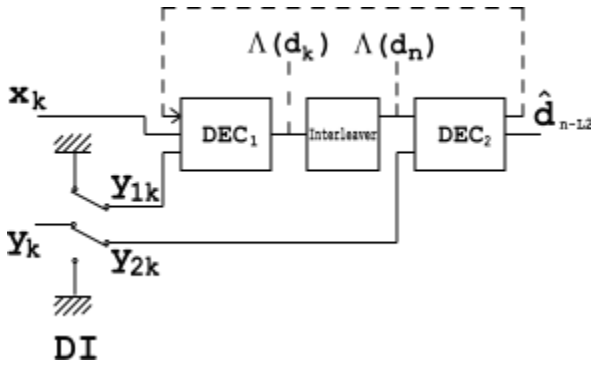

Figura 18: Diagrama de bloques de un turbo descodificador, coa realimentación do segundo descodificador ao primeiro en liña descontinua. Autor: Anton Petrov, Creative commons 3.0

A invención dos códigos turbo foi unha bafarada de aire fresco. Deseguida, os investigadores se decataron de que o mesmo principio de descodificación iterativa con paso de información de "fiabilidade" se podía usar para a descodificación duns códigos que foran propostos por Gallager no MIT na súa tese doutoral, nada menos que en 1960, e que foran descartados entón por imprácticos. Coñécense como "códigos de comprobación de paridade de baixa densidade" (xeralmente, denomínanse co seu acrónimo en inglés, LDPC) e son códigos bloque moi longos nos que a redundancia se xera de forma pseudoaleatoria. Ao mesmo tempo que se progresaba no deseño destes códigos, fóronse producindo avances moi importantes na comprensión dos algoritmos que se empregan na súa descodificación e na dos códigos turbo, que se poden formular baixo un paradigma coñecido como "propagación da convicción" para o que hai moitas outras aplicacións. Os códigos LDPC empréganse en numerosos estándares modernos de comunicacións, para

[6]Un barallador pseudoaletorio desordena os bits nun modo que parece aleatorio pero que en realidade responde a un algoritmo determinista e, polo tanto, repetible no outro extremo.

difusión de televisión vía satélite (DVB-S2) ou terrestre (DVB-T2), nas redes WiFi (IEEE 802.11 n) ou en redes Ethernet a 10 Xigabits por segundo.

Chung, Forney, Richardson e Urbanke publicaron en febreiro de 2001 un código LDPC que se encontraba a só 0,040 decibelios do límite de Shannon. Ese mesmo mes falecía Shannon, devastado polo Alzheimer nos seus últimos anos, incapaz de sorrir vendo que, por fin, 50 anos despois, a súa adiviña fora resolta. Como adoita acontecer coas grandes ideas, o teorema de Shannon non é senón un tronco do que xermolaron centos de pólas, porque centos eran as situacións que requirían novos desenvolvementos teóricos. A codificación conxunta de fonte e canle; as canles de acceso múltiple; as canles de difusión; as canles con multitraxecto; as redes gráficas; as redes con repetidores, e un longo etcétera, son algunhas das frondosas ramas que manteñen ocupados a numerosos investigadores teóricos e aplicados.

III

Permítanme que discorra por unha desas pólas para contar a miña relación coa codificación de canle. Moitos de vostedes coñecerán a teoría dos seis graos de separación, mesmo pode que recorden a película. No meu caso, seis son precisamente os graos académicos que me separan dos pioneiros da codificación: Fano, de quen antes falei, dirixiu a tese a Desoer, quen dirixiu a tese a Newcomb, quen dirixiu a tese a Kamen, quen dirixiu a tese a Lewis, quen dirixiu a tese a Abdallah, quen foi o meu director de tese. Curiosamente, con Desoer produciuse a mutación que levou aos seus descendentes, un servidor incluído, a centrar as súas teses na teoría dos sistemas lineais e o control automático. Así que, en realidade, debo o meu interese pola codificación de canle á empresa Televés, que a principios dos anos 90 comezou a traballar na entón incipiente televisión dixital por satélite e que, grazas á visión e ousadía do seu director de I+D, José Luis Fernández Carnero, confiou nun grupo de entón mozotes da Universidade de Vigo para que os acompañase nunha longa e frutífera colaboración que segue viva tras máis de vinte anos.

Unha etapa particularmente memorable dese camiño consistiu no deseño dun sistema de acceso condicional para a distribución de sinais de televisión dixital. Os de "pay-per-view" son o exemplo mellor coñecido de sistemas de acceso condicional. En 1995, como parte do proxecto, buscabamos unha forma de cifrar os sinais dixitais de modo que se puidese intuír o contido, permitindo o acceso completo só a aqueles usuarios que dispuxeran das credenciais axeitadas. Un dos membros do meu equipo, Sergio Cruces, agora profesor na Universidade de Sevilla, chegou un día falando dunha tecnoloxía denominada "esteganografía" que era parte dunha disciplina máis ampla, entón completamente incipiente, chamada "marcado de auga dixital". Tan atractivo resultou ser o problema do marcado de auga que se acabou convertendo na miña liña de investigación máis fecunda.

O marcado de auga utilízase para embeber información en obxectos multimedia co requisito de que o resultado sexa indistinguible perceptualmente do orixinal. Son numerosas as súas aplicacións, pero a que entón actuaba como motriz era a protección do copyright dos DVD. En poucas palabras, trátase de embeber nos fotogramas unha marca invisible que dependa dun identificador único do soporte de almacenamento--o DVD--. O reprodutor le o identificador e a marca invisible e comproba se son conformes; en caso afirmativo, procede a reproducir o contido.

Para que a solución fose efectiva, a marca debía ser invisible, difícil de eliminar e fiable, é dicir, que a información extraída coincidise coa que fora embebida.

O que naqueles momentos facía o problema interesante era que tanto os métodos de inserción coma os de detección da marca eran puramente heurísticos, xeralmente baseados en intuicións provenientes da área do tratamento de imaxes. Non obstante, a miña visión, sesgada pola miña experiencia previa en codificación de canle, era radicalmente diferente: diante tiñamos un problema de comunicacións, no que a información a enviar (os bits da marca de auga), se transmitía sobre unha canle (os fotogramas de vídeo) para ser recuperada no reprodutor de DVD. Dende esta perspectiva, se queriamos aumentar a fiabilidade dos bits extraídos no reprodutor, só tiñamos que empregar codificación de canle. Aproveitei unha viaxe a San Francisco en verán de 1996 para propoñer a idea como tese ao meu ex alumno Juan Ramón Hernández, que por aquel entón cursaba un máster en Stanford. Ao seu regreso a Vigo, comezamos a traballar co frenesí de quen encontrou un filón, porque case todos os métodos de codificación coñecidos funcionaban. De feito, coa codificación de canle podiamos achegarnos tamén ao límite da capacidade para este problema. Ou iso criamos…

A finais de 1998, mentres preparabamos un artigo con algúns dos nosos achados, decatámonos de que algo non encaixaba: con algunhas modificacións sinxelas no codificador era posible ir máis alá da capacidade de Shannon. Para entender a perplexidade en que estes resultados me sumiron, pódese pensar no experimento reportado polo CERN en 2011 no que os neutrinos parecían moverse a unha velocidade maior que a da luz. Afortunadamente, naquel caso, novas medidas realizadas en 2012 permitiron concluír a existencia dun erro nas primeiras. Non obstante, aquí todo parecía ser correcto. Pasei o verán de 1999 intentando descifrar o enigma mentres lía o meu fillo por enésima vez o conto de *O barrio de Winnie the Pooh*. Souben despois que varios colegas pasamos aquel verán tratando independentemente de entender que acontecía, sen ser conscientes de que Chen e Wornell, dous investigadores do MIT--outra vez o MIT--, presentaran había poucos meses nunha conferencia unha explicación que, se ben non totalmente pechada, contiña as claves da solución. Aínda que Wornell era ben coñecido polas súas contribucións en comunicacións dixitais e tratamento de sinal, no campo do marcado de auga era un completo *outsider*, e polo tanto non estaba contaminado como nós. Cantas veces os avances en ciencia chegaron dende fóra? E a pesar diso ou quizais por iso, os círculos científicos seguen sendo tan pechados…

Ao longo de varios traballos, estes investigadores do MIT foron debullando a súa idea, que culminou coa publicación en 2001 dun artigo no que analizaban o seu método, que denominamos "marcado de auga baseado en cuantificación", dende o punto de vista da teoría da información. Así puidemos entender por que se podía ir

máis alá do límite da capacidade de Shannon; ata entón, trataramos o sinal hóspede, isto é, aquel no que se embebe a marca de auga, como ruído. Pero había unha diferenza esencial: cando se embebe unha marca de auga dixital, o sinal hóspede é coñecido, mentres que cando se transmite información sobre a canle modelada por Shannon, o ruído é descoñecido para o transmisor. Entón, cal é a capacidade deste modelo de canle? Resultou que Max Costa, un brasileiro facendo a súa tese en Stanford, publicara en 1983 a solución ao problema e non tivera ningún eco, porque ninguén sabía entón para que podería servir ese tipo de canle. O artigo de Costa, rescatado por Chen e Wornell, titúlase *Escribindo en papel sucio*, unha gráfica metáfora que alude ao feito de que cando un escribe sobre un papel con manchas, como pode ver en que lugar se encontran estas, é capaz de adaptar a súa escritura para saltárseas. Tras este precioso título, aos códigos que se empregan neste tipo de canle chámaselles "códigos de papel sucio". Coa axuda dos meus estudantes Félix Balado, primeiro, e Pedro Comesaña, despois, traballei durante os seguintes anos na análise e o deseño de códigos de papel sucio que podían achegarse con certa facilidade á capacidade de Costa, aproveitando, por suposto, o que se sabía sobre como alcanzar a capacidade de Shannon.

A pesar de que a miña principal actividade investigadora discorre actualmente por camiños alleos á codificación de canle, de cando en vez seguimos botando man do aprendido, que remata en insospeitados produtos, como a aplicación de segunda pantalla que recentemente lanzou a TVG.

IV

Unha consecuencia do éxito case inmediato do artigo de Shannon foi a proliferación de traballos propugnando a aplicación da súa teoría aos campos máis dispares, a miúdo sen comprender os seus fundamentos matemáticos. Escandalizado, Shannon publicou en 1956 unha breve peza titulada *The bandwagon*, que podería traducirse por "subir ao carro". Dicía Shannon que os traballadores--non se atrevía a chamalos investigadores--noutras disciplinas "deberían decatarse de que os resultados básicos desta materia apuntan nunha dirección moi específica, unha dirección que non é necesariamente relevante en campos como a psicoloxía, a economía e outras ciencias sociais,". Por contraste, unha das áreas onde as ideas de Shannon parecen encontrar máis sentido é a bioloxía. A súa propia tese doutoral titúlase *Un álxebra para a Xenética Teórica*, aínda que nada ten que ver coa teoría que anos máis tarde o faría famoso. De feito, o "código da vida", o ADN, atraeu a atención de varios expertos en teoría da información, esporeados por outro enigma: por que a Natureza parece non saber de codificación de canle?

Dunha forma moi resumida, o ADN utiliza un alfabeto con catro bases (adenina, timina, citosina e guanina, A, C, T, G) que fan as veces do que en comunicacións denominamos símbolos. O xenoma ten dous tipos de porcións, chamadas intróns e exóns; as primeiras non conteñen información propiamente dita, mentres que os exóns conteñen a información que serve aos ribosomas das células para fabricar as proteínas como secuencias de aminoácidos. Estes aminoácidos codifícanse a partir de grupos de tres bases consecutivas que se denominan codóns. Con catro bases diferentes[7] e tres posicións poderíanse codificar ata 4 ^ 3 =64 diferentes aminoácidos; non obstante, na Natureza só se empregan 20 aminoácidos, máis un codón de stop, que se usa para finalizar a síntese da proteína. Durante o proceso de réplica do ADN ou debido a radiacións ou axentes químicos, poden acontecer erros denominados mutacións, que alteran a secuencia de bases.

[7]Mentres escribo estas liñas coñeceuse que uns investigadores en California conseguiron sintetizar unha bacteria viable cuxo ADN emprega 6 bases, dúas delas artificiais. Iso aumenta máis o misterio, porque as 64 combinacións tamén se poderían codificar con codóns de 2 bases consecutivas (2 ^ 6 =64).

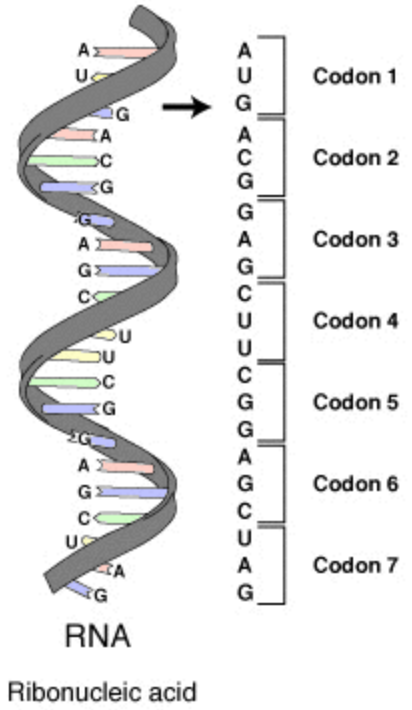

Figura 19: ARN amosando a estrutura en codóns (no ARN a timina do ADN, T, reemplazase por uracilo, U). Creative commons 3.0.

Meramente dende o punto de vista da codificación de canle, para evitar estes erros cabería pensar en usar só 21 das 64 posibles combinacións, de modo que as 43 restantes, por imposibles, servisen para detectar mutacións e "cancelar" o proceso de réplica. Non obstante, en realidade empréganse todas as 64 combinacións de 3 bases. O misterio do "código xenético" encóntrase na falta de lóxica--dende un punto de vista puramente de corrección de erros--da asignación de codóns a aminoácidos: mentres algúns aminoácidos se codifican con só unha das combinacións, outros pódense xerar a partir de 6 combinacións distintas. En codificación de canle, a falta de simetría, como de forma patente acontece neste caso, adoita ser garantía de que o código non é óptimo. En parte debido a esta asimetría, e en parte ao feito de que as mutacións son un feito relativamente frecuente que non obstante non se traduce nunha variabilidade tan grande, algúns autores postularon a existencia de códigos de corrección de erros no ADN. Por exemplo, Battail apunta á posibilidade de que os intróns conteñan a redundancia que permite corrixir erros; desgraciadamente, para corrixir erros sería necesario algún mecanismo computacional no proceso de réplica que non foi achado ata a data.

Standard genetic code

1st base	2nd base								3rd base
	U		C		A		G		
U	UUU	(Phe/F) Phenylalanine	UCU	(Ser/S) Serine	UAU	(Tyr/Y) Tyrosine	UGU	(Cys/C) Cysteine	U
	UUC		UCC		UAC		UGC		C
	UUA	(Leu/L) Leucine	UCA		UAA	Stop (*Ochre*)	UGA	Stop (*Opal*)	A
	UUG		UCG		UAG	Stop (*Amber*)	UGG	(Trp/W) Tryptophan	G
C	CUU		CCU	(Pro/P) Proline	CAU	(His/H) Histidine	CGU	(Arg/R) Arginine	U
	CUC		CCC		CAC		CGC		C
	CUA		CCA		CAA	(Gln/Q) Glutamine	CGA		A
	CUG		CCG		CAG		CGG		G
A	AUU	(Ile/I) Isoleucine	ACU	(Thr/T) Threonine	AAU	(Asn/N) Asparagine	AGU	(Ser/S) Serine	U
	AUC		ACC		AAC		AGC		C
	AUA		ACA		AAA	(Lys/K) Lysine	AGA	(Arg/R) Arginine	A
	AUG[A]	(Met/M) Methionine	ACG		AAG		AGG		G
G	GUU	(Val/V) Valine	GCU	(Ala/A) Alanine	GAU	(Asp/D) Aspartic acid	GGU	(Gly/G) Glycine	U
	GUC		GCC		GAC		GGC		C
	GUA		GCA		GAA	(Glu/E) Glutamic acid	GGA		A
	GUG		GCG		GAG		GGG		G

Figura 20: Táboa co código xenético. Fonte: Wikipedia.

Empregando argumentos de teoría da codificación, en particular o procedemento de particións sucesivas inventado por Ungerboeck, de quen antes falamos, si parece xustificarse un proceso polo que na vida primordial se tivesen empregado inicialmente codóns con só dúas bases, e máis tarde o código fose ampliado a codóns de tres bases para dar cabida a máis aminoácidos. Estes argumentos apoiarían as teorías que explican a evolución do código xenético como un proceso de expansión biosintética.

Outra importante consideración ten que ver coa optimalidade do código. En codificación de canle clásica sempre se busca que o número de erros sexa o menor posible; non obstante, un proceso sen erros estaría disputado coa evolución. Se se pensa no ADN como un mecanismo de exploración do espazo biolóxico de posibilidades, a comisión de erros tamén ten vantaxes competitivas. É lóxico, polo tanto, que o código xenético, respondendo a funcións de utilidade diferentes, conduza a configuracións diferentes da codificación de canle clásica. Aínda que a solución ao misterio pasa necesariamente pola bioquímica e a xenética de poboacións, é un exercicio apaixonante e aberto empezar "polo outro extremo" e tratar de determinar que función de utilidade é a que optimizou o código xenético. De feito, un enfoque multidisciplinar que inclúa a teoría da codificación é, sen lugar a dúbidas, o camiño axeitado a tan esquivo e intrigante problema.

Conclúo xa. Gocei moito preparando este discurso, achegándome á historia dunha das materias que maiores éxitos proporcionaron á Enxeñaría de Telecomunicación, e por extensión á Humanidade, e comprendendo mellor o home que, mediante a súa adiviña, nos axudou a explorar o sistema solar. A cultura popular construíu lendas en torno aos "momentos eureka" que axudan a imaxinar o xenio en acción: a mazá de Newton, Arquímedes na súa bañeira, Poincaré a punto de subir ao ómnibus... cando a Shannon lle preguntaron polo seu momento eureka, o gran malabarista das infinitas dimensións respondeu: "posiblemente teríao tido de ter sabido deletrear a palabra".

Agradecementos

Agradezo a Félix Balado e Juan Ramón Troncoso ter compartido comigo as súa visións sobre o código xenético e orientar o meu mergullo na literatura existente. O Profesor Carlos Mosquera aportou tamén algunhas referencias bibliográficas de interese. Miña máis fonda gratitude aos todos os membros do Grupo de Procesado de Sinais en Comunicacións da Universidade de Vigo por axudarme a manter a cabeza nas nubes e aos traballadores do Centro Tecnolóxico de Telecomunicacións de Galicia (Gradiant) por ancorar os meus pes ao chan. E, sobre todo, a miña familia por aturarme así estirado.

Bibliografía

O. Aftab, P. Cheung, A. Kim, S. Thakkar, N. Yeddanapudi. Information theory and the digital revolution. Project history MIT 6:933, 2001.

F. Balado, *Digital Image Data Hiding Using Side Information*. Tese doutoral, Universidade de Vigo, 2003.

G. Battail, *Information Theory and Error-Correcting Codes in Genetics and Biological Evolution*, en M. Barbieri (ed.), Introduction to Biosemiotics, pp. 299–345. Springer Science+Business Media B.V. 2008.

G. Battail, Information and Life, Springer Science+Business Media Dordrecht 2014.

B. Chen e G. W. Wornell, *Quantization index modulation: a class of provably good methods for digital watermarking and information embedding*, IEEE Transactions on Information Theory 47 (4), pp. 1423–1443, 2001.

E. Chiu, J. Lin, B. McFerron, N. Petigara e S. Seshasai, *A Mathematical Theory of Claude Shannon -- A study of the style and context of his work up to the genesis of information theory*, Final project paper for course “The structure of engineering revolutions”, MIT, Outono 2001.

H.W. Chung, M. Karzand, J. Sun, D. Wang, *Interview with David Forney*, MIT, Xuño 2013. http://www.mit.edu/~dawang/materials/forney_interview_20130605.pdf

A.C. Clarke, *Voice Across the Sea*, HarperCollins, 1975.

P. Comesaña, *Side-informed data hiding: robustness and security analysis*. Tese doutoral, Universidade de Vigo, 2006.

M. Costa, *Writing on dirty paper.* IEEE Trans. Information Theory 29 (3), pp. 439–441, Maio 1983.

D.J. Costello Jr. e G.D. Forney, *Channel Coding: The Road to Channel Capacity*, Proceedings of the IEEE 95 (6), Xuño 2007.

D.J. Costello Jr., J. Hagenauer, Fellow, H. Imai e S.B. Wicker, Applications of Error-Control Coding, IEEE Trans. On Information Theory, 44 (6), pp. 2531-2560, Outubro 1998.

Z. Dawy, P. Hanus, J. Weindl, J. Dingel, F. Morcos, *On Genomic Coding Theory*, Eur. Trans. Telecomm. 18, pp. 873–879, 2007.

L.C.B. Faria, A.S.L. Rocha, J.H. Kleinschmidt, M.C. Silva-Filho, E. Bim, R.H. Herai, M.E.B. Yamagishi, R. Palazzo Jr., *Is a Genome a Codeword of an Error-Correcting Code?*, PLOS ONE, 7 (5), Maio 2012.

J. Gleick, *The Information: A History, a Theory, a Flood*, Pantheon Books, 2011.

A. Goldstein, *Oral-History: Interview with David G. Forney*, IEEE Global History Network, Interview #254 for the Center for the History of Electrical Engineering, IEEE, 1995.

A. Goldstein, *Oral-History: Interview with Robert Gallager*, IEEE Global History Network, Interview #156 for the Center for the History of Electrical Engineering, IEEE, 1993.

E.M. Guizzo, *The Essential Message: Claude Shannon and the Making of Information Theory*, MS Thesis, MIT, 2003.

E.M. Guizzo, *Closing in on the perfect code*, IEEE Spectrum 41 (3), pp. 36-42, Marzo 2004.

J.R. Hernández Martín, *Técnicas de sellado invisible para la protección de los derechos de autor de imágenes digitales.* Tese doutoral, Universidade de Vigo, 1998.

J. Horgan, *Claude E. Shannon*. IEEE Spectrum 29 (4), pp. 72-75, Abril 1992.

R. Ludwig e J. Taylor, *Voyager Telecommunications*, DESCANSO Design and Performance Summary Series, JPL-NASA, Marzo 2002.

J.L. Massey, *Deep-Space Communications and Coding: A Marriage Made in Heaven*, en J. Hagenauer (ed.), Advanced Methods for Satellite and Deep Space Communications, pp. 1-17. Lecture Notes in Control and Information Sciences 182. Heidelberg and New York: Springer,
1992.

D. Morton, *Oral-History: Interview with Andrew J. Viterbi*, IEEE Global History Network, Interview #377 for the Center for the History of Electrical Engineering, IEEE, 1999.

NASA, *Páxina web da Misión Voyager*, http://voyager.jpl.nasa.gov/

F. Nebeker, *Oral-History: Interview with Gottfried Ungerboeck*, IEEE Global History Network, Interview #445 for the Center for the History of Electrical Engineering, IEEE, 2004.

T.S. Perry, Irwin Jacobs: Captain of CDMA, IEEE Spectrum 50 (5),pp. 52-55, Maio 2013.

R. Price. *Oral-History: Interview with Claude Shannon*, IEEE Global History Network, Interview #423 for the Center for the History of Electrical Engineering, IEEE, 1982.

R. Price. *A Conversation with Claude Shannon*. IEEE Communications Magazine, 22 (5), pp. 123–26, 1984.

C.E. Shannon, *A Mathematical Theory of Communication*. Bell System Technical Journal, vol. 27, pp. 379–423, 1948.

C.E. Shannon, *The Bandwagon*. IRE Transactions Information Theory, 2 (1), p. 3, 1956.

S. Verdú, *A Conversation with Robert Fano*. IEEE Information Theory Society Newsletter, pp. 6-9, Setembro 2013.

M.M. Waldrop, *Claude Shannon: Reluctant Father of the Digital Age*, MIT Technology Review, pp. 64-71, 2001.