El binomio Matemáticas- Técnicas de transmisión de la información: 60 años de una sinergia exitosa

Luis Muñoz
Dept. de Ingeniería de Comunicaciones
ETSII Telecomunicación
Universidad de Cantabria

luis@tlmat.unican.es

- Comentarios sobre el título
  - Matemáticas ≠ Los matemáticos
  - Técnica ≠ Ingenieros
- Lo importante es cómo se piensa y no el título
  - El rigor intelectual no está reñido con la intuición
- TELECOMAT, personas confortables en ambos lados
- Colaboración fructífera en ambos sentidos

⇓

Simbiosis

- Simbiosis: Cojo a hombros de ciego
  - Ciego ≠ Ingeniero, Cojo ≠ Matemático
  - Tanto monta, monta tanto …
- Refrán español: "Más vale maña que fuerza"
- ¿Cuándo se acuñó?
  - Exponente de ello en el mundo griego:
    - Arquímedes
    - Estática
  - "Dadme un punto de apoyo y moveré el mundo".

- Otro ejemplo: Claude Shannon

- Doble titulación: Ingeniero Eléctrico, Matemáticas
  - Máster MIT: Ingeniería Eléctrica
  - Doctorado MIT: Matemáticas

- Bell Labs: "A Mathematical theory of communication" (1948), 32 años

- "…No conozco ningún ejemplo de un avance matemático de importancia desarrollado por una persona que haya superado los 50. La matemática es asunto de jóvenes" (G.H. Hardy, "Apología de un matemático").

- Críticas: Matemáticos no lo aceptaban
  - *"The discussion is suggestive throughout, rather than mathematical and it is not always clear that the author's mathematical intentions are honorable".* J. Doob; Gran teórico del cálculo de probabilidades.

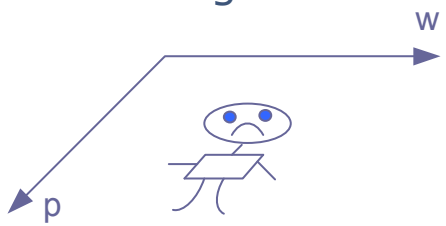
- Su homólogo ruso: A. Kolmogorov

  "Shannon's mathematical intuition was amazingly precise. He can be ranked as both of the leading mathematicians and one of the leading engineers of this time".

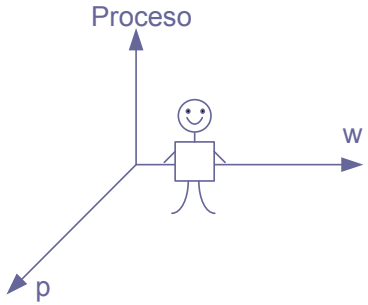
- Críticas: Los ingenieros lo consideran una curiosidad matemática
- Cambio radical en la forma de pensar en conflicto con la intuición
- El transmisor juega un papel tan importante como el receptor en la supresión del ruido
- El ruido en el canal limita la velocidad de transmisión pero no la tasa de error alcanzable

RESUMIENDO

- Antes de 1948, los recursos del ingeniero eran dos:
  - Ancho de banda, y potencia
  - Mundo de "dos dimensiones"



- A partir de 1948, hay recursos de dos tipos:
  - Físicos: Fuerza (P,W)
  - "Neuronales": Maña, proceso



- Cambio del título: "*The Mathematical theory of communication*" (1949)

- Eco incluso en una canción:

"As time goes by"

inolvidable película, "Casablanca"

This day and age we´re living in
Gives cause for apprehension
With speed and new inventions
And things like **third Dimension**
Yet we get a trifle weary
with Mr. **Einstein's (Shannon???) Theory**

Volvamos a Shannon

- Demostración matemática indirecta, no constructiva

- Desilusión entre los ingenieros
  - Injustificada:
    Ninguna teoría fundamental tiene como objetivo construir nada

- Cota fundamental con la que comparar sistemas reales. Ideal hacia el que llegar

  "We venture to say that 19.2 Kbps is the maximum conceivable rate, even with all-out use of the most powerful coded modulation"

  (D. Forney, R. Gallager, 1948)

- *"Why would voice and images be transmitted digitally? Doesn't digital transmission squander bandwidth? A voice modem cost ten times as much as a telephone, and is incapable of transmitting voice signal with quality comparable to an ordinary telephone"*

  (Lee Messerschmitt, "Digital Communications", 1ª edición, 1988)

- "Not so long ago, digital transmission of voice and video was considered wasteful of bandwidth, and the cost of concern. More recently, there has been a complete turnabout of thinking … "

  (idem, 2ª Edición 1994)

- Shannon es un visionario: Indica el camino

  Qué se puede hacer

  No dice cómo (algorítmica)

  Ni mucho menos, con qué (dispositivos electrónicos)
- No existían circuitos integrados.
- El transistor se inventó en 1948.
- Curiosamente: Mismo año y mismo lugar (Bell)
- Esas dificultades tecnológicas explican (justifican) el retraso del mundo real respecto al conceptual.
- Un ejemplo:

  Primera implementación PCM: EEUU, 1962

  Patente francesa (ITT, Reeves) en 1939

- Progreso muy lento.
- Carencias teóricas, no sólo tecnológicas.
- Razón fundamental:

  La demostración indirecta de Shannon

  Estudio del comportamiento, en media, de todos los codificadores
- Escoger codificadores aleatoriamente y de longitud grande está bien para demostrar teoremas, no para traducir mensajes.
- El teorema de existencia es sin embargo útil: Hay una aguja en el pajar. Encontrarla es otro asunto.
- Había una firme determinación en llegar a saber cómo hacer lo que se puede hacer.

  Comparable a:

  "*Wir müssen wissen, wir werden wissen*" (D. Hilbert)

- El primer invento vino de inmediato: Hamming (1948)

  Corregir 1 error en bloques de 2^m-1 bits. (m: parámetro)

  Sacrificar alguno (r=m) de los 2^m-1 para indicar la posición del error

- ¿Corregir t > 1 en bloques de 2^m-1 bits?

  Sacrificar r > m

  ¿Cuántos? y ¿Cómo seleccionar las filas binarias a añadir a la matriz de comprobación?

- Los matemáticos ignoraban el tema.
- Todo estaba en manos de los ingenieros → ¡Impasse!
- 10 años de estancamiento.

- Bose-Chaudhuri: 1960
- Cuerpos de Galois: GF(2^m)

  No añadan filas binarias una a una! Sino m a m!

  Así, la solución es obvia!

  A la pregunta: ¿Cómo decodificarían?

  Respondieron: ¿Qué es decodificar?
- Álgebra moderna ya había entrado antes en el tema.
- D. Slepian

  Tabla de Slepian = Visualización gráfica del teorema de D'Alembert.
- Con Bose-Chaudhuri, entra de lleno.
- En álgebra moderna había una aplicación DE VERDAD!

- "…La mayor parte de las matemáticas superiores son inútiles. El álgebra moderna, la teoría de números no pasarían la prueba de la utilidad…" (G.H Hardy)

- Contribución de Bose-Chaudhuri

  Un buen ejemplo del origen aplicado de las matemáticas, muy frecuente antaño, pero no tan usual en nuestros días

- Una vez abierta la puerta:
  - Ecuaciones algebraicas en GF(2^m) cuyas raíces localizan los errores.
  - Polinomios mínimos de elementos del cuerpo para obtener los polinomios generadores.

- Año 1960: Doble (triple!) Big-Bang
- Aparecen también los códigos Reed-Solomon.

  Muy ubicuos: Sondas, NASA, CD, DVD, DVB, ..

  Símbolos: elementos de GF(2^m), no bits.

  r mínima para *t* dada

  Algoritmo de decodificación muy eficiente E. Berlekamp, 1968.
- Polinomio generador del código: Producto de *r* polinomios.

  Raíces del polinomio generador: Como potencias de un elemento generador del cuerpo, tiene exponentes consecutivos.
- Ingenieros cada vez más aturdidos!

- Una vez producido el alumbramiento, las contribuciones de los ingenieros son fundamentales.
  - ¿Con qué polinomios irreducibles se construye GF(2^m)?
    Irrelevante(?): ¡Todos los GF(2^m) son isomorfos!
    ¡Dígaselo a mis baterías!
  - ¿En qué potencia se empieza para construir el polinomio generador del codificador Reed-Solomon?
    Irrelevante(?): Todos los códigos son equivalentes.
    Implementación: Memorias ROM.
  - ¿Cómo se puede aprovechar el que (digamos) el demodulador me indique la baja fiabilidad de una de sus decisiones?

- Es improbable que estas preguntas se las plantease alguien sin formación técnica.

- En 1960 hubo también otro alumbramiento importante

- Códigos con matriz de comprobación de baja densidad. (Low Density Parity Check Codes ≈LDPCC)

  Tesis de Doctorado de R. Gallager: MIT

  Máster: MIT, 1956

  El lugar era el apropiado: hegemonía total del MIT

  - Estructura: Regularidad estadística de los grandes números
    Conjunto concreto de matrices aleatorias de Gallager tienen excelentes propiedades estadísticas
  - El receptor decodifica con un algoritmo iterativo probabilista, que diseña

- Es improbable que la idea de los LDPCC se le hubiese ocurrido a un matemático.
- Planteado matemáticamente el algoritmo de decodificación: Interpretable como paso de información entre nodos de un grafo bipartito.
- Ejecución del algoritmo de forma paralela.
- Muy conveniente con números grandes, 6400 bits, con un número de condiciones de comprobación elevado (entre 6000 y 48000, aprox.)
- Área interesante y activa de trabajo: Estructura del grafo, condiciones de convergencia (rápida), etc.
- ¿Qué pasó con los códigos LDPCC?

- Gallager ni los menciona (en su libro "Information theory and reliable communication", 1968)

- Peterson-Weldon (Error correcting codes, 1972)

  "…Low density codes do not appear to be as attractive for use in practical systems as do some of the other (algebraic) codes presented in this book. However, the decoding algorithms proposed for these codes have provided the basis for much work…".

  (Se refiere a la decodificación por mayoría, J. Massey, 1963).

- Sentimiento de Gallager con su tesis

  El mayoritario: olvido

- Pero algunas tesis tienen mucho eco:
  - Inmediato
    - Louis de Broglie

    (Tesis: 1925, Nobel: 1929)
  - Tardío
    - J. Nash

    (Tesis: 1950, Nobel 1994)
    - M. Tomlimson

    (Tesis: 1970, TCM: 1984)
    - R. Gallager

    (Tesis: 1960, resurrección: 1993)

- Renacimiento del interés por la decodificación probabilística y los LDPCC debida a la intervención de los Turbo-Códigos (Berrou-Glavieux, 1993)
- Improbable que este esquema se le hubiera ocurrido a alguien sin formación técnica:
  - Realimentación entre los dos decodificadores
  - Estabilidad: Lleva al concepto de información extrínseca.
- Fue recibido por los ingenieros con escepticismo, sólo había pruebas experimentales.
- Finalmente se impuso: 1998, premio al mejor artículo (IEEE Information Theory).
- Contemplado en el estándar UMTS (ETSI).

- Otro invento difícil de concebir sin formación técnica.
- Hay que entender claramente los conceptos de ancho de banda, velocidad de modulación, velocidad de transmisión, eficiencia espectral.
- Conceptos familiares a los especialistas en transmisión, no así a otros colectivos.

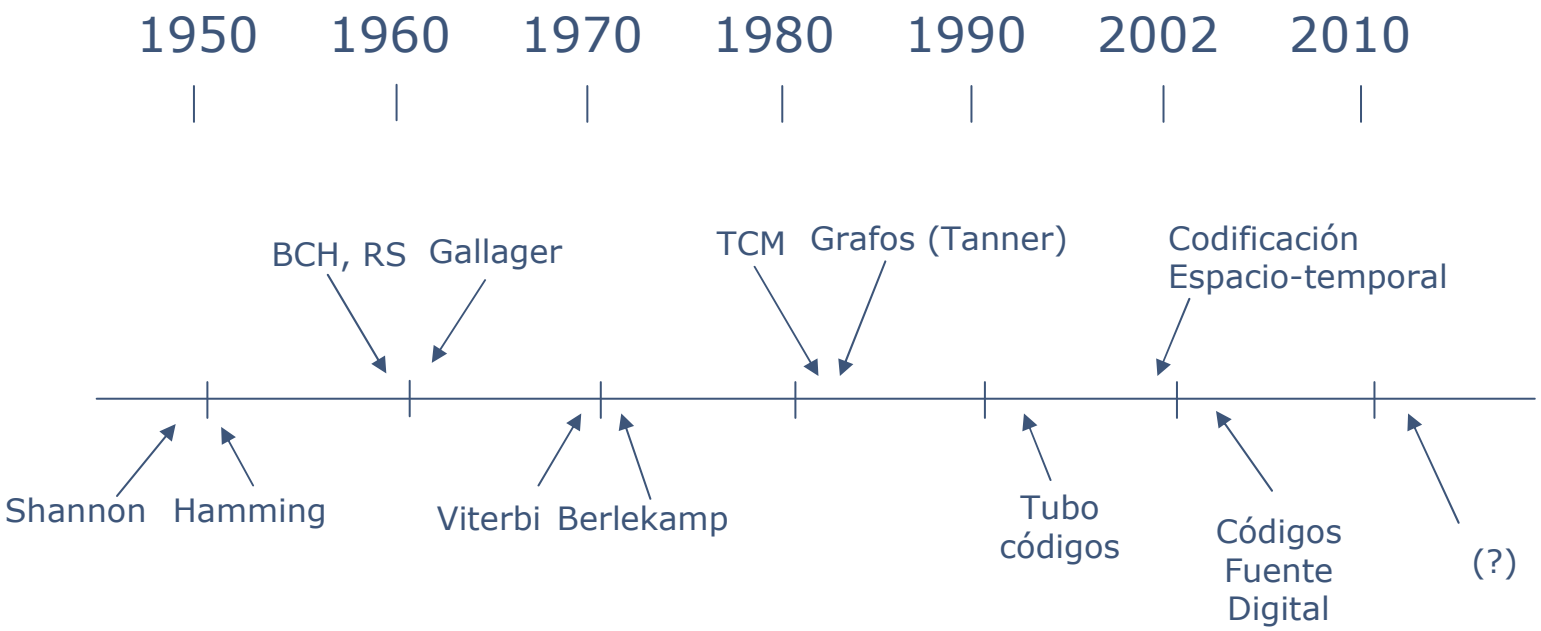
  "The number of bits that can be transmitted per second through a channel is the bandwidth of the channel"

  "A modem commonly runs at 9600 bits per second or 9600 bauds. Baud is not technically the same as bits per second, but has come to be used interchangeably, as I have done in this text"

  N. Negroponte, "*Being Digital*"

- El invento se conoce como TCM (Trellis Coded Modulation)
- G. Ungerboeck: 1977,1982
- Recibido con escepticismo en 1977
- Premio al mejor artículo IEEE Inf. Theory: 1982
- Muchas mejoras y refinamientos posteriores por aportaciones matemáticas.
- Cristalizado en normas: V.34, V.90, V.92, DSL
- Extrema importancia práctica: Red acceso Internet
- Ejemplo de la determinación de hacer aquello que se sabe se puede hacer.
- Situación 1977: 9600 bps en líneas dedicadas (Torremolinos, 1976). Teoría Shannon ≈ 30 kbps.

- Renacimiento LDPCC: Otro efecto beneficioso códigos "fuente digital" (Digital fountain)
- Reconstruir la información a pesar de la pérdida de paquetes en la red de transporte.
- Mejora del caudal extremo-extremo en Internet.
- Código basados en grafos bipartitos altamente irregulares.
- Las aportaciones de carácter matemático: mejora los diseños iniciales (Luby, 2002)
- El futuro de la codificación se guía por los principios fundamentales de su pasado, brillantemente expuestos por Shannon hace ya años.



- Los hitos más importantes se han producido cada 10 años. Se espera otro hacia el 2012. ¡Ojala sea una contribución española!