

LAS MATEMATICAS Y LA TÉCNICA  
EN LA TRANSMISION DE INFORMACION:  
ALGUNAS REFLEXIONES.

E. SANVICENTE

DEPT. ING. TELEMÁTICA

e.sanvicente.entel.upc.es

COMENTARIOS SOBRE EL TÍTULO

MATEMÁTICAS ≠ LOS MATEMÁTICOS

TECNICA ≠ INGENIEROS

CÓMO SE PIENSA, NO EL TÍTULO

RIGOR INTELECTUAL NO ESTA  
REÑIDO CON LA INTUICION  
INGENIERIL

TELECOMAT, PERSONAS CONFORTABLES  
EN AMBOS LADOS

COLABORACION FRUCTIFERA EN AMBOS  
SENTIDOS

SIMBIOSIS

SIMBIOSIS : COJO A HOMBROS DE CIEGO  
CIEGO ≠ INGENIERO, COJO ≠ MATEMATICO  
TANTO MONTA, MONTA TANTO...

REFRAN ESPAÑOL: "MAS VALE MAÑA  
QUE FUERZA"

CUANDO SE ACUÑA?

EXPONENTE DE ELLO EN EL  
MUNDO GRIEGO:

ARQUIMEDES

ESTATICA

"DADME UN PUNTO DE APOYO Y  
MOVERE EL MUNDO"

OTRO EJEMPLO: CLAUDE SHANNON

DOBLE TITULACION: ING. ELECTRICO, MATEMATICAS

MASTER MIT: ING. ELECTRICA

DORTORADO MIT: MATEMATICAS

INSTITUTO DE ESTUDIOS AVANZADOS, PRINCETON

BELL LABS: "A MATHEMATICAL THEORY OF COMMUNICATION" (1948), 32 AÑOS

"NO CONOZCO NINGUN EJEMPLO DE UN AVANCE MATEMATICO DE IMPORTANCIA DESARROLLADO POR UNA PERSONA QUE HAYA SUPERADO LOS 50. LA MATEMATICA ES ASUNTO DE JOVENES" (HARUY, APOLOGIA DE UN MATEMATICO)

CRITICAS: MATEMATICOS 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 TEORICO DEL CALCULO DE PROBABILIDADES

SU HOMOLOGO RUSSO: A. KOLMOGOROV

"SHANNON'S MATHEMATICAL INTUITION WAS AMAZINGLY PRECISE. HE CAN BE RANKED AS BOTH ONE OF THE LEADING MATHEMATICIANS AND ONE OF THE LEADING ENGINEERS OF THIS TIME"

CRITICAS : LOS INGENIEROS LO CONSIDERAN  
UNA CURIOSIDAD MATEMATICA

CAMBIO RADICAL EN LA FORMA DE PENSAR  
EN CONFLICTO CON LA INTUICION

EL TRANSMISOR JUEGA UN PAPEL TAN  
IMPORTANTE COMO EL RECEPTOR EN LA  
SUPRESION DEL RUIDO

EL RUIDO EN EL CANAL LIMITA LA  
VELOCIDAD DE TRANSMISION 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'



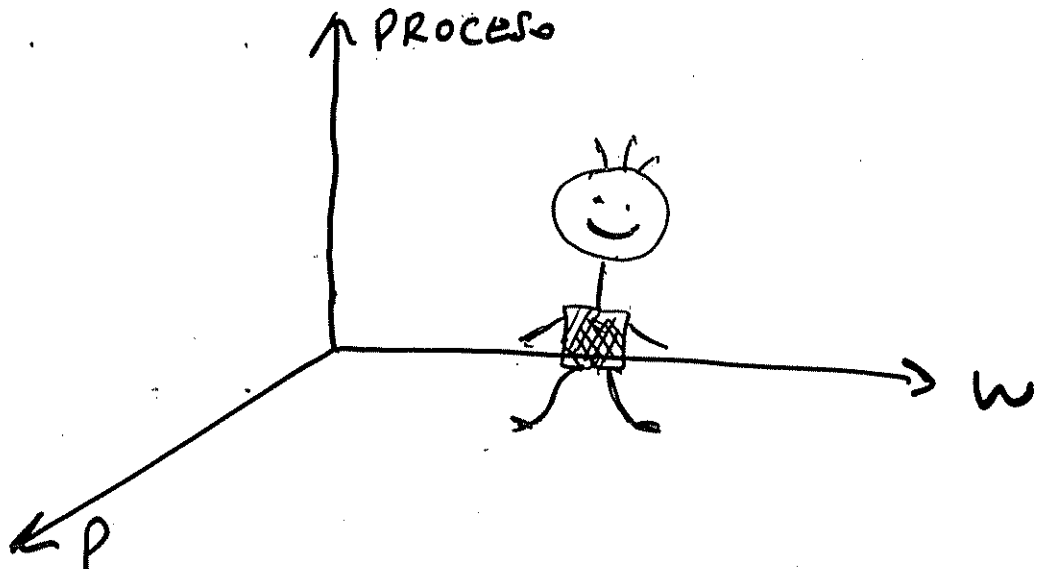
A PARTIR DE 1948

HAY RECURSOS DE DOS TIPOS

FISICOS : FUERZA (P, W)

'NEURONALES' : MAÑA, PROCESO

SHANNON DESCUBRE LA TERCERA DIMENSION



CAMBIO DEL TITULO : " THE MATHEMATICAL THEORY OF COMMUNICATION" (1949)

ECO INCLUDES EN UNA CANCION

"AS TIME GOES BY"

INOLVIDABLE PELICULA: "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. SHANNON'S THEORY

⋮

## NOTA AÑADIDA POSTERIORMENTE A LA CONFERENCIA

EN LA CONFERENCIA COMENTE QUE LA LETRA DE "AS TIME GOES BY" NO PODIA SER EXACTAMENTE LA QUE REFLEJABA LA TRANSPARENCIA. EN EFECTO, LA PELICULA TIENE COMO TRANSFONDO LA II GUERRA MUNDIAL, MIENTRAS QUE EL TRABAJO DE SHANNON ES POSTERIOR. ASI, EN LUGAR DEL DE SHANNON, EL NOMBRE QUE APARECE EN LA CANCION ES EL DE EINSTEIN. SI ME PERMITI ESTE PEQUEÑO CAMBIO (ACLARADO LUEGO IN SITU) FUE PARA QUE LA AUDIENCIA RECORDASE TAMBIEN 'AUDITIVAMENTE' LA TERCERA DIMENSION DE SHANNON. DISO 'AUDITIVAMENTE' PORQUE LA CANCION FUE ADMIRABLEMENTE INTERPRETADA AL SAXOFON POR MARIA GRACIA, ALUMNA DE 1º DE LA ETS ING. CAMINOS E HITA DE IGNACIO GRACIA, PROFESOR DEL

DEPARTAMENTO DE MATEMÁTICA APLICADA IV.

NO OBSTANTE, LA LETRA CON EL NOMBRE DE EINSTEIN ES TAMBIÉN CONCEPTUALMENTE INCORRECTA, YA QUE DEBERÍA DECIR 'CUARTA' DIMENSION Y NO 'TERCERA', QUE ES LO QUE APARECE EN LAS DOS VERSIONES QUE YO TENGO (TONY BENNETT; '20 GOLDEN HITS' ROD STEWART: 'THE GREAT AMERICAN SONG BOOK' VOL. II); RECIENTEMENTE, MIGUEL ÁNGEL FIOL (TAMBIÉN DEL DPTO. MAT. AP. IV) ME HA HECHO LLEGAR OTRA VERSIÓN DE DICHA CANCIÓN EN LA QUE APARECE EINSTEIN CON LA CUARTA DIMENSION.

¿CUANTAS VERSIONES HABRÁ CON CADA UNO DE ESTOS ADJETIVOS?

QUIZA ALGUIEN CON TIEMPO PUEDA ECHAR LUZ SOBRE ESTA CUESTIÓN.

VOLVAMOS A SHANNON

DEMOSTRACION MATEMATICA INDIRECTA, NO CONSTRUCTIVA

DESILUACION ENTRE LOS INGENIEROS

INJUSTIFICADA

NINGUNA TEORIA 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, 1984)

' 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 1<sup>st</sup> EDITION, 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 ... "

(ID, 2<sup>nd</sup> EDITION, 1994)

SHANNON ES UN VISIONARIO: INDICA EL CAMINO  
QUE SE PUEDE HACER

NO DICE CÓMO (ALGORITMICA)

NI, MUCHO MENOS, CON QUE (DISPOSITIVOS ELECTRONICA)

NO EXISTIAN CIRCUITOS INTEGRADOS

EL TRANSISTOR SE INVENTO EN 1948

CURIOSAMENTE: MISMO AÑO, MISMO LUGAR (BELL)

ESAS DIFICULTADES TECNOLOGICAS EXPLICAN  
(JUSTIFICAN) EL RETRASO DEL MUNDO REAL  
RESPECTO AL CONCEPTUAL

UN EJEMPLO:

PRIMERA IMPLEMENTACION PCM: BELL, 1962

PATENTE FRANCESA (ITT, REEVES): 1939

PROGRESO MUY LENTO

CARENCIAS TEÓRICAS, NO SOLO 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 TRANSMITIR MENSAJES.

EL TEOREMA DE EXISTENCIA ES SIN EMBARGO  
ÚTIL: HAY UNA AGUJA EN EL PAJAR

ENCONTRARLA ES ASUNTO DE OTROS

HABÍA UNA FIRME DETERMINACIÓN EN LLEGAR A  
SABER COMO 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  
( $m$ : PARAMETRO)

SACRIFICAR ALGUNO ( $\tau = m$ ) DE LOS  $2^m - 1$   
PARA INDICAR LA POSICION DEL ERROR

CORREGIR  $t > 1$  EN BLOQUES DE  $2^m - 1$  BITS?

SACRIFICAR  $\tau > m$

¿CUANTOS?

¿CÓMO SELECCIONAR LAS FILAS BINARIAS A  
AÑADIR A LA MATRIZ DE COMPROBACION?

LOS MATEMATICOS IGNORARON EL TEMA

TODO ESTABA EN MANOS DE 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  $m$ !

ASI, LA SOLUCION ES OBUIA!

A LA PREGUNTA : ¿ CÓMO DECODIFICARIAN ?  
RESPONDIERON : ¿ QUÉ ES DECODIFICAR ?

ALGEBRA MODERNA YA HABIA ENTRADO ANTES  
EN EL TEMA

D. SLEPIAN

TABLA DE SLEPIAN = VISUALIZACION GRAFICA DEL  
TEOREMA DE D'ALEMBERT

COR BOSE - CHAUDHURI, EXTRA DE LLENO

EN ALGEBRA MODERNA HABIA UNA  
APLICACION DE VERDAD!

' LA MAYOR PARTE DE LAS MATEMATICAS  
SUPERIORES SON INUTILES. EL ALGEBRA  
MODERNA, LA TEORIA DE NUMEROS  
NO PASARIAN LA PRUEBA DE LA  
UTILIDAD (G. H. HARDY)

CONTRIBUCION DE BOSE-CHAUDHURI  
UN BUEN EJEMPLO DEL ORIGEN APLICADO DE  
LAS MATEMATICAS, MUY FRECUENTE ANTES,  
PERO NO TAN USUAL EN NUESTROS  
DIAS

UNA VEZ ABIERTA LA PUERTA:

ECUACIONES ALGEBRAICAS EN  $GF(2^m)$   
CUYAS RAICES LOCALIZAN LOS  
ERRORES

POLINOMIOS MINIMOS DE ELEMENTOS  
DEL CUERPO PARA OBTENER LOS  
POLINOMIOS GENERADORES

AÑO 1960: DOBLE (TRIPLE!) BIG-BANG

APARECEN TAMBIEN LOS CODIGOS REED-SOLOMON

MUY UBICOS: SONDAS NASA, CD, DVD, DVR, ...

SIMBOLOS: ELEMENTOS DE  $GF(2^m)$ , NO BITS

$t$  MINIMA PARA  $t$  DADA

ALGORITMO DE DECODIFICACION MUY EFICIENTE  
BERLEKAMP, 1968

POLINOMIO GENERADOR DEL CODIGO: PRODUCTO DE  
 $t$  MONOMIOS

RAICES DEL POLINOMIO GENERADOR: COMO  
POTENCIAS DE UN ELEMENTO GENERADOR  
DEL CUERPO, TIENEN EXPONENTES  
CONSECUTIVOS

INGENIEROS CADA VEZ MAS 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 BATERIAS !

- ¿ EN QUÉ POTENCIA SE EMPLEA PARA CONSTRUIR EL POLINOMIO GENERADOR DEL CODIFICADOR DE REED-SOLOMON ?

IRRELEVANTE(?) : TODOS LOS CODIGOS SON EQUIVALENTES

IMPLEMENTACION : MEMORIAS ROM

- CÓMO SE PUEDE APROVECHAR EL QUE (DIGAMOS) EL DEMODULADOR ME INDICAME LA BAJA FIABILIDAD DE UNA DE SUS DECISIONES

ES IMPROBABLE QUE ESTAS PREGUNTAS SE LAS PLANTEASE ALGUIEN SIN FORMACION TECNICA

EN 1960 HUBO TAMBIEN OTRO ALUMBRAMIENTO  
IMPORTANTE

CODIGOS CON MATRIZ DE COMPROBACION DE BAJA  
DENSIDAD

(LOW DENSITY PARITY CHECK CODES  $\equiv$  LDPC)

TESIS DE DOCTORADO DE R. GALLAGER : MIT  
MASTER : MIT, 1956.

EL LUGAR ERA EL APROPIADO: HEGEMONIA  
TOTAL DEL MIT

- ESTRUCTURA : REGULARIDAD ESTADISTICA  
DE LOS GRANDES NUMEROS

CONJUNTO CONCRETO DE MATRICES ALEATORIA  
DE GALLAGER TIENEN EXCELENTES PROPIEDADES  
ESTADISTICAS

- EL RECEPTOR DECODIFICA CON UN  
ALGORITMO ITERATIVO PROBABILISTA,  
QUE DISEÑA

ES IMPROBABLE QUE LA IDEA DE LOS LDPC SE LE  
HUBIESE OCURRIDO A UN MATEMATICO

PLANTEADO MATEMATICAMENTE EL ALGORITMO DE  
DECODIFICACION : INTERPRETABLE COMO PASO  
DE INFORMACION ENTRE NODOS DE UN GRAFO  
BIPARTITO

EJECUCION DEL ALGORITMO DE FORMA PARALELA

MUY CONVENIENTE CON NUMEROS GRANDES  
64000 BITS, CON UN NUMERO DE  
CONDICIONES DE COMPROBACION ELEVADO  
(ENTRE 6000 Y 48000, APROX.)

AREA INTERESANTE Y ACTIVA DE  
TRABAJO : ESTRUCTURA DEL GRAFO,  
CONDICIONES DE CONVERGENCIA (RAPIDA), ETC.

¿QUE PASO CON LOS CODIGOS LDPC?

GALLAGER NI LOS MENCIONA

(INFORMATION THEORY AND RELIABLE COMMUNICATION, 1968)

PETERSON-WELDON

CYCLIC 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 DECODIFICACION POR MAYORIA, 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)

TARDIO

• J. NASH

(TESIS 1950, NOBEL 1994)

M. TOMLINSON

(TESIS 1970, TCM: 1984)

R. GALLAGER

(TESIS 1960, RESURRECCION: 1993)

" LA FEIKA BEN FETA ... "

RENACIMIENTO DEL INTERES POR LA  
DECODIFICACION PROBABILISTA Y LOS LDPC

DEBIDA A LA INVENCIÓN DE LOS TURBO-CODIGOS  
(BERROU-GLAVIEUX, 1993)

IMPROBABLE QUE ESTE ESQUEMA SE LE  
HUBIESE OCURRIDO A ALGUIEN SIN FORMACION  
TECNICA

REALIMENTACION ENTRE LOS DOS DECODIFICADORES  
ESTABILIDAD: LLEVA AL CONCEPTO DE  
INFORMACION EXTRINSECA

RECIBIDO POR INGENIEROS CON ESCEPTICISMO

SOLO HABIA PRUEBAS EXPERIMENTALES

FINALMENTE SE IMPUSO: 1998, PREMIO AL  
MEJOR ARTICULO (IEEE INF. THEORY)

CONTEMPLADO EN EL ESTANDAR UMTS  
(ETSI)

OTRO INVENTO, DIFÍCIL DE CONCEBIR SIN  
FORMACION TECNICA

HAY QUE ENTENDER CLARAMENTE LOS  
CONCEPTOS DE ANCHO DE BANDA, VELOCIDAD  
DE MODULACION, VELOCIDAD DE TRANSMISION,  
EFICIENCIA ESPECTRAL

CONCEPTOS FAMILIARES A LOS ESPECIALISTAS  
EN TRANSMISION, NO ASI 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 MEJOR ARTICULO IEEE INF. TH. : 1982

MUCHAS MEJORAS Y REFINAMIENTOS  
POSTERIORES POR APORTACIONES  
MATEMATICAS

CRISTALIZADO EN NORMAS : V.34, V.90

V.92, DSL

EXTREMA IMPORTANCIA PRACTICA : RED ACCESO  
INTERNET

EJEMPLO DE LA DETERMINACION DE HACER  
AQUELLO QUE SE SABE SE PUEDE  
HACER

SITUACION 1977: 9600 BPS EN LINEAS  
DEDICADAS (TORREMOLINOS, 1976)

TEORIA SHANNON  $\approx$  30 KBPS.

RENACIMIENTO LDPCC: OTRO EFECTO BENEFICIOSO

CODIGOS "FUENTE DIGITAL" (DIGITAL FOUNTAIN)

RECONSTRUIR LA INFORMACION A PESAR  
DE LA PERDIDA DE PAQUETES EN LA  
RED DE TRANSPORTE

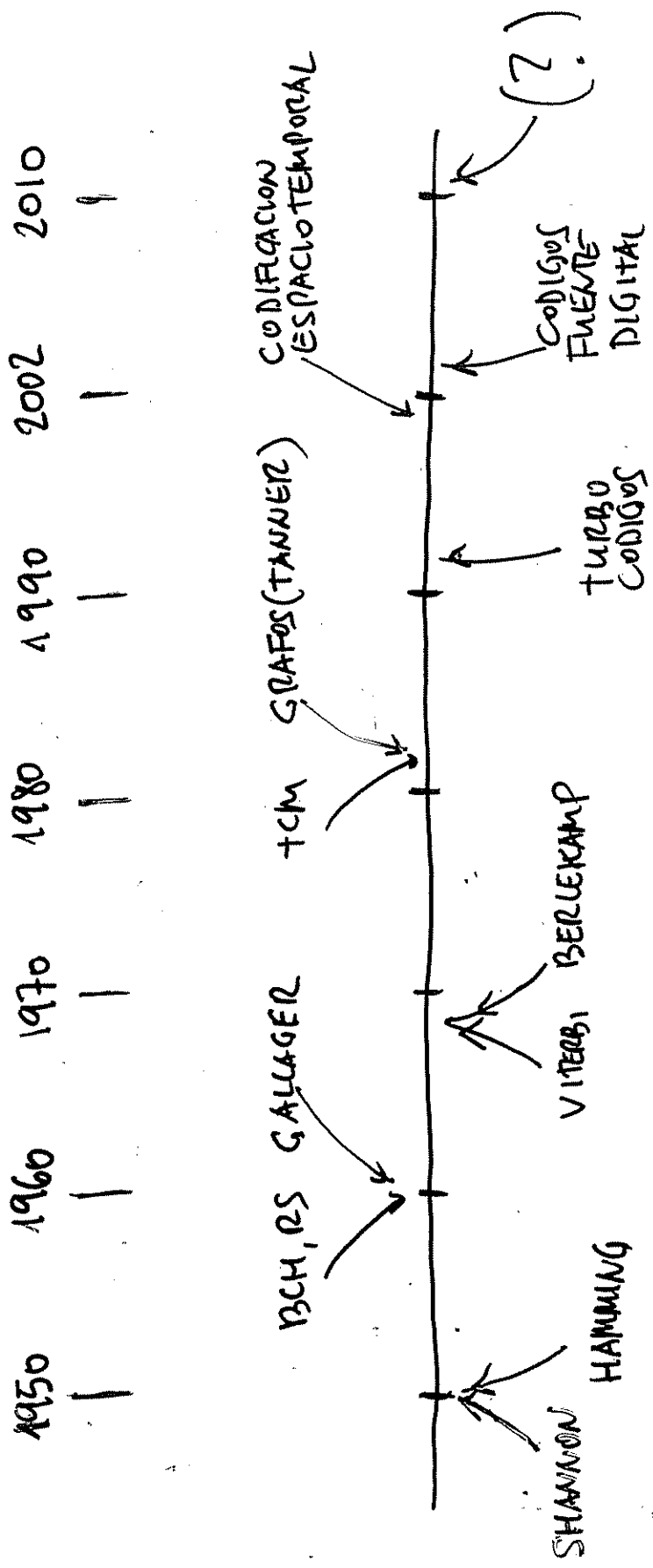
MEJORA DEL CAUDAL EXTREMO-EXTREMO  
EN INTERNET

CODIGOS BASADOS EN GRAFOS BIPARTITOS  
ALTAMENTE IRREGULARES

LAS APORTACIONES DE CARACTER  
MATEMATICO: MEJORA DE LOS  
DISEÑOS INICIALES

(LUBY, 2002)

EL FUTURO DE LA CODIFICACION SE  
GUIA POR LOS PRINCIPLOS FUNDAMENTALES  
DE SU PASADO, BRILLANTEMENTE EXPUESTOS  
POR SHANNON HACE YA MAS DE  
50 AÑOS.



LOS HITOS IMPORTANTES SE HAN PRODUCIDO CADA 10 AÑOS. SE ESPERA OTRO HACIA EL 2012. ¡OTRA SEA UNA CONTRIBUCION ESPAÑOLA!

GRACIAS