Prossimi al limite di Shannon, 60 anni dopo

Marzio **Barbero**,
Natasha **Shpuza**

Sommario

Sessanta anni fa Claude E. Shannon formulava una relazione fondamentale, destinata a rivoluzionare la teoria delle telecomunicazioni. Tale relazione consente di valutare la capacità di un canale digitale in funzione della sua larghezza di banda. Negli anni immediatamente successivi fu rapida l'evoluzione della teoria dei codici per la protezione dagli errori, con l'obiettivo di individuare schemi in grado di approssimare la capacità massima teorica del canale, denominata "limite di Shannon". Inizialmente le applicazioni furono soprattutto nell'ambito delle comunicazioni dal profondo spazio. Più recentemente i progressi in questo campo sono stati fondamentali per la realizzazione di applicazioni e servizi oggigiorno indispensabili, quali la telefonia mobile e la diffusione televisiva digitale. Negli ultimi quindici anni, con l'avvento dei turbo codici e la successiva riscoperta dei codici LDPC, si è in grado di approssimare, e quasi raggiungere, il limite. La prima applicazione che ha ottenuto tale risultato è stato il sistema di diffusione televisiva digitale da satellite di seconda generazione (DVB-S2).

1. Sessanta anni fa: un contributo leggendario

E' importante ricordare alcune delle tappe fondamentali che hanno consentito lo sviluppo delle teorie e delle tecniche che sono alla base dei sistemi di comunicazione moderni.

In particolare, basilare è il contributo costituito dalla coppia di articoli pubblicati proprio sessanta anni fa da Claude E. Shannon, destinata a rivoluzionare la tecnologia alla base delle telecomunicazioni [1].

Nel numero precedente di questa rivista è stata pubblicata la prima parte di un articolo ("Rivelazione, correzione e mascheramento degli errori") sulle tecniche di protezione dagli errori, tecniche alla base delle notevoli prestazioni raggiunte negli ultimi anni nel campo della diffusione e memorizzazione dei segnali audio e video. La seconda parte, a completamento, sarà pubblicata nel prossimo numero.

Il presente articolo è strettamente correlato con tale panoramica, approfondendo maggiormente l'aspetto storico dei progressi teorici che hanno consentito il rapido sviluppo a cui assistiamo oggi.

L'evoluzione delle teoria dei codici per la protezione degli errori ha trovato dapprima applicazione soprattutto nel campo delle telecomunicazioni spaziali, ma negli ultimi anni sono state proprio le applicazioni di uso più generalizzato (diffusione televisiva digitale, telefonia mobile e *wireless*) a mettere in pratica in modo sempre più efficiente le teorie, anche quelle già pubblicate decenni fa, grazie alle possibilità offerte dai progressi dei circuiti VLSI in termini di velocità e di capacità di memoria.

In particolare il sistema di diffusione televisiva da satellite di seconda generazione (DVB-S2) è stato il primo a consentire di avvicinarsi come non era mai avvenuto prima al limite teorico della capacità di un canale digitale, quello indicato da Shannon sessant'anni fa.

2. 1948: il limite di Shannon

Scriveva Shannon: *"Il problema fondamentale della comunicazione è quello di riprodurre in un punto o esattamente, o approssimativamente, un messaggio definito in un altro punto."*

Shannon formulò una relazione fondamentale che consente di valutare la capacità C di un canale soggetto a rumore additivo con distribuzione gaussiana e caratterizzata da una larghezza di banda W.

"Può sembrare sorprendente che si debba definire un capacità C definita per un canale rumoroso, poiché non possiamo mai inviare informazione certa in un tale caso. E' chiaro, tuttavia, che inviando l'informazione in forma ridondante, la probabilità di errori può essere ridotta. ... Di fatto la capacità C precedentemente definita ha un significato completamente determinato. E' possibile inviare informazione alla velocità C attraverso il canale ***con una frequenza di errori o imprecisioni piccola a piacere*** *per mezzo di una codifica appropriata. Questa affermazione non è valida per velocità di segnalazione superiori a C."*

Acronimi e sigle

APP	A Posteriori Probability
ASI	Agenzia Spaziale Italiana www.asi.it
AWGN	Additive White Gaussian Noise
BCH	Bose Chaudhuri Hocquenghem
BVD	Big Viterbi Decoder
CCSDS	Consultative Committee for Space Data Systems www.ccsds.org
CRC	Cyclic Redundancy Check
DVB	Digital Video Broadcasting www.dvb.org
-S	- Satellite
-RCS	- Return Channel over Satellite
-RCT	- Return Channel over Terrestrial
-S2	- Satellite (new generation)
-T2	- Terrestrial (new generation)
ESA	European Space Agecy www.esa.int
HDTV	High Definition TeleVision
IRA	Irregular Repeat Accumulate
JPL	Jet Propulsion Laboratory www.jpl.nasa.gov
LDPC	Low Density Parity Check
MRO	Mars Reconnaisance Orbiter
NASA	National Aereonautics and Space Administration www.nasa.gov
PLL	Phase Lock Loop
RM	Reed Muller
RS	Reed Solomon
SHV	Super Hi-Vision
SOVA	Soft-Output Viterbi Algorithm
VA	Viterbi Algorithm
VLSI	Very Large Scale Integration

La relazione fra capacità e larghezza di banda è fornita da:

"Teorema 17: La capacità di un canale di banda W perturbato da un rumore termico bianco di potenza N quando la potenza media del trasmettitore è limitata a P è data da:

$$C = W \log_2 \frac{P+N}{N}$$

La capacità C è espressa in bit al secondo per un canale soggetto a rumore additivo con distribuzione gaussiana (AWGN), W è la larghezza di banda del canale in Hertz, P e N sono rispettivamente le potenza del segnale trasmesso e la potenza di rumore espressi in Watt.

Sessanta anni fa veniva quindi definito il limite teorico della capacità di un canale binario e suggerito l'uso di *codici efficienti*, come quello di Hamming, per avvicinarsi a tale limite.

3. 1949-1962: l'evoluzione nella teoria dei codici

Il matematico Richard Hamming era stato assunto nel 1946 dai Bell Labs per lavorare sulla teoria dell'elasticità e utilizzava i computer del tempo, poco affidabili: nel caso in cui veniva rivelata la presenza di un errore l'esecuzione del programma si arrestava.

Hamming cercò una soluzione: organizzare i bit in blocchi, a cui aggiungere dei bit di parità in grado non solo di rivelare la presenza di un errore, ma anche di correggerlo, in modo da consentire ai programmi di completare i calcoli e giungere alla conclusione.

Nacque così il primo codice correttore di errori, H(7,4,3)[Nota 1] e Shannon lo descrive nel 1948 (figura 1) come "*un codice efficiente, che consente la correzione completa di errori e la trasmissione alla velocità C (fondato su un metodo dovuto a R. Hamming)*".

I due paragrafi di descrizione del codice di Hamming contenuti nell'articolo di Shannon furono lo stimolo per l'articolo del 1949 di Marcel Golay [2]. Questo articolo è ritenuto da molti il più notevole mai scritto sulla teoria dei codici, perché in meno di una pagina vengono presentati: due codici *perfetti*[Nota 2], uno binario (23, 12, 7) ed uno ternario (11, 6, 5), la generalizzazione dei codici di Hamming e la prima pubblicazione di una matrice di controllo della parità.

Nota 1 - Nella notazione (n,k,d_{min}) n indica la lunghezza del codice a blocco, k il numero di simboli che costituiscono il codice e d_{min}, la distanza minima di Hamming, è legata al numero di errori che il codice consente di correggere.

Nota 2 - In termini matematici, in un codice perfetto, le sfere intorno alle parole di codice costituiscono una partizione dello spazio dei vettori.

Fig. 1

17. An Example of Efficient Coding

The following example, although somewhat unrealistic, is a case in which exact matching to a noisy channel is possible. There are two channel symbols, 0 and 1, and the noise affects them in blocks of seven symbols. A block of seven is either transmitted without error, or exactly one symbol of the seven is incorrect. These eight possibilities are equally likely. We have

$$C = \text{Max}\,[H(y) - H_x(y)]$$
$$= \tfrac{1}{7}\,[7 + \tfrac{8}{8}\log\tfrac{1}{8}]$$
$$= \tfrac{4}{7}\ \text{bits/symbol}.$$

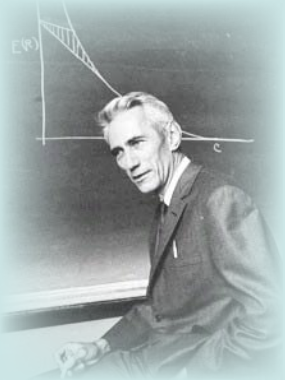
An efficient code, allowing complete correction of errors and transmitting at the rate C, is the following (found by a method due to R. Hamming):

Let a block of seven symbols be $X_1, X_2, \ldots X_7$. Of these X_3, X_5, X_6 and X_7 are message symbols and chosen arbitrarily by the source. The other three are redundant and calculated as follows:

X_4 is chosen to make $\alpha = X_4 + X_5 + X_6 + X_7$ even
X_2 " " " " $\beta = X_2 + X_3 + X_6 + X_7$ "
X_1 " " " " $\gamma = X_1 + X_3 + X_5 + X_7$ "

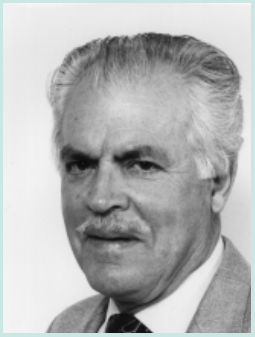
When a block of seven is received α, β and γ are calculated and if even called zero, if odd called one. The binary number $\alpha\,\beta\,\gamma$ then gives the subscript of the X_i that is incorrect (if 0 there was no error).

Ritratto di alcuni dei protagonisti



Claude Elwood Shannon: nato a Petoskey (Michigan) nel 1916 e morto nel 2001. Da ragazzo lavorò come telegrafista e conseguì due lauree nel 1936, in matematica e in ingegneria elettrica. Del 1940 è il dottorato, dal '41 al '72 lavorò ai Bell Labs. Durante la seconda guerra mondiale si occupò di ricerca per la guida di "missili". Dal '58 al '78 fu professore al MIT.

Richard Hamming: nato a Chicago nel 1915 e morto a Monterey (CA) nel 1998. Nel 1945 entrò a far parte del progetto Manhattan, il progetto per realizzare la bomba atomica, a Los Alamos. Nel 1946 iniziò l'attività nei Bell Laboratories dove restò fino al 1976.



Irving S. Reed, nato a Seattle nel 1923. ottiene il dottorato al California Institute of Technology nel 1949. Dal 1951 al 1960 associato al MIT. Professore, dal 1963, alla University of South California.

Andrew James Viterbi, nasce nel 1935 a Bergamo ed emigra con i genitori, a causa delle leggi razziali, nel 1939 negli Stati Uniti, dove studia al MIT dal 1952 al 1957. Ha fondato diverse società fra cui la Qualcomm, nel 1985.

Robert G. Gallager, nato a Filadelfia nel 1931, fa parte del personale tecnico dei Bell Labs nel 1953-54, ottiene il dottorato al MIT nel 1960. Professore e autore di numerosi testi sulla teoria dell'informazione.

L'articolo in cui Hamming descrive il codice è del 1950 [3], cioè fu pubblicato due anni dopo quello di Shannon. La spiegazione di tale ritardo rispetto alla citazione di Shannon, fu fornita da Hamming stesso: *"il lavoro fu concluso in tre mesi, ma per ragioni brevettuali fu tenuto in sospeso per due anni"*.

Sia i codici di Hamming che quelli di Golay sono *lineari*, cioè la somma modulo-q di una coppia di parole di codice costituite da simboli q-ari (cioè binari, ternari...) è anch'essa una parola di codice.

Nel 1954 Muller [4] descrive l'applicazione di codici nel contesto della progettazione in logica booleana, e Reed identifica tali codici come classe di codici lineari a blocco e ne propone l'algoritmo di decodifica [5].

Sempre nel 1954 viene descritto l'algoritmo di decodifica di Wagner, il primo algoritmo in letteratura di decodifica *soft-decision*. Questo è un approccio fondamentale per l'evoluzione della decodifica e per consentire le prestazioni oggi raggiunte: la decodifica tiene conto della affidabilità della decisione sul simbolo in uscita dal canale.

P. Elias inventa nel 1954 i codici prodotto [6] ed un anno dopo inventa i codici convoluzionali [7]. Il suo allievo, Robert Gallager, puntualizza che in tale articolo è evidenziato che *"l'ottenimento di una probabilità di errore piccola, a qualsiasi probabilità prossima alla capacità, richiede necessariamente un codice con una elevata lunghezza di blocco"*.

Successivamente (1957) vennero scoperti i codici *ciclici* [8], che sono codici a blocco, lineari e che godono dell'ulteriore proprietà: lo shift ciclico di una parola di codice è ancora una parola di codice. Questa caratteristica consente di realizzare codificatori e decodificatori di limitata complessità. Inoltre tali codici possono essere descritti mediante un *polinomio generatore*. Sono anche denominati CRC; il loro uso è limitato generalmente alla sola rivelazione degli errori, infatti la complessità del decodificatore cresce esponenzialmente con il numero di errori correggibili.

Una sottoclasse dei codici ciclici è scoperta quasi contemporaneamente da Hocquenghem nel 1959 [9] e da Bose e Ray-Chaudhuri [10] nel 1960 e pertanto sono noti come codici BCH.

Sempre nel 1960 [11] Reed e Solomon descrivono i codici universalmente oggi noti con i loro nomi (RS): sono una classe non binaria dei codici BCH, o, in alternativa, i BCH sono sono sottocodici di un sottocampo di codici RS.

Nel 1962 [12], Gallager è motivato, nella sua tesi di dottorato con la supervisione di Elias, dalla ricerca di una classe di codici quasi casuali che possano consentire una decodifica prossima alla capacità del canale e caratterizzati da una complessità tale da non comprometterne la fattibilità: introduce così i codici LDPC. L'algoritmo di decodifica APP descritto è ritenuto la prima citazione in letteratura dell'algoritmo somma-prodotto oggi ampiamente utilizzato.

Nei primi quattordici anni, a partire dall'articolo di Shannon, erano state poste tutte le basi teoriche su cui si fondano gli sviluppi tecnologici realizzati anche in anni molto più recenti. Ma in quegli anni le applicazioni pratiche non erano state così rapide come l'evoluzione teorica.

4. Comunicazioni dallo Spazio

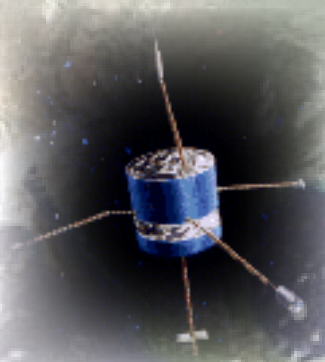
Un canale di comunicazione che ha ampiamente tratto vantaggio dall'uso delle tecniche di recupero delle informazioni in presenza di elevato rumore è quello delle comunicazioni spaziali.

Il 4 ottobre del 1957 l'Unione Sovietica lanciò nello spazio lo Sputnik, il 31 gennaio 1958 gli Stati Uniti, colti di sorpresa, risposero con il lancio di Explorer I, progettato e costruito da JPL (laboratorio fondato dall'Istituto di Tecnologia della California nel 1930) su richiesta dell'eser-

continua a pag 50...

Comunicazioni dallo Spazio Profondo

Pioneer 9



La serie di sonde Pioneer fu progettata per valutare l'operatività dei veicoli spaziali, su orbita solare. Nelle prime missioni, in base a comandi inviati da terra, potevano essere selezionati cinque bit-rate: 512, 256, 64, 16, e 8 bit/s.

La sonda Pioneer 9, lanciata nel 1968, fu la prima ad utilizzare un codice convoluzionale, R=1/2, L=25, con decodifica sequenziale di Fano. Uno schema analogo, L=32, fu utilizzato nelle successive missioni Pioneer 10 (1972), 11 (1973) e 12 (1978) che esplorarono Giove, Saturno e Venere.

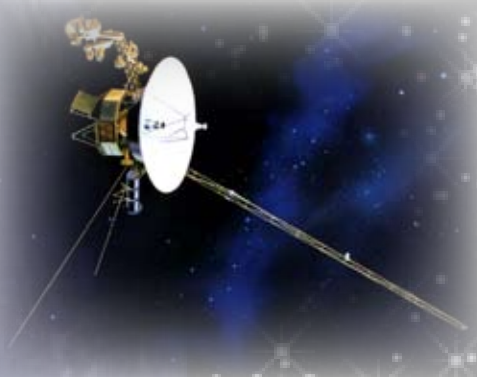
Mariner

Le sonde Mariner utilizzarono dal 1969 al 1973 un codice Reed-Muller RM(32,6,8) con R=0,1875, costituito da parole di 32 bit, 6 di informazione e 26 di parità, in grado di correggere fino a 7 errori. Il canale permetteva la trasmissione di 16 kbit/s verso la terra.

Il Mariner 6 (1969) registrò e inviò a terra 143 immagini della superficie di Marte. Il Mariner 9 (1971) fotografò il 100% della superficie di Marte e le sue lune Phobos e Deimos. Il Mariner 10, lanciato nel novembre 1973, nel febbraio '74 sorvolò Venere e nel marzo '74 Mercurio.

Viking

Analogo schema di codifica fu utilizzato per la missione Viking 1, lanciata nell'agosto 1975: la navicella in orbita fotografò la superficie di Marte e il modulo di atterraggio inviò foto a colori dal luogo dell'atterraggio. Dati pervennero fino al novembre 1982.



Voyager 1 e 2

Le sonde Voyager 2 e 1 furono lanciate, rispettivamente, a maggio e settembre del 1977.

Lo schema di codifica utilizzato era basato su un codice convoluzionale, R=1/2 e L=7, con decodifica di Viterbi, concatenato con codice RS(255,233). Il decoder RS, grazie ad un hardware sviluppato appositamente, era in grado di operare a 1 Mbit/s. Il Voyager 2 ha utilizzato anche un codice di Golay.

La sonda Voyager 1 dal febbraio 1998 è diventato l'oggetto realizzato dall'Uomo più lontano dal Sole, avendo superato la distanza raggiunta da Pioneer 10.
Poiché ora la distanza è prossima alle 15 ore luce, i dati raccolti dalla sonda arrivano con tale ritardo al centro di controllo della JPL.
Voyager 2, lanciata prima della sua gemella, viaggia su un orbita meno veloce, si è "avvicinato" a Giove (1979), Saturno (1981), Urano (1986), Nettuno (1989) e ora lavora per la sua missione interstellare. La NASA ritiene che il contatto potrebbe essere mantenuto con le due sonde oltre il 2020.

Galileo

La missione era stata inizialmente progettata per inviare la navicella spaziale verso Giove con un viaggio diretto della durata prevista di circa tre anni e mezzo. Dopo l'incidente del Challenger (1986), per ragioni di sicurezza fu riprogettato il viaggio in modo da non richiedere l'uso di potenti stadi vettori. Il veicolo spaziale Galileo, portato in orbita dallo shuttle Atlantis, avrebbe sfruttato la forza gravitazionale interplanetaria, per raggiungere Giove in sei anni.

Atlantis decollò il 18 ottobre 1989, con Galileo nella stiva. Una volta iniziato il suo viaggio interplanetario, e a causa della modifica della traiettoria, la navicella spaziale Galileo fu soggetta a temperature molto più elevate di quelle originariamente previste. Il collegamento tra la sonda e terra era assicurato da due antenne a basso guadagno, mentre l'antenna ad alto guadagno, racchiusa come un ombrello, era protetta da scudi termici. Nell'aprile 1991, ormai sufficientemente lontano dal sole, l'antenna principale poteva spiegarsi per raggiungere il diametro previsto, di 4,8 m. Ma l'operazione non riuscì: l'ombrello non si aprì completamente.

Per consentire la trasmissione dei dati verso terra utilizzando le antenne a basso guadagno, dal 1993 al 1996 venne progettato uno schema di codifica molto più potente, in base al quale riprogrammare i codificatori di bordo, e che potesse consentire la decodifica al bit-rate previsto, grazie ad una struttura di elaborazione più complessa.

Lo schema di codifica concatenava un codice interno di tipo convoluzionale R=1/4, L=15, e un insieme di più codici esterni di tipo RS. La complessità hardware del decoder aumenta esponenzialmente al crescere di L, e con L=15 il numero di stati è pari a 2^{14}. Per la decodifica fu realizzato il BVD, basato su strutture di calcolo parallelo in grado di operare alle velocità richieste: ad esempio Galileo inviava dati telemetrici a 134,4 kbit/s.

Galileo arrivò in prossimità di Giove nel dicembre 1995, ed ha completato la sua missione il 21 settembre 2003, lanciato deliberatamente attraverso l'atmosfera gioviana.

Cassini

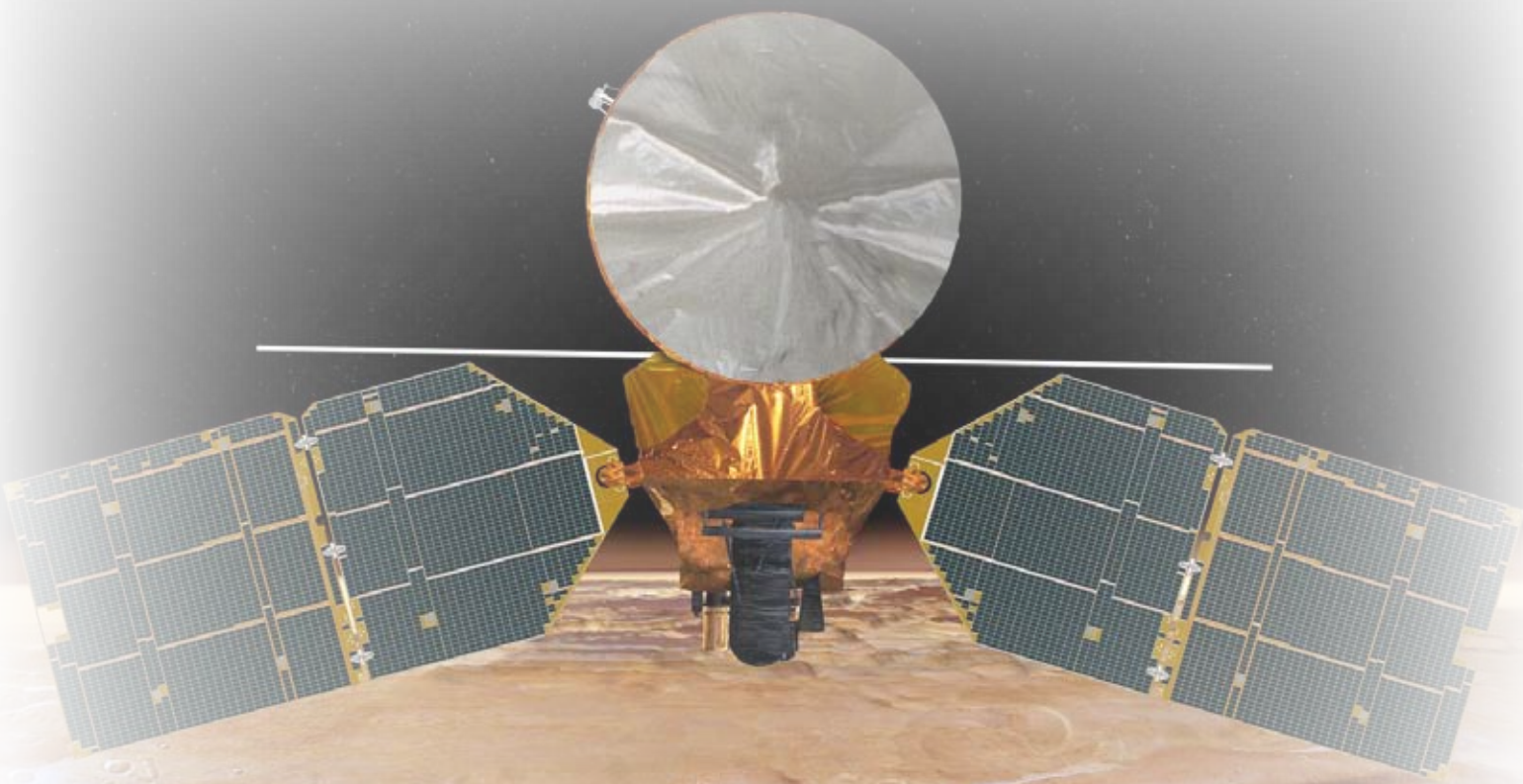
Lanciata nel 1997, è una missione congiunta della NASA, della ESA e della ASI. Prevedeva l'invio di un veicolo spaziale in orbita a Saturno per consentire lo studio del sistema del pianeta e dei suoi anelli per un periodo di quattro anni.

Per acquisire l'energia gravitazionale necessaria a raggiungere la destinazione, è passato accanto a Terra, Giove e Venere (due volte).

Cassini è entrato nell'orbita di Saturno il 1 luglio 2004, nel gennaio 2005 la sonda Huygen è discesa sulla superficie di Titano. Dal 2008 è iniziata una estensione di due anni della missione.

Il veicolo spaziale comunica con due antenne a basso guadagno e un'antenna a grande guadagno.

Lo schema di codifica adottato è basato su codice convoluzionale R=1/6, L=15 concatenato con un fattore I=5 al codice RS(255,233).



MRO
Mars Reconnaisance Orbiter

Lanciato nell'agosto 2005 per cercare le prove della presenza di acqua sulla superfice marziana per un lungo periodo.

MRO è dotato di potenti mezzi di comunicazione e utilizza il turbo codice (8929,1/6)

MRO può trasmettere i dati verso Terra, distante 100 milioni di km, a velocità fino a 6 Mbit/s, grazie all'ampia antenna, al potente amplificatore e al veloce computer. Fino ad oggi ha inviato più dati di tutti i veicoli spaziali JPL messi insieme.

Le immagini che compongono le pagg. 46-49 sono tratte dai siti della NASA.

...continua da pag 45

cito americano. Era nata la competizione per lo spazio, che ebbe come conseguenza un ampio dibattito sul controllo civile o militare della spazio: il 29 luglio 1958, 50 anni fa, il presidente Eisenhower firmava l'atto di nascita dell'agenzia civile NASA, di cui JPL è oggi Laboratorio.

Per consentire la comunicazione con le navicelle spaziali, in JPL furono messe a punto due tecniche fondamentali: l'uso di shift register per codificare le informazioni aggiungendo la ridondanza necessaria alla correzione degli errori e l'uso del PLL, indispensabile per agganciare la frequenza dell'oscillatore locale per demodulare le informazioni ricevute.

I motivi per cui sono state le comunicazioni verso lo spazio a dare inizialmente il maggior spunto agli studi sugli schemi di codifica di canale sono:

- il canale è affetto solo da rumore gaussiano bianco
- la banda è, di fatto, illimitata
- guadagni di frazioni di decibel hanno un valore economico e scientifico molto importante (la capacità di carico dei primi razzi era minima e la potenza disponibile a bordo per la trasmissione dei dati era bassa)
- la complessità, ed il corrispondente ingombro e costo, degli apparati di ricezione e di decodifica, può essere notevole

Nella missione Mariner del 1965 furono inviate con successo immagini di Marte da 200 x 200 pixel, ciascuno rappresentato da 6 bit (64 livelli) ad una velocità di 8 bit al secondo: la trasmissione di ogni singola immagine richiedeva circa 8 ore, non erano utilizzati codici.

Nelle missioni successive, dal 1969 al 1977, le cose migliorarono notevolmente con l'utilizzo dei codice Reed-Muller (RM). I codici RM sono caratterizzati da un insieme di parametri e la scelta flessibile dei valori ne ha consentito un ampio uso. Il guadagno di codifica offerto non era molto elevato, circa 3,2 dB, ma si stima che a quel tempo ogni dB di guadagno corrispondesse ad un risparmio sul costo della missione spaziale di circa un milione di dollari. Grazie al codice RM utilizzato, cui ad ogni 6 bit di informazione sono associati 26 bit per la correzione degli errori, il bit-rate era cresciuto a 16 kbit/s. Con la missione Viking (1976) le immagini sono trasmesse a colori, come tre componenti separate, una per ciascun colore primario.

Il codice era stato messo a punto da Irving Reed, chiamato nel 1963 alla JPL in quanto aveva assunto notorietà per aver sviluppato, alla RAND Corporation, un computer della dimensione di una scrivania, dieci volte meno ingombrante dei suoi contemporanei. Era stato Andrew Viterbi, in JPL dal giugno 1957, a suggerire l'assunzione di Reed.

E proprio a Viterbi è associato l'algoritmo di decodifica noto con il suo nome (VA), introdotto nel 1967 [13], che ha consentito di realizzare decodificatori veloci per i codici convoluzionali.

Infatti i codici convoluzionali furono fra i primi ad essere utilizzati per le comunicazioni spaziali, poiché il codificatore è realizzabile con una struttura estremamente semplice, basata su alcuni flip-flop e porte logiche. Nella missione Pioneer 9 (1968) in ricezione si utilizzava un minicomputer a 16-bit con clock da 1 MHz, decisione soft basata su campioni quantizzati a tre bit e decodifica sequenziale con algoritmo di Fano. Il bit-rate del canale era 512 bit/s.

L'algoritmo di Viterbi fu presto riconosciuto come algoritmo di decodifica ottimo per la decodifica convoluzionale, la cui realizzazione pratica, ad esempio con una macchina a 64 stati, poteva consentire guadagni dell'ordine di 6 dB. In effetti il decoder a 64 stati realizzato dalla Linkabit, fondata, fra gli altri, da Viterbi nel 1968, era *un grande mostro che riempiva un rack*, ma in grado di operare a 2 Mbit/s. Già nel 1975 era possibile integrare l'algoritmo di Viterbi in un chip, rendendolo disponibile per una più ampia gamma di applicazioni nelle telecomunicazioni.

Nelle missioni Voyager del 1977 è introdotto lo schema costituito dal codice RS(255,223,33), in grado di correggere fino a 16 byte errati, come *inner code* concatenato con il codice convoluzionale a 64 stadi, R=1/2, L=7[Nota 3]. Tale schema diviene lo standard NASA.

Nel 1993, a causa degli inconvenienti a dispiegare l'antenna principale nel corso della missione Galileo (vedere riquadro "Comunicazioni dallo Spazio Profondo") fu realizzato uno schema di decodifica a 2^{14} stati denominato BVD, in grado di operare ad una probabilità di errore dell'ordine di $2\ 10^{-7}$ con E_b/N_0[Nota 4] di ≈ 0,8 dB e un guadagno di codifica reale di ≈ 10,2 dB.

Nota 3 - il code rate R è il rapporto k/n dove n è il numero di bit in uscita dal codificatore in corrispondenza di k bit di informazione in ingresso: i bit in uscita sono generati in funzione dei k bit in ingresso e dei precedenti L-1 blocchi di k bit, dove L è denominata constraint length.

Nota 4 - E_0/N_0 è il rapporto fra E_b, l'energia media per bit, e N_0, la densità spettrale del rumore, cioè la potenza su una banda di 1 Hz.

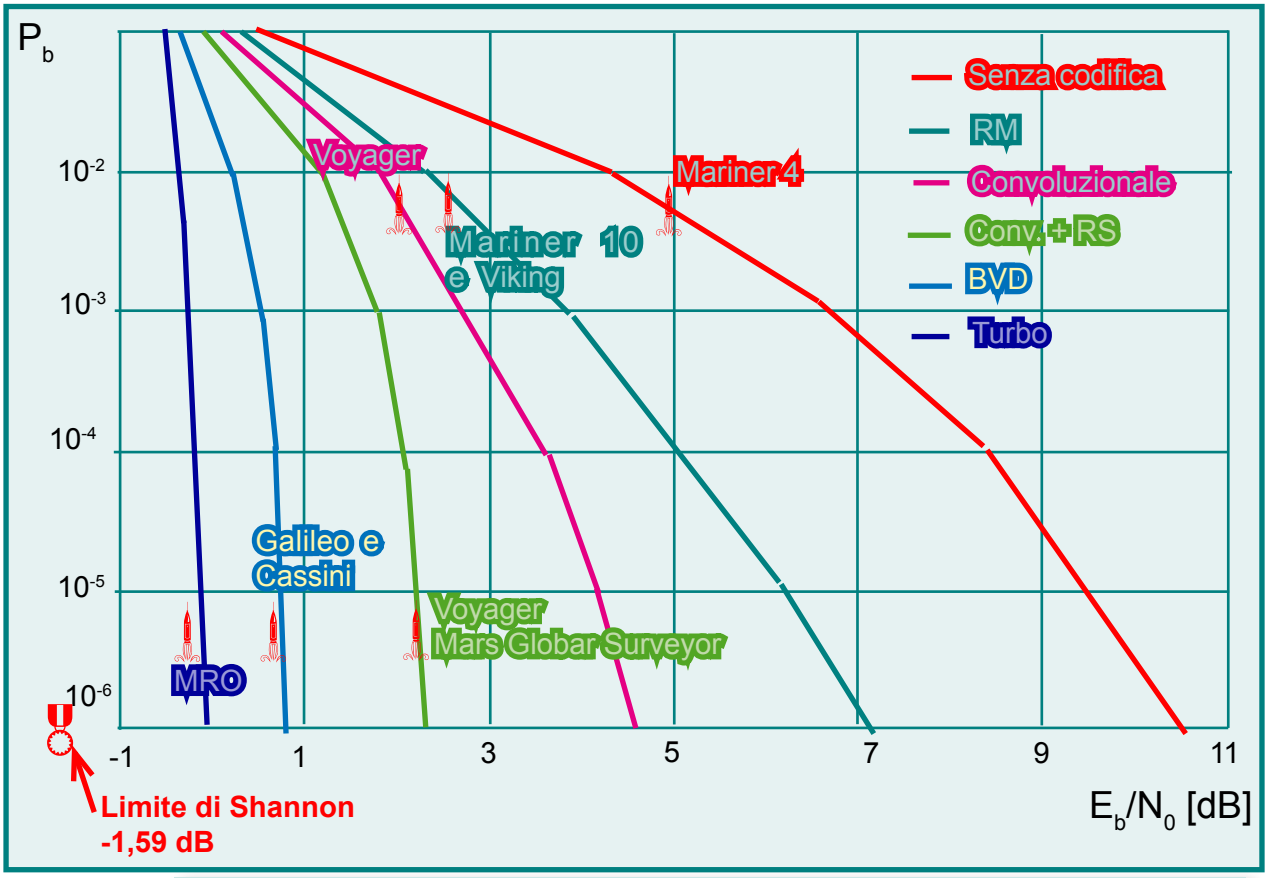


Fig. 2 - Le sonde Mariner 2,4, 5 non utilizzarono codifica per la protezione dagli errori. Mariner 6,7,9 10 e Viking utilizzarono il codice RM(32,6). Voyager 1 e 2, Magellan, Mars Global Surveyor utilizzarono il codice convoluzionale R=1/2, L=7 con decodifica di Viterbi. Galileo, Mars Pathfinder, Cassini e Mars Exploration Rover utilizzano il codice convoluzionale con L=15 e Big Viterbi Decoding. Messenger to Mercury e Mars Reconnaisance Orbiter utilizzano il turbo codice (8920, 1/6).

5. 1993: i codici mettono il turbo

Proprio nell'anno in cui lo schema basato su codice convoluzionale e codici RS raggiungeva il suo massimo (BVD), si verifica un evento [14] che dà un significativo impulso nella realizzazione di schemi di codifica che approssimano il limite di Sannon: i turbo-codici.

Claude Berrou, un fisico professore di progettazione VLSI, interessato alla integrazione dell'algoritmo di Viterbi con decodifica iterativa, ipotizza che sia possibile migliorare la decodifica utilizzando un sistema a retroazione, con decodifiche ripetitive. Da qui il nome assegnato a questi codici: il decodificatore ottiene risultati sorprendenti utilizzando una retroazione (*feedback*), così come il motore turbo migliora le prestazioni riutilizzando parte dei gas di scarico.

I risultati delle simulazioni riportati dagli autori indicano come il limite di Shannon possa essere approssimato, con una differenza inferiore a 0,7 dB. Inizialmente tali risultati sono considerati con scetticismo, ma presto altri ricercatori ottengono risultati simili, e verificano che le prestazioni dei turbo codici dipendono dalla dimensione del codice *n* e dal fattore di *interleaving*: come aveva già indicato Elias nel 1954, le prestazioni del codice crescono al crescere della dimensione del blocco.

La prima missione spaziale a utilizzare il nuovo schema raccomandato dalla CCSDS basato su turbo codice è del 2005, il MRO (figura 2).

6. Codici e diffusione delle informazioni televisive

Ovviamente non sono solo le missioni spaziali a trarre vantaggio dai progressi nella codifica per la protezione dagli errori.

Nell'ambito televisivo e multimediale possiamo ricordare che il codice di Hamming è utilizzato nei servizi teletext (in Italia Televideo) introdotti negli anni '70. E' del 1982 la definizione del formato del CD, seguita da quella del DVD nel 1996: entrambi i formati utilizzano due codici RS, in uno schema di codifica a prodotto.

I sistemi digitali di diffusione televisiva da satellite sono stati resi possibile fin dall'origine dall'impiego di schemi sofisticati di protezione dagli errori. Infatti i sistemi di compressione delle informazioni video e audio, riducendo al minimo la ridondanza e non prevedendo la ritrasmissione dei messaggi in caso di errori, richiedono che la probabilità di errore per il flusso di dati ricevuti sia molto bassa, dell'ordine di 10^{-9}.

Gia nel primo esperimento, in occasione dei campionati mondiali di Italia '90, di trasmissione del segnale in Alta Definizione si utilizzò uno schema di codifica basato su codice esterno RS(255,239) e interno convoluzionale. Il bit rate complessivo, di poco inferiore a 70 Mbit/s, era trasmesso utilizzando una coppia di trasponder del satellite Olympus, essendo la capacità massima dei modulatori e del canale costituito da ciascun trasponder di circa 34 Mbit/s.

Lo standard DVB-S (1996) adotta uno schema basato su codice esterno accorciato RS(204,108) seguito da interleaver con profondità 12 e codice interno convoluzionale R=1/2, L=7.

Gli standard DVB-RCS e DVB-RCT adottano turbo codici.

E il DVB-S2, lo standard di seconda generazione per la diffusione da satellite, adotta uno schema di protezione basato sui codici LDPC.

7. Oggi: il ritorno dei codici LDPC

Dopo il 1993, a seguito dell'avvento dei turbo codici, molti ricercatori riprendono in considerazione anche schemi di codifica le cui prestazioni non erano state nel passato considerate soddisfacenti, a causa dei vincoli in termini di complessità di calcolo e capacità di memoria. In particolare l'attenzione si focalizza sui codici

proposti da Robert Gallager nel 1962 e viene dimostrato che prestazioni molto prossime al limite di Shannon possono essere raggiunte con codici LDPC di grandi dimensioni e decodifica iterativa.

Lo standard DVB-S2 (2003) adotta la concatenazione di due codici: un BCH come codice esterno e un LDPC come codice interno. Il codice LDPC utilizzato dal DVB è denominato *Extended IRA code* con una lunghezza di parola che può essere n=64800 (per le trame normali) o n=16200 (per le trame corte). Approssima il limite di Shannon entro 0,6÷0,8 dB e, con le tecniche di integrazione attuali, è di facile realizzazione [17].

Il DVB-S2 è attualmente utilizzato per la diffusione via satellite di programmi televisivi ad Alta Definizione (HDTV).

E' uno degli elementi fondamentali per la dimostrazione di trasmissione via satellite delle immagini Super Hi-Vision (SHV), che si tiene in occasione della IBC 2008 [18]. Le immagini SHV sono composte da un numero di pixel 16 volte superiore a quelle HDTV, grazie all'evoluzione dei sistemi di compressione video è possibile ridurre il bit-rate a 140 Mbit/s, che, poiché non sono attualmente disponibili demodulatori adatti a tale capacità, vengono suddivisi in due flussi da 70 Mbit/s.

Anche il sistema di diffusione terrestre di seconda generazione, il DVB-T2, adotta la codifica LDPC per la protezione dagli errori [19].

Altri standard che utilizzano questi codici sono le nuove versioni di WiMax mobile (IEEE 802.16e-2005) e WiFi (IEEE 802.11n).

7. Conclusione

Sembrerebbe quindi che i sistemi attuali raggiungano il limite indicato sessanta anni fa da Shannon e che sarà pertanto difficile assistere in futuro a progressi significativi in questo campo.

Molte delle informazioni utilizzate per la stesura di questo articolo sono tratte da [20][Nota 5], e in tale articolo si cita un Workshop, tenuto in Florida nell'aprile 1971, che è ricordato come "*la codifica è morta*", perché sembrava che nulla di nuovo potesse essere aggiunto a quanto fino allora pubblicato sul tema.

Abbiamo visto che l'avvento, del tutto imprevisto, dei turbo codici nel 1993 aprì nuove prospettive per consentire l'avvicinamento al limite di Shannon.

Da questo punto di vista può quindi risultare azzardata la conclusione in [17][Nota 6]: *"I codici LDPC di DVB-S2 approssimano il limite di Shannon a 0,6÷0,8 dB ... Può risultare difficile giustificare la loro sostituzione nei prossimi decenni a venire."*

Nota 5 - Per approfondimenti sui codici si rimanda al numero speciale "Turbo.Information Processing: Algorithms, Implementations & Applications", del giugno 2007 di Proceeding of the IEEE.
Ricchi di informazioni sono inoltre i siti delle organizzazioni ASI, ESA, NASA, CCSDS, le cui URL sono indicate nella tabella che riporta acronimi e sigle.

Nota 6 - Per quanto riguarda il DVB-S2, si rimanda a "Special Issue on The DVB-S2 Standard for Broadband Satellite Systems", guest editors
Alberto Morello and Ulrich Reimers,
Int. J. Satell. Commun. Network., vol. 22, No 3, May-June 2004.

Bibliografia

1. C. E. Shannon: “A Mathematical Theory of Communication”, The Bell System Technical Journal, vol. 27, pp. 379-423, 623-656, July, October, 1948.
2. M. J. E. Golay, “Notes on digital coding,” Proc. IRE, vol. 37, p. 657, June 1949.
3. R. W. Hamming: “Error detecting and error correting codes”, Bell Syst. Tech. J. 29:147-60,1950.
4. D. E. Muller, “Application of Boolean algebra to switching circuit design and to error detection,” IRE Trans. Electron. Comput., vol.EC-3, pp. 6–12, Sept. 1954.
5. I. S. Reed, “A class of multiple-error-correcting codes and the decoding scheme,” IRE Trans. Inform. Theory, vol. IT-4, pp. 38–49, Sept. 1954.
6. P. Elias, “Error-free coding”, IRE Trans. Inform. Theory, vol. IT-4, pp.29-37, Sept. 1954.
7. P. Elias, “Coding for noisy channels,” IRE Conv. Record, vol. 4, pp. 37–47, 1955.
8. E. Prange, “Cyclic error-correcting codes in two symbols,” Tech. Rep. TN-57-103, Air Force Cambridge Research Center, Cambridge, MA, Sept. 1957.
9. A. Hocquenghem, “Codes correcteurs d’erreurs,” Chiffres, vol. 2, pp. 147–156, 1959.
10. R. C. Bose and D. K. Ray-Chaudhuri, “On a class of error correcting binary group codes,” Information and Control, vol. 3, pp. 68–79, Mar 1960
11. I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” J. SIAM, vol. 8, pp. 300–304, June 1960.
12. R.Gallager, “Low-density parity-check codes,” IRE Trans. Information Theory, pp. 21-28, Jan. 1962.
13. A. J. Viterbi: “Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm,” IEEE Transactions on Information Theory, Volume IT-13, pages 260-269, April, 1967.
14. C. Berrou, A. Glavieux, P. Thitimasjshima: “Near Shannon limit error correcting coding and decoding: Turbo-codes”, Proc. IEEE Int. Conf. on Commun., Geneva, maggio 1993, pp. 1064-1070.
15. D.J.MacKay, R.M.Neal: “Near Shannon limit performance of low-density-parity-check codes.”, Elect. lett., vol. 32, pp. 1645-1646, August 1996.
16. A. Morello, V. Mignone: “Il sistema DVB-S2 di seconda generazione per la trasmissione via satellite e Unicast”, Elettronica e Telecomunicazioni, dicembre 2003.
17. M. Eroz, F.W. Sun, L.N. Lee: “DVB-S2 low density parity check codes with near Shannon limit performance”, Int. J. Satell. Commun. Network., vol. 22, No 3, May-June 2004.
18. A. Morello: “Super Future: DVB-S2 Enables 140 Mps Super Hi-Vision By Satellite at IBC 2008”, DVB Scene, No. 27, August 2008 (www.dvb.org)
19. N. Wells:”A Spec is Born. DVB-T2: A new Terrestrial Standard”, DVB Scene, No. 27, August 2008 (www.dvb.org)
20. G.D. Forney, D.J. Costello: “Channel Coding: The Road to Channel Capacity”, IEEE Procs, Vol. 95, Issue 6, p. 1150-1177, June 2007