La Matematica nella Società e nella Cultura

Rivista dell'Unione Matematica Italiana

Chiara Ravazzi

Analisi asintotica di codici di tipo turbo: spettri medi e distanze minime

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **5** (2012), n.1 (Fascicolo tesi di Dottorato), p. 87–90.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2012_1_5_1_87_0>

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2012.

La Matematica nella Società e nella Cultura
Rivista dell'Unione Matematica Italiana
Serie I, Vol. V, Aprile 2012, 87-90

Analisi asintotica di codici di tipo turbo: spettri medi e distanze minime

Chiara Ravazzi

1. – Introduzione

La tesi analizza le proprietà di schemi di codifica di tipo turbo. La principale motivazione dello studio affrontato proviene dalla teoria dei codici e, più precisamente, dal problema della trasmissione di dati attraverso un canale di comunicazione. La teoria dei codici studia come aggiungere ridondanza a un messaggio sorgente in modo che, corrotto dalla trasmissione su un canale rumoroso, possa essere ricostruito correttamente. Un generico schema di codifica-decodifica può essere descritto come segue

$$\begin{array}{ccccccc} \mathbb{Z}_2^k & \xrightarrow{\phi} & \mathbb{Z}_2^n & \xrightarrow{\text{canale}} & \mathcal{Y}^n & \xrightarrow{\psi} & \mathbb{Z}_2^k \\ U & \xrightarrow{\phi} & X=\phi(U) & \xrightarrow{\text{canale}} & Y & \xrightarrow{\psi} & \widehat{U}=\psi(Y) \end{array}$$

La sorgente emette un messaggio di informazione $U \in \mathbb{Z}_2^k$. Il codificatore $\phi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ con $n > k$ è un omomorfismo che associa deterministicamente a U la parola di codice $X = \phi(U)$ da spedire sul canale. A partire dall'osservazione dell'uscita Y del canale (che è l'oggetto che introduce aletorietà nel sistema), il ricevitore decodifica deterministicamente il messaggio $\widehat{U} = \psi(Y) \in \mathbb{Z}_2^n$. Il rapporto $R = k/n$ fra la dimensione e la lunghezza del codice ($\mathrm{im}(\phi)$) è detto *rate* e fornisce una misura della ridondanza introdotta. È ragionevole pensare che si possa rendere arbitrariamente piccola la probabilità di errore aumentando indefinitamente la quantità di ridondanza introdotta dalla codifica. Tuttavia incrementare la ridondanza in modo illimitato non è una scelta possibile: il trasferimento dell'informazione, per essere efficiente, non deve richiedere un tempo proibitivo. Per questo motivo trasmissioni per le quali $R \to 0$ risultano di nessun interesse applicativo. Fissato il canale, il teorema di Shannon [1] garantisce l'esistenza di una soglia $C > 0$, legata al canale, tale per cui, la probabilità di errore può essere resa piccola a piacere, purché si accettino codici di lunghezza n sempre più grande, trasmettendo ad un rate fissato $R < C$.

Fissato $R < C$, gran parte della teoria dei codici classica si concentra sulla costruzione di codici con distanza minima più grande possibile. Nel caso di codici binari lineari la distanza minima coincide con il più piccolo peso di Hamming (e.g. numero di elementi non nulli in una stringa) di una sequenza non nulla. Essa fornisce una misura della capacità di rilevazione e correzione degli errori, dal momento che parole di

codice simili nel senso di Hamming avranno, a causa degli errori introdotti dal canale, una maggiore probabilità di essere equivocate mentre parole molto diverse risulteranno difficilmente confondibili. Questo giustifica la seguente definizione. Una successione di codificatori ϕ_n di lunghezza n, dimensione k_n e distanza minima d_n si definisce *asintoticamente buona* se

$$\liminf_{n\to+\infty} k_n/n = R \qquad \liminf_{n\to+\infty} d_n/n = \delta(R) > 0$$

Se si assume una decodifica di tipo massima verosimiglianza, le prestazioni sono anche influenzate dai pesi enumerativi del codificatore. Essi specificano lo spettro del codice, cioè il numero di parole di codice con un dato peso di Hamming. I pesi enumerativi sono i principali ingredienti nella stima delle probabilità di errore e caratterizzano la capacità di correzione del codice. Infine, parte rilevante consiste nello studio delle funzioni spettrali, cioè i coefficienti di crescita esponenziale per $n \to \infty$ dei pesi enumerativi, in grado di fornire importanti informazioni asintotiche sul codice e, in particolare, sulla distanza minima.

La teoria di Shannon [1] assicura l'esistenza di codificatori asintoticamente buoni ma non fornisce tecniche costruttive nella pratica.

Se da un lato la maggior struttura algebrica permette un più efficiente processo di codifica e decodifica, dall'altro le prestazioni di codici maggiormente strutturati rimangono generalmente ben lontane da quelle promesse da Shannon.

L'introduzione nell'ultimo ventennio di schemi noti come turbo codici [2] ha permesso una rapida evoluzione nella teoria della trasmissione numerica. Il principio strutturale alla base dei turbo codici è quello di interconnettere codificatori in parallelo o in serie attraverso un permutatore. Tali schemi di codifica, combinando l'uso di codificatori semplici ma strutturati con componenti capaci di introdurre casualità, presentano prestazioni asintoticamente buone vicine al limite teorico predetto dalla teoria di Shannon. Inoltre la possibilità di utilizzare algoritmi di decodifica subottimi a bassa complessità li rende di grande interesse applicativo.

L'obiettivo della tesi è quello di andare oltre la semplice giustificazione sperimentale, fornendo una dimostrazione matematica delle ottime prestazioni che questa classe di codici propone.

2. – Schemi di codifica turbo seriale

Siano $\psi_N^{\mathrm{o}} : \mathbb{Z}_2^{kN} \to \mathbb{Z}_2^{nN}$ e $\psi_N^{\mathrm{i}} : \mathbb{Z}_2^{nN} \to \mathbb{Z}_2^{nN}$ due codificatori ottenuti dal troncamento di un codificatore convoluzionale (una mappa a stati finiti con aggiornamento lineare dell'ingresso e dell'uscita). Il codificatore turbo seriale è definito dalla composizione del codificatore esterno ψ_N^{o} con una cascata di m codificatori interni ψ_N^{i} attraverso permutazioni che agiscono sui simboli:

$$\phi_N = \psi_N^{\mathrm{i}} \circ \pi_m \circ \ldots \circ \psi_N^{\mathrm{i}} \circ \pi_1 \circ \psi_N^{\mathrm{o}} \qquad \pi_i \in S_{nN}, \forall i \in \{1, \ldots m\}$$

L'uso del metodo probabilistico per l'analisi teorica di questi codificatori è una ca-

ratteristica fondamentale. Si introduce, cioè uno spazio di probabilità che ha per elementi i codificatori (tale spazio viene chiamato *ensemble*) e si dimostra che alcune proprietà sono soddisfatte con probabilità uno da un codice campionato dall'ensemble. Nel caso di codificatori seriali si considera l'ensemble ottenuto al variare delle permutazioni possibili $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_m) \in S_{nN}^m$ e si studia la distribuzione della distanza minima di un codice estratto uniformemente dall'ensemble.

Nell'analisi della distanza minima si distinguono due linee di ricerca: in una, fissata la lunghezza di troncamento N, vengono analizzati pesi enumerativi e la distribuzione della distanza minima come funzione di m; nell'altra, fissato il numero di inteconnessioni m, si studiano le proprietà intrinseche di questi schemi di codifica in funzione della lunghezza N.

Il primo approccio [3] garantisce l'esistenza di una successione di codificatori nell'ensemble asintoticamente buoni ma non permette di dimostrare che tutti i codificatori nell'ensemble lo siano effettivamente. Questa difficoltà nasce dal fatto che i due limiti per $m \to \infty$ and $N \to \infty$ non possono essere scambiati automaticamente.

In questa tesi si persegue la seconda strategia. Il caso con $m = 1$, che include lo schema seriale classico (due codificatori convoluzionali concatenati attraverso una singola permutazione) è studiato in dettaglio in [4]. In particolare, si dimostra che questi codificatori non sono asintoticamente buoni: la distanza minima cresce solo sub-linearmente nella lunghezza N. Il caso con $m = 2$ include i codici Repeat double-Accumulate (RA^2) [4], per i quali è stato dimostrato che le distanze minime crescono linearmente nella lunghezza N con probabilità uno. Le simulazioni Monte-Carlo mostrano che per $m \geq 2$ le distanze minime crescono linearmente nella lunghezza del codice e il coefficiente di crescita lineare è molto vicino alla distanza di Gilbert-Varshamov (GV), la miglior stima dal basso (nota in letteratura) della maggior distanza minima raggiungibile da un codice di rate R. Tuttavia, rimangono ancora molte questioni aperte e la comprensione di questi fenomeni non si può considerare del tutto completa.

Come primo passo, ci concentriamo sui codificatori convoluzionali, che sono i principali componenti degli schemi turbo seriali. In particolare, la tesi presenta una analisi dettagliata dei pesi enumerativi e delle funzioni spettrali.

Il contributo è principalmente teorico. I pesi enumerativi sono espressi come coefficienti di serie formali di potenze a coefficienti non negativi. Il calcolo di tali espressioni richiede una alta complessità computazionale quando le lunghezze di troncamento N crescono. Applicando una estensione del metodo di punto di sella si dimostra che i pesi enumerativi ammettono una approssimazione accurata, che permette una valutazione numerica più efficiente. Alcuni esempi mostrano che questa approssimazione è molto precisa anche per basse lunghezze di troncamento, migliorando così le stime sui pesi enumerativi note in letteratura.

Il metodo di punto di sella è poi usato per ottenere una espressione esatta delle funzioni spettrali. Questa rappresentazione permette di dimostrare che esse sono continue, concave e derivabili nelle variabili, proprietà congetturate in letteratura ma mai provate. Le espressioni ottenute possono essere valutate solo numericamente. Tuttavia, la procedura numerica può essere migliorata usando algoritmi

standard di minimizzazione non vincolata di funzioni convesse (cfr. metodo del gradiente). Infine, si dimostra che i coefficienti di crescita esponenziale in N dei pesi enumerativi convergono uniformemente alla funzione spettrale limite quando $N \to +\infty$.

Costruendo su questi risultati, si studiano le funzioni spettrali degli spettri medi di distanze dell'ensemble turbo seriale. Il contributo consiste nel mostrare analiticamente che nel caso di concatenazioni multiple le funzioni spettrali esibiscono caratteristiche diverse rispetto al caso di una concatenazione semplice: più precisamente, se $m \geq 2$ è provata l'esistenza di una soglia $\delta_m > 0$ sotto la quale esse sono identicamente nulle. Essendo tali funzioni non negative, questo non è sufficiente a concludere che questi schemi di codifica sono asintoticamente buoni. Tuttavia, combinando la tecnica di *union bound* con l'analisi delle funzioni spettrali, si dimostra che le distanze minime presentano andamenti lineari nella lunghezza delle permutazioni e che il coefficiente di crescita lineare, per m fissato, è esattamente dato da δ_m. Infine, sotto opportune ipotesi non particolarmente restrittive sul codificatore esterno, si dimostra che le funzioni spettrali formano una sequenza di funzioni uniformemente convergente in m. La funzione limite è uguale al massimo fra zero e la funzione spettrale dell'ensemble di codificatori lineari. Come conseguenza, la successione di soglie δ_m converge alla distanza di Gilbert-Varshamov quando $m \to +\infty$.

Per dimostrare questi risultati si sfruttano strumenti di analisi combinatoria e tecniche provenienti dall'analisi non lineare. Riassumendo, i risultati ottenuti estendono e completano le analisi sviluppate in [4, 3, 5], e permettono di raggiungere una comprensione più profonda riguardo alla distribuzione della distanza minima e agli spettri medi di schemi di tipo turbo seriale.

BIBLIOGRAFIA

[1] C. E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal, **27** (1948), 379-423 and 623-656.

[2] C. Berrou, A. Glavieux e P. Thitimajshima, *Near Shannon limit error-correcting coding and decoding: Turbo codes*, Proc. IEEE Int. Conf. Commun. (ICC) (1993).

[3] H. D. Pfister e P. H. Siegel, *The serial concatenation of rate-1 codes through uniform random interleavers*, IEEE Trans. on Inform. Theory, **49** (2003), 1425-1438.

[4] L. Bazzi, M. Mahdian e A. Spielman, *The minimum distance of turbo-like codes*, IEEE Trans. on Inform. Theory, **55** (2009), 6-15.

[5] C. Ravazzi e F. Fagnani, *Spectra and minimum distances of Repeat multiple-accumulate codes*, IEEE Trans. on Inform. Theory, **55** (2009), 4905-4924.

Dipartimento di Matematica, Politecnico di Torino
e-mail: chiara.ravazzi@polito.it
Dottorato in Matematica per le Scienze dell'Ingegneria
con sede presso il Politecnico di Torino — Ciclo XXIII
Direttore di ricerca: Fabio Fagnani, Dipartimento di Matematica,
Politecnico di Torino