La Matematica nella Società e nella Cultura

Rivista dell'Unione Matematica Italiana

Federica Garin

Ensemble di codici turbo seriali generalizzati: analisi e progetto

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **2** (2009), n.2 (Fascicolo Tesi di Dottorato), p. 247–250.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2009_1_2_2_247_0>

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2009.

La Matematica nella Società e nella Cultura
Rivista dell'Unione Matematica Italiana
Serie I, Vol. II, Agosto 2009, 247-250

Ensemble di codici turbo seriali generalizzati: analisi e progetto

Federica Garin

Questa tesi si sviluppa nell'ambito della teoria dei codici moderna, e consiste nell'analisi di un'ampia classe di codici turbo seriali.

La teoria della codifica di canale riguarda tecniche per aggiungere ridondanza ad un messaggio della sorgente, per garantire un messaggio corretto al ricevitore, dopo un'opportuna decodifica, anche in presenza di rumore sul canale di comunicazione. Nel suo lavoro fondamentale [5], Shannon ha fornito una formalizzazione matematica del problema della comunicazione digitale, introducendo modelli probabilistici delle sorgenti e dei canali, e studiando sia la codifica di sorgente (compressione) che la codifica di canale (correzione di errori). Il sorprendente teorema di Shannon della codifica di canale garantisce che la probabilità di errore può essere resa arbitrariamente piccola, al prezzo di aumentare la complessità del codice. La dimostrazione di Shannon è basata sul metodo probabilistico: codici casuali hanno buone proprietà con alta probabilità. Tuttavia, i codici casuali in generale hanno una complessità intrattabile, soprattutto nella decodifica. Pertanto, per più di quarant'anni, si è sviluppata una teoria algebrica dei codici, per la creazione di codici con particolare struttura, che semplificasse la decodifica, ma le prestazioni con queste costruzioni rimanevano lontane da quelle ottimali previste da Shannon. Al contrario, due classi moderne di codici portano ad un eccellente compromesso tra prestazioni e complessità: i codici turbo, introdotti in [2], ed i codici LDPC (low-density parity check, ovvero con matrice di parità sparsa), introdotti già nel 1963 [3], ma riscoperti più di recente [4]. Le eccellenti prestazioni di queste due famiglie di codici sono dovute ad un algoritmo iterativo che riduce significativamente la complessità di decodifica, da esponenziale a lineare nella lunghezza delle parole, permettendo dunque l'uso di codici molto lunghi. La decodifica iterativa è subottima rispetto alla decodifica a massima verosimiglianza, ma permette in genere di ottenere una bassa probabilità di errore.

Le prestazioni dei codici turbo e LDPC sono state mostrate con simulazioni Monte-Carlo, ed inoltre si è sviluppata una vasta letteratura volta a fornire una spiegazione teorica di tali risultati. Tuttavia, rimangono molti problemi aperti e la teoria non si può considerare completa. Da una parte, la ricerca si può concentrare sulle proprietà intrinseche dei codici (o meglio, di famiglie di codici): la distanza minima tra coppie di parole del codice e la probabilità di errore che il codice darebbe se fosse decodificato col criterio della massima verosimiglianza. Una seconda linea di

ricerca, invece, riguarda l'algoritmo iterativo di decodifica e le sue proprietà di convergenza. In questa tesi, si considera prevalentemente il primo problema, per famiglie di codici di tipo turbo, in particolare schemi turbo seriali e loro generalizzazioni.

La maggior parte della teoria dei codici moderna riguarda codici binari. Tuttavia, in molte applicazioni, per ragioni di efficienza nell'occupazione della banda durante la trasmissione, la comunicazione usa un alfabeto non-binario. Un approccio pragmatico consiste nell'usare dei codici binari, nonostante essi siano ottimizzati per un canale diverso, ma per alcuni canali, rilevanti nelle applicazioni, quali ad esempio il canale gaussiano additivo con modulazione PSK, si possono sfruttare le simmetrie del canale per associare una struttura di gruppo all'alfabeto di ingresso del canale, e progettare codici *ad hoc*. In questa tesi si persegue questa seconda strategia, proponendo risultati per codici seriali su gruppi abeliani.

Un codificatore turbo seriale classico, binario, è la composizione di un codificatore esterno $\phi_o : \mathbb{Z}_2^{kN} \to \mathbb{Z}_2^{rN}$, un interlacciatore, cioè una permutazione $\pi \in S_{rN}$ che modifica l'ordine dei bit del codice esterno, e infine un codificatore interno $\phi_i : \mathbb{Z}_2^{rN} \to \mathbb{Z}_2^{nN}$; i codificatori esterno ed interno sono ottenuti come restrizioni di un codice convoluzionale (una funzione di trasferimento razionale, che agisce su sequenze infinite) a sequenze di lunghezza finita. Gli schemi seriali sono stati introdotti in [1], insieme ad un opportuno algoritmo iterativo di decodifica, e ad una prima analisi teorica delle prestazioni, che consiste nel separare il progetto dei codici costituenti (esterno ed interno) da quello dell'interlacciatore. La tecnica, detta dell'interlacciatore uniforme, è l'analisi di un *ensemble*, come spesso avviene in teoria dei codici: invece di studiare un singolo codice, si studia una famiglia, introducendo un'opportuna distribuzione di probabilità su di essa; in questo caso, l'*ensemble* si ottiene fissando i codificatori ϕ_o e ϕ_i, mentre l'interlacciatore Π è una variabile aleatoria uniformemente distribuita su S_{rN}; il parametro che descrive le prestazioni è la probabilità di errore, sotto l'assunzione che la decodifica sia di massima verosimiglianza, e in particolare si cerca l'andamento della probabilità di errore quando N tende a infinito e per canali con rapporto segnale-rumore sufficientemente alto. Le considerazioni riportate in [1] forniscono, sia pure senza una dimostrazione formalmente rigorosa, l'andamento della probabilità di errore media per questo *ensemble*: un decadimento polinomiale del tipo C/N^{μ}, con un esponente $\mu = \lfloor (d_f^o - 1)/2 \rfloor$, dove d_f^o è la distanza libera del codice esterno, cioè il più piccolo peso di Hamming (numero di elementi diversi da zero) tra le parole di codice non nulle.

In questa tesi, questo risultato è dimostrato rigorosamente, in un contesto più generale di codici su gruppi abeliani per trasmissione su canali simmetrici.

In un codificatore turbo seriale generalizzato i due codificatori costituenti sono ottenuti per restrizione a sequenze finite di un codificatore convoluzionale su un gruppo abeliano, mentre l'interlacciatore è una permutazione, o più in generale, è

l'azione di un gruppo sul codice esterno, che soddisfi alcune proprietà che sostanzialmente garantiscono un numero di invarianti finito anche al crescere di N; quest'estensione permette ad esempio di considerare sottogruppi di permutazioni. Si suppone che il canale goda di simmetrie che rispecchiano la struttura del gruppo, ad esempio il canale gaussiano con modulazione m-PSK è simmetrico rispetto al gruppo $\mathbb{Z}_m$.

Per questo *ensemble* generalizzato, sotto opportune ipotesi sui codificatori (non catastroficità, ricorsività) si è dimostrato che, al crescere della lunghezza delle parole, la probabilità di errore media decade polinomialmente: $P(e) \asymp N^{-\mu}$ per $N \to \infty$, dove μ è caratterizzato come soluzione di un problema di ottimizzazione intera che coinvolge gli eventi di errore dei codificatori costituenti, e soddisfa le disuguaglianze $\lfloor (d_f^o - 1)/2 \rfloor \leq \mu \leq d_f^o - 1$. La caratterizzazione di μ richiede di definire un'opportuna distanza, che dipende dal canale considerato (ad esempio, distanza euclidea per il canale gaussiano), mentre il calcolo della distanza libera d_f^o considera semplicemente il peso di Hamming, cioè il numero di elementi non-nulli.

Un secondo risultato della tesi riguarda un'analisi più approfondita dello schema turbo seriale classico. In questo caso più semplice, si è cercato un risultato probabilistico più raffinato dell'andamento medio: si è trovato l'andamento tipico, seguendo un approccio che è classico in teoria dell'informazione e nella letteratura sui codici LDPC (ad esempio [3]), ma è completamente nuovo per i codici di tipo turbo. Si è trovato che l'andamento medio è fortemente influenzato da una piccola frazione di codici pessimi, mentre la tipica successione di codici di lunghezza crescente ha un comportamento molto migliore: la probabilità di errore media decade polinomialmente in $1/N$, mentre l'andamento tipico è approssimativamente $\exp(-N^{\beta})$, $0 < \beta < 1$. La presenza di un comportamento tipico lontano da quello medio è diverso dai risultati classici per altri *ensemble* di codici, in cui si osservavano fenomeni di concentrazione intorno alla media.

Più precisamente, se si considera una successione di interlacciatori $\{\Pi_N\}$ indipendenti, uniformemente distribuiti su S_{rN}, e si considerano le variabili aleatorie $X_N = \log(-\log(P(e)|\Pi_N))/\log N$, sotto alcune ipotesi sui codificatori costituenti e sul canale, esiste $\beta \in (0,1)$ tale che X_N converge a β in probabilità. Inoltre, si ottiene il curioso risultato che, quasi certamente, la successione X_N assume tutti i valori di un insieme denso nell'intervallo $[\alpha, \beta]$, per un opportuno $\alpha \in (0, \beta)$. I parametri α e β sono funzioni crescenti della distanza libera d_f^o, che è quindi confermata come il principale parametro di progetto del codificatore esterno.

Una versione più raffinata dei due risultati precedenti (l'andamento medio e tipico dell'*ensemble* seriale con interlacciatore uniforme) nel caso binario permette di evidenziare anche un parametro di progetto per il codificatore interno: la distanza libera effettiva, ovvero il più piccolo peso di Hamming tra le parole ottenute restringendo l'ingresso a parole di peso di Hamming due.

Infine, si è considerata una diversa classe di codici binari che rientrano nello schema seriale generalizzato proposto in questa tesi e che possono essere visti anche come particolari codici LDPC strutturati, che generalizzano i cosiddetti codici Repeat-Accumulate. Più in dettaglio, il codificatore esterno è un semplice codice di ripetizione, mentre il codificatore interno è a sua volta la composizione di un sommatore (somma modulo due blocchetti di bit consecutivi) e di un codice convoluzionale; la non iniettività del sommatore è compensata dalla trasmissione anche dei bit di ingresso non codificati (bit sistematici), garantendo una non-catastroficità generalizzata dello schema. L'andamento medio della probabilità di errore segue dal risultato generale, ma per permettere di trovare un parametro di progetto del codificatore interno si propone di considerare anche un particolare sotto-*ensemble*, per il quale si fornisce un risultato più fine. Inoltre si paragona l'andamento teorico, valido sotto l'ipotesi che la decodifica sia a massima verosimiglianza, con quello di simulazioni Monte-Carlo che usano un algoritmo di tipo iterativo. Per la decodifica iterativa, non è possibile usare direttamente l'algoritmo adatto ai codici turbo seriali, a causa della non-iniettività del codificatore interno; è invece possibile usare l'algoritmo di *belief propagation* solitamente usato per i codici LDPC. Si nota però che la presenza di molti cicli nel grafo associato a tale algoritmo, dovuta alla parte strutturata di questi codici, deteriora le prestazioni. Pertanto, si propone una variante a tale algoritmo, che consiste sostanzialmente nel raggruppare blocchi di vertici del grafo a cui associare variabili non-binarie, e per questo algoritmo si propone un'analisi con la tecnica della cosiddetta *density evolution*. Infine, dai risultati teorici e dalle simulazioni, si forniscono suggerimenti per il progetto di codici all'interno di questa famiglia.

BIBLIOGRAFIA

[1] Benedetto S., Divsalar D., Montorsi G. e Pollara F., *Serial Concatenation of Interleaved Codes: Performance Analysis, Design and Iterative Decoding*, IEEE Transactions on Information Theory, **44** (1998), 909-926.

[2] Berrou C., Glavieux C. e Thitimajshima P., *Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes*, ICC'93 (Ginevra, Svizzera, 1993), 1064-1070.

[3] Gallager R.G., *Low Density Parity Check Codes*, MIT Press, Cambridge, MA (1963).

[4] MacKay D. J. C. e Neal R.M., *Good Codes Based on Very Sparse Matrices*, Cryptography and Coding. 5th IMA Conf. (Cirencester, UK, 1995), 100-111.

[5] Shannon C.E., *A mathematical theory of communication*, Bell Systems Technical Journal, **27** (1948), 379-423 and 623-656.

Dipartimento di Elettronica e Informatica, Università di Padova
e-mail: garin@dei.unipd.it
Dottorato in Matematica per le Scienze dell'Ingegneria
con sede presso il Politecnico di Torino – Ciclo XX
Direttore di ricerca: prof. Fabio Fagnani, Dipartimento di Matematica, Politecnico di Torino