La Matematica nella Società e nella Cultura

Rivista dell'Unione Matematica Italiana

Giacomo Como

Ensemble di codici su gruppi abeliani

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **2** (2009), n.2 (Fascicolo Tesi di Dottorato), p. 227–230.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2009_1_2_2_227_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, 227-230

Ensemble di codici su gruppi abeliani

GIACOMO COMO

Nell'ambito della trasmissione su canali rumorosi, i codici su gruppi consentono di utilizzare costellazioni di segnali ad alta effcienza spettrale ed ereditano molte delle proprietà strutturali dei codici lineari binari. In questa tesi vengono studiati i limiti fondamentali, dal punto di vista della teoria dell'informazione, dei codici su gruppi abeliani, e le prestazioni dei codici a bassa densità su gruppi abeliani.

1. – Introduzione

Questa tesi verte sull'analisi ed il progetto di codici di trasmissione con struttura di gruppo abeliano. La principale motivazione tecnologica proviene dall'ingegneria delle telecomunicazioni, e, più precisamente, dal problema della trasmissione di dati digitali su canali rumorosi a banda limitata. Si tratta di un problema classico della teoria dell'informazione, che risale al lavoro originale di C.E. Shannon del 1948 [7]. Shannon dimostrò che ogni canale rumoroso è caratterizzato da una soglia C, detta capacità del canale: è possibile trasmettere in maniera affidabile ad ogni rate inferiore a C, mentre la trasmissione a rate maggiore di C è necessariamente inaffidabile. Per circa cinquanta anni i limiti predetti dalla teoria di Shannon sono rimasti irragiungibili nella pratica delle telecomunicazioni: solo verso la metà degli anni '90, con l'invenzione dei codici turbo e la riscoperta dei codici a bassa densità, è stato possibile progettare ed implementare sistemi di trasmissione pratici che raggiungessero tali limiti teorici. Sia i sistemi di trasmissione turbo, che quelli a bassa densità, sono basati su codici lineari binari che ammettono rappresentazione grafica sparsa: tale rappresentazione consente l'efficace applicazione di algoritmi iterativi di decodifica a bassa complessità. In particolare, i codici a bassa densità sono codici lineari binari che possono essere rappresentati come spettri di matrici binarie sparse, cioè contenenti un basso numero di elementi non nulli.

L'uso del metodo probabilistico è una caratteristica fondamentale della teoria dell'informazione sin dai suoi albori. Per dimostrare l'esistenza di un codice con determinate caratteristiche, si considera uno spazio di probabilità che ha per elementi codici (tale spazio viene chiamato *ensemble* di codici), e si dimostra che la proprietà desiderata è soddisfatta con probabilità non nulla da un codice campionato dell'*ensemble*. Non soltanto il metodo probabilistico costituisce una potente tecnica dimostrativa, ma, nella moderna teoria dei codici, esso fornisce altresí uno strumento

fondamentale per il progetto. Infatti, se un *ensemble* di codici soddisfa una determinata proprietà con alta probabilità, allora un efficace metodo di progetto consiste semplicemente nel generare un codice a caso dall'*ensemble* stesso.

Dato un gruppo finito G, i codici su G sono sottogruppi del gruppo prodotto G^n. Furono introdotti da D. Slepian negli anni '60 [8]: permottono di usare costellazioni di segnali geometricamente uniformi ad alta efficienza, ed ereditano le buone proprietà strutturali dei codici lineari binari. Questa tesi presenta una teoria dei codici a bassa densità su gruppi abeliani. Nella prima parte vengono analizzate le proprietà fondamentali dei codici su gruppi abeliani, senza vincoli di densità: tale analisi è propedeutica allo studio dei codici su gruppi a bassa densità perché permette di distinguere i limiti alle prestazioni indotti dalla struttura algebrica da quelli indotti dal vincolo di sparsità della rappresentazione grafica. I due risultati principali di questa parte consistono nella caratterizzazione della capacità raggiungibile dai codici su gruppi abeliani, e nello studio delle distanze minime e degli esponenti di errore tipici degli *ensemble* di codici su gruppi abeliani. Nella seconda parte della tesi, vengono studiate le proprietà strutturali dei codici a bassa densità su gruppi abeliani, ed in particolare i loro spettri medi di distanze.

2. – Capacità dei codici su gruppi abeliani

Per gruppi abeliani G isomorfi al gruppo additivo di un campo di Galois, risultati classici della teoria dell'informazione mostrano che i codici su G sono sufficienti a raggiungere la capacità di Shannon e l'esponente di errore medio su canali di trasmissione simmetrici senza memoria. Una congettura di Loeliger [6] del '91 ipotizzava che il risultato dovesse continuare a valere per codici su gruppi ciclici per certe costellazioni di segnali note come 'PSK'. Nella tesi, la congettura di Loeliger viene dimostrata. Più in generale, si fornisce una caratterizzazione generale della capacità raggiungibile da codici su gruppi abeliani G arbitrari. Viene mostrato come, per particolari costellazioni di segnali geometricamente uniformi, i codici su grupi abeliani non permettono di raggiungere la capacità di Shannon. Viene anche analizzato l'esponente di errore medio degli *ensemble* di codici su grupi abeliani; confermando una congettura di Dobrushin [4], viene dimostrato che – anche quando suffcienti a raggiungere la capacità di Shannon – gli *ensemble* di codici su gruppi abeliani non isomorfi al gruppo additivo di un campo di Galois non raggiungono l'esponente di errore medio del canale. Questi risultati sono stati pubblicati in [2].

3. – Distanze minime ed esponenti di errore tipici dei codici su gruppi abeliani

Oltre alla questione della capacità, una domanda fondamentale è se, dato un canale di trasmissione con determinate simmetrie, il progetto di codici che tengano conto di tali simmetrie possa o meno garantire migliori prestazioni. I risultati della

sezione precedente sembrerebbero suggerire una risposta negativa, dal momento che, anche nei casi in cui i codici su un gruppo abeliano G permettono di raggiungere la capacità di Shannon, gli *ensemble* di codici su G presentano esponenti di errore medi inferiori a quelli dell'*ensemble* di tutti i codici. Nella tesi viene dimostrato che questa conclusione è fuorviante, in quanto tali risultati si riferiscono al codice medio, piuttosto che a quello tipico. L'analisi delle distanze minime e degli esponenti di errore proposta, dimostra infatti che, almeno per canali PSK, i G-codici tipici hanno prestazioni superiori a quelle del tipico codice senza struttura algebrica: i primi raggiungono asintoticamente con probabilità uno il 'Gilbert-Varshamov bound' sulla distanza minima e 'l'esponente di errore espurgato' (che molti teorici dell'informazione congetturano essere i limiti ultimi delle prestazioni dei codici su un dato canale), mentre i secondi no. Questi risultati sono alla base della pubblicazione [3].

4. – Codici a bassa densità su gruppi abeliani

I codici a bassa densità binari, inventati da Gallager nel '60 [5] e riscoperti a metà degli anni '90, sono sottospazi lineari di Z_2^n che possono essere rappresentati come nuclei di matrici sparse. Gallager introdusse anche i codici a bassa densità su un generico gruppo abeliano G, come nuclei di omomorfismi di dominio G^n che ammettono una rappresentazione grafica sparsa. Il modo standard di costruire *ensemble* codici a bassa densità su G consiste nel generare un ipergrafo regolare casuale con n nodi di un dato grado c, e $l = nc/d$ iperlati di grado d, e nell'associare ad ogni iperlato un omomorfismo casuale da G^d in G. La bassa densità viene poi garantita asintoticamente, considerando il limite per n ed l crescenti, con c e d fissati. Mentre i criteri di ottimizzazione dei gradi c e d sono stati ampiamente studiati per i codici a bassa densità binari, il modo di associare gli omomorfismi agli iperlati è un parametro di progetto peculiare dei codici su gruppi non binari.

Nella seconda parte della tesi, vengono studiate le proprietà strutturali di diversi *ensemble* di codici a bassa densità regolari su gruppi abeliani non binari. In tali *ensemble*, gli automorfismi locali sono scelti con probabilità uniforme su un generico sottogruppo F del gruppo degli automorfismi di G. I casi estremi sono F costituito dalla sola identità, e F coincidente con l'intero gruppo degli automorfismi di G. Per generici G e F, vengono trovate formule esplicite per il calcolo del coefficiente di crescita esponenziale della funzione enumeratrice dei tipi media. Vengono inoltre dimostrate delle stime asintotiche sul coefficiente di crescita lineare delle distanze di Hamming tipiche. Tali risultati permettono di ottimizzare F dato G, ed in particolare viene mostrato come la scelta di F coincidente con il gruppo completo degli automorfismo di G permetta in generale di ottenere prestazioni superiori al caso di F coincidente con la sola identità. Questi risultati sono stati pubblicati in [1].

BIBLIOGRAFIA

[1] Como G. e Fagnani F., *Average spectra and minimum distances of low-density parity-check codes over Abelian groups*, SIAM Journal on Discrete Mathematics, **23** (1) (2008), 19-53.

[2] Como G. e Fagnani F., *The capacity of finite Abelian group codes over memoryless symmetric channels*, IEEE Transctions on Information Theory, **55** (5) (2009), 2037-2054.

[3] Como G., *Group codes outperform binary coset codes on non-binary symmetric memoryless channels*, IEEE Transctions on Information Theory, **submitted** (2008).

[4] Dobrushin L.R., *Asymptotic optimality of group and systematic codes for some channels*, Theory of Probability and its Applications, 8 (1963), 47-59.

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

[6] Loeliger H.-A., *Signal sets matched to groups*, IEEE Transctions on Information Theory, **37** (6) (1991), 1675-1679.

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

[8] Slepian D., *Group codes for the Gaussian channel*, Bell Systems Technical Journal, **47** (1968), 507-602.

LIDS, MIT – Cambridge, MA (USA)
e-mail: giacomo@mit.edu
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