La Matematica nella Società e nella Cultura

Rivista dell'Unione Matematica Italiana

Laura Luzzi

Frazioni continue e codici per le comunicazioni wireless

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **1** (2008), n.2 (Fascicolo Tesi di Dottorato), p. 291–294.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2008_1_1_2_291_0>

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2008.

La Matematica nella Società e nella Cultura
Rivista dell'Unione Matematica Italiana
Serie I, Vol. I, Agosto 2008, 291-294

Frazioni continue e codici per le comunicazioni wireless

Laura Luzzi

Le frazioni continue erano oggetto di studio in matematica molto prima che si sviluppasse la moderna teoria dei sistemi dinamici, e sono tra i pochi modelli per cui si ha un'analisi statistica soddisfacente (ergodicità, misure invarianti, decadimento delle funzioni di correlazione).

L'interesse per questo modello non è limitato al campo dei sistemi dinamici, ma si estende alla teoria dei numeri, alla teoria dell'informazione e all'algoritmica.

Gli sviluppi in frazione continua forniscono una rappresentazione dei numeri reali particolarmente vantaggiosa per lo studio dei problemi di approssimazione diofantea. Essa è più concisa dello sviluppo decimale e non dipende dalla scelta di una base, tuttavia ha il grande svantaggio di essere poco adatta al calcolo: persino operazioni come la somma e il prodotto diventano complesse in questa rappresentazione. Probabilmente per questo motivo, gli esempi di applicazioni delle frazioni continue all'ingegneria sono piuttosto rari.

Recentemente, si assiste ad un interesse crescente nello studio del comportamento di famiglie di sistemi dinamici alla frontiera della caoticità (per citare solo uno degli esempi più noti, ricordiamo l'analisi dettagliata delle biforcazioni della mappa logistica). In questo contesto emergono spesso fenomeni quali transizioni di fase, autosimilarità e insiemi frattali.

La prima parte del mio lavoro di ricerca riguarda le α-frazioni continue per $\alpha \in [0,1]$, una famiglia ad un parametro di trasformazioni dell'intervallo che danno origine ad una classe di sviluppi in frazione continua. Così come le frazioni continue nel caso classico sono un'accelerazione dell'algoritmo di divisione euclidea, le α-frazioni continue si ottengono imponendo la condizione che il resto della divisione euclidea appartenga all'intervallo $[\alpha - 1, \alpha)$.

Questa prospettiva più ampia permette di studiare il passaggio dall'algoritmo classico di Gauss ($\alpha = 1$) allo sviluppo basato sull'approssimazione "all'intero più vicino" $\left(\alpha = \frac{1}{2}\right)$, che converge più rapidamente e ha entropia maggiore. Il caso $\alpha = 0$, corrispondente all'"approssimazione per eccesso", presenta proprietà differenti dovute alla comparsa di un punto fisso parabolico: in particolare il sistema non ammette una misura invariante finita, e l'algoritmo associato è più lento.

Risulta quindi naturale esaminare come avvenga questa transizione, in particolare studiando la *stabilità statistica* della famiglia delle densità invarianti in funzione

del parametro a. Nella sezione §2.1 viene mostrato che questa famiglia è continua nella norma L^1.

A partire dall'espressione delle densità, è possibile calcolare l'entropia $h(a)$ del sistema, che fornisce informazioni sulla complessità dell'algoritmo corrispondente ([1]), e sul suo tasso di creazione di informazione [1].

Purtroppo non è noto alcun algoritmo per determinare le densità invarianti. Un approccio generale, introdotto da Rohlin e detto *metodo dell'Estensione Naturale*, consiste nel trovare un'applicazione bidimensionale $\overline{T}$ di cui la mappa iniziale T è un fattore, e un dominio opportuno su cui $\overline{T}$ risulta biunivoca. La densità di T si può quindi ricavare dalla densità di $\overline{T}$ semplicemente per proiezione.

Uno dei risultati principali del lavoro di tesi è l'espressione delle estensioni naturali per la successione $a = \dfrac{1}{n}$. La forma del dominio dell'estensione naturale in questo caso è più complessa del previsto, e la densità si può esprimere solo con una formula ricorsiva. Il risultato sulla continuità L^1 delle densità mi ha permesso inoltre di dimostrare una congettura di Cassa che afferma che l'entropia tende a 0 per $a \to 0$.

Il nostro studio numerico della funzione entropia ha evidenziato una struttura autosimilare sorprendentemente ricca, simile ad una scala di Cantor, che rimane inspiegata. In particolare, contrariamente alle aspettative l'entropia non sembra monotona in alcun intorno dell'origine. I risultati numerici suggeriscono la presenza di infinite transizioni di fase (punti di discontinuità di $h'(a)$), oltre alla discontinuità ben nota in corrispondenza del numero d'oro.

La seconda parte del lavoro di tesi ha preso l'avvio dallo studio di alcune applicazioni recenti delle frazioni continue alla costruzione di codici "spazio-tempo" per un canale wireless.

La crescente diffusione delle comunicazioni wireless ha portato alla necessità di sviluppare nuovi sistemi di codifica per migliorare le prestazioni in presenza di effetti di *fading*. Con questo termine si indicano perturbazioni e attenuazioni del segnale dipendenti dalle condizioni ambientali, che causano una perdita di capacità rispetto al modello classico del canale gaussiano. L'uso di più antenne in trasmissione e in ricezione con una codifica appropriata permette di compensare questi effetti senza aumentare la potenza totale trasmessa, aumentando il numero di percorsi indipendenti di trasmissione-ricezione (detto *diversità* del sistema).

Per un canale MIMO con M antenne in trasmissione ed N in ricezione, il vettore di informazione u è codificato in un "blocco spazio-tempo", cioè una matrice $M \times T$ $B(u) = (b_{ij})$, dove b_{ij} è il segnale emesso dall'antenna i all'istante $j \in \{1, \dots, T\}$, e T è la durata del segnale.

([1]) Più precisamente, per $a \in (0, 1]$ la lunghezza media dello sviluppo in frazione continua di un numero razionale $\dfrac{p}{q}$ è $h(a) \log(q)$; per $a = 0$ la complessità è dell'ordine di $\log^2(q)$, vedi [4].

Il tasso di informazione massimo che si può ottenere usando blocchi spazio-tempo è di $\min(M,N)$ simboli per utilizzo del canale; la diversità è uguale a MR, dove R è il minimo rango delle matrici $B(u)$, e dev'essere massimizzata. Nel caso di diversità massima, il termine dominante nella stima dell'"union bound " per la probabilità di errore è il *coding gain* $\Delta^{\frac{1}{M}}$, dove $\Delta = \min_u (B(u)B(u)^H)$.

Nell'articolo [3], il problema di massimizzare il coding gain per una classe di codici MIMO di rango massimo detti *Threaded Algebraic Space-Time Codes* o TAST viene ricondotto ad un problema di approssimazione diofantea di numeri complessi con numeri algebrici. Una generalizzazione del Teorema di Liouville permette di stimare le prestazioni di questi codici. In particolare, la scelta dei parametri di codifica si basa sulla ricerca di opportuni numeri algebrici che siano "mal approssimabili" con dei razionali, cioè tali che gli elementi del loro sviluppo in frazione continua siano piccoli. In effetti,

> "La progettazione di codici spazio-tempo si può interpretare come ricerca di numeri irrazionali che siano "il più lontano possibile" dalle approssimazioni razionali. D'altronde, il processo di decodifica consiste nel cercare i razionali più vicini a dei numeri irrazionali dati; e entrambi, codifica e decodifica, sono legati allo stesso algoritmo di ricerca di vettori non nulli in un reticolo fissato (la Decodifica Sferica)." [3]

I codici TAST garantiscono diversità massima; tuttavia, il loro determinante minimo, corrispondente al coding gain, tende a zero quando la cardinalità della costellazione di segnali tende all'infinito. Un nuovo tipo di costruzioni, basate sulle algebre di divisione, ha permesso di risolvere questo problema: l'insieme dei determinanti risulta discreto perchè coincide con l'insieme delle norme ridotte in un ordine massimale.

Nel caso 2×2, il miglior codice noto attualmente è il *Golden Code* $\mathcal{G}$ [2], che si basa su un'algebra di quaternioni contenente il campo di numeri $\mathbb{Q}(i,\theta)$, dove θ indica il numero d'oro. Questo codice ha rango e tasso di trasmissione massimi, e la forma cubica del reticolo corrispondente ai segnali codificati è particolarmente efficiente sia dal punto di vista energetico che per quanto riguarda la complessità di decodifica. Nel lavoro di tesi mi sono interessata al problema di costruire codici con un buon rendimento nel caso di un canale *slow fading*. Quando il canale varia così lentamente da potersi considerare costante per un certo intervallo di tempo L, l'ipotesi di ergodicità non è più valida e le prestazioni del Golden Code peggiorano.

Per far fronte a questo problema, si possono considerare codici a blocchi di dimensioni $2 \times 2L$ basati sul Golden Code. Ogni parola di codice è della forma $\mathbf{X} = (X_1, \ldots, X_L)$, con $X_i \in \mathcal{G}$. Nell'espressione del determinante minimo del codice compaiono non solo i determinanti delle componenti X_i, ma anche termini misti della forma $\|\widetilde{X}_i X_j\|_F^2$, dove $X \to \widetilde{X}$ è un'involuzione, e $\| \ \|_F$ indica la norma di Frobenius. Perciò l'analisi della struttura additiva del codice non è sufficiente per ottenere una buona stima del coding gain.

Nella sezione § 6.5 ho considerato dei codici a blocchi basati sul quoziente di $\mathcal{G}$ per un ideale sinistro di indice 4. In questo caso particolarmente semplice, i termini misti nell'espressione del determinante minimo si possono calcolare direttamente, almeno per piccoli valori di L. Nel caso di ideali di indice maggiore, l'approccio basato sul calcolo diretto dei pesi delle parole di codice è troppo complesso. Usando ideali bilateri si possono ottenere stime globali, poichè essi sono invarianti sia rispetto alla moltiplicazione che all'involuzione. Inoltre è preferibile scegliere ideali il cui indice è una potenza di due, in modo da ottenere una partizione binaria.

Nella sezione § 6.6.2, ho descritto la struttura degli ideali bilateri di $\mathcal{G}$ il cui indice è una potenza di due e dei rispettivi quozienti, che risultano essere anelli di matrici su $\mathbb{F}_{2^n} + u\mathbb{F}_{2^n}$. In un primo tempo ho considerato dei semplici "codici di ripetizione" sull'anello quoziente; le simulazioni numeriche per la catena di trasmissione per questi codici evidenziano una migliore prestazione rispetto al caso del Golden Code "non codificato", confermando le stime per i termini misti.

Nella sezione § 6.8 ho considerato uno schema combinato di "modulazione codificata": un codice interno (il Golden Code) garantisce la diversità massima, mentre un codice correttore di errori esterno sul quoziente $\mathcal{G}/2\mathcal{G}$ (nel nostro caso un codice di Reed-Solomon) permette di aumentare la distanza minima di Hamming. Le simulazioni numeriche mostrano che nel caso di costellazioni 4-QAM, corrispondenti ad un solo segnale per ogni laterale di $\mathcal{G}/2\mathcal{G}$, questo schema migliora notevolmente il rendimento del Golden Code alla stessa efficacia spettrale, cioè con lo stesso tasso di informazione per ogni utilizzo del canale. La costruzione si può estendere al caso della modulazione 16-QAM, anche se il guadagno in questo caso è minore, essendo limitato dal determinante minimo dell'ideale.

BIBLIOGRAFIA

[1] J. Bourdon, B. Daireaux, B. Vallée, *Dynamical analysis of α-Euclidean algorithms,* J. Algorithms, **44** (2002), 246-285.

[2] J-C. Belfiore, G. Rekaya, E. Viterbo, *The Golden Code: a* 2×2 *full-rate Space-Time Code with non-vanishing determinants,* IEEE Trans. Inform. Theory, **51**, n. 4 (2005), 1432-1436.

[3] M. Damen, A. Tewfik, J-C. Belfiore, *A construction of a space-time code based on number theory,* IEEE Trans. Inform. Theory, **48**, n. 3 (2002).

[4] B. Vallée, *Dynamical analysis of a class of Euclidean algorithms,* Theoret. Comput. Sci., **297** (2003), 447-486.

Département Communications et Electronique,
École Nationale Supérieure des Télécommunications, Paris
e-mail: luzzi@telecom-paristech.fr
Perfezionamento in Matematica per la Tecnologia e l'Industria
(sede amministrativa: Scuola Normale Superiore di Pisa)
Direttore di ricerca: Prof. Stefano Marmi, Scuola Normale Superiore di Pisa
Correlatore: Prof. Emanuele Viterbo, Università della Calabria