Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Massimiliano Sala

Su alcuni metodi algebrici per la teoria dei codici a correzione d'errore

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **4-A**—*La Matematica nella Società e nella Cultura* (2001), n.3 (Fascicolo Tesi di Dottorato), p. 539–541.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2001_8_4A_3_539_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2001.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. IV-A, Dicembre 2001, 539-541

Su alcuni metodi algebrici per la teoria dei codici a correzione d'errore.

Massimiliano Sala

La Teoria dei Codici a Correzione d'Errore ([3]) costituisce un campo di ricerca in continua espansione, su cui si basano numerose applicazioni (telecomunicazioni, wireless, segnalazione ferroviaria, etc.) e che trae beneficio da nuovi approcci teorici, particolarmente fecondi.

I codici più usati oggigiorno sono i codici lineari a blocchi, tra cui emergono per importanza i codici ciclici. Per studiare tali codici sono state sviluppate molte tecniche, specialmente partendo da risultati algebrici sui campi finiti, sia tramite la teoria dei campi di Galois che tramite risultati di Geometria Algebrica. Recentemente sono stati proposti anche degli approcci completamente diversi, tra cui l'uso di trasformate di Fourier discrete, l'implementazione di problemi di programmazione lineare e il calcolo di basi di Gröbner.

I parametri più importanti per un codice sono la distanza di Hamming e la distribuzione dei pesi:

- la distanza di Hamming è direttamente correlata alle proprietà di correzione di un codice: tanto meglio è stimata, tanto meglio si riesce a capire quanti errori si possono correggere o rilevare;
- la distribuzione dei pesi permette invece di stimare abbastanza accuratamente la protezione offerta da un codice contro l'accettazione di una parole valida ma errata (questo fenomeno avviene quando il rumore presente durante la trasmissione trasforma la parola trasmessa in un'altra parola di codice).

I risultati della tesi sono raggruppati nelle sezioni seguenti:

1. – Stime sulla distribuzione dei pesi.

In un importante lavoro ([2]), Kasami, Fujiwara e Lin introducono l'uso della programmazione lineare per stimare accuratamente la distribuzione dei pesi per i codici binari. Nella tesi viene mostrato un raffinamento di tale metodo, che è tra l'altro specializzabile per i codici ciclici. Questo metodo permette di ottenere le migliori stime note per una classe di codici interessante: i BCH binari di lunghezza 255 ([4]). Questi codici sono molto studiati, essendo ampiamente utilizzati ad esempio nella comunicazione tra treni e dispositivi elettronici lungo i binari (questa parte della tesi è stata realizzata congiuntamente con l'Ing. A. Tamponi dell'Ansaldo Segnalamento Ferroviario).

2. – Basi di Gröbner e distanza dei codici ciclici.

Recentemente sono stati proposti dei metodi per ottenere la distanza di un codice ciclico tramite il calcolo di una base di Gröbner per un certo ideale costruito *ad hoc*. L'ideale usato in questi metodi è generato da polinomi con un numero elevato di variabili, rendendo il calcolo oneroso anche nei casi più semplici. D'altra parte esistono dei metodi simili ma di più agevole applicazione, usati per la correzione degli errori, piuttosto che per la determinazione della distanza.

Il risultato presentato nella tesi consiste nel modificare uno dei metodi «correttori» in modo che possa essere usato per trovare la distanza. Con questo metodo si ridimostrano dei risultati classici, sia in maniera teorica che col calcolo esplicito di basi di Gröbner.

3. – Stime dal basso della distanza dei codici ciclici.

Esiste un algoritmo dovuto a Schaub, in grado di dare le migliori stime dal basso per la distanza dei codici ciclici di lunghezza media. In particolare l'algoritmo di Schaub fornisce le migliori stime note per la distanza dei codici duali dei BCH binari di lunghezza 255. Schaub sfrutta la struttura delle radici del polinomio generatore dei codici, applicando convenientemente la trasformata di Fourier discreta ai sottocodici ciclici. In ultima analisi, Schaub riesce a mostrare che la distanza del codice è almeno il minimo dei ranghi di certe matrici circolanti.

Nella tesi si riesce a sfruttare la circolarità delle matrici di Schaub per raffinare ulteriormente le stime ottenute. In particolare si esibiscono nuove stime per delle classi di codici importanti, tra cui i duali dei BCH binari di lunghezza 255.

4. – Stime dall'alto della distanza dei codici ciclici.

Sono stati proposti, sia classicamente che recentemente (si veda ad esempio [1]), diversi algoritmi probabilistici che cercano parole di peso piccolo all'interno di un codice. Il peso trovato è chiaramente una stima dall'alto della distanza. Il punto delicato è riuscire a trovare parole con il peso più piccolo possibile, esaminando nel contempo il numero minore di parole.

Nella tesi si mostra come individuare dei sottocodici ciclici, tali da contenere una quantità relativamente elevata di parole di peso piccolo, rendendo più veloce ed efficiente il calcolo da parte degli algoritmi probabilistici. Si dimostra formalmente che l'uso di questo sottocodice migliora in media l'efficienza dell'algoritmo di Brouwer e lo si mostra numericamente nel caso dei duali dei BCH binari di lunghezza 255.

BIBLIOGRAFIA

[1] A. CANTEAUT, F. CHABAUD, *A New Algorithm for Finding Minimum-Weight Words in a Linear Code: Application to McEliece's Cryptosystem and to Narrow-Sense BCH Codes of Length* 511, IEEE Trans. on Inf. Th., **44** (1998), 367-378.

[2] T. KASAMI, T. FUJIWARA, SHU LIN, *An Approximation to the Weight Distribution of Binary Linear Codes*, IEEE Trans. on Inf. Th., **31** (1985,), 769-780.

[3] F. J. MACWILLIAMS, N. J. A. SLOANE, *The Theory of Error-Correcting Codes*, North Holland (1977).

[4] M. SALA, A. TAMPONI, *A Linear Programming Estimate of the Weight Distribution of* $BCH(255, k)$, IEEE Trans. on Inf. Th., **46** (2000), 2235-2237.

Dipartimento di Matematica «L. Tonelli», Università di Pisa
e-mail: sala@dm.unipi.it
Dottorato in Matematica (sede amministrativa: Milano) - Ciclo XI
Direttore di ricerca: Prof. Carlo Traverso