Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Werner Heise, Pasquale Quattrocchi

Il teorema di equivalenza per i codici ciclici

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **78** (1985), n.6, p. 263–267.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1985_8_78_6_263_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1985.

RENDICONTI

DELLE SEDUTE

DELLA ACCADEMIA NAZIONALE DEI LINCEI

Classe di Scienze fisiche, matematiche e naturali

Seduta del 28 giugno 1985

Presiede il Presidente della Classe GIUSEPPE MONTALENTI

SEZIONE I

(Matematica, meccanica, astronomia, geodesia e geofisica)

Algebra. — *Il teorema di equivalenza per i codici ciclici.* Nota di WERNER HEISE (*) e PASQUALE QUATTROCCHI (**), presentata (***) dal Socio G. ZAPPA.

SUMMARY. — Every unit u in the ring Z_n of the residual classes mod n induces canonically an automorphism π of the algebra $R_n(q) = GF(q)[z]/(z^n - 1)$. Let $\mathscr{C} \subset R_n(q)$ be a cyclic code, i.e. an ideal. If the numbers n and q are relatively prime then there exists a well-known characterization of the code $\pi(\mathscr{C})$. We extend this characterization to the general case.

1. INTRODUZIONE

Siano n un numero naturale e $q > 1$ una potenza di un numero primo p. Con $V_n(q)$ indichiamo lo spazio vettoriale delle n–uple a componenti in $F := GF(q)$. Ogni sottospazio k–dimensionale $\mathscr{C}$ di $V_n(q)$ è detto (n, k)–codice lineare (di lunghezza n ed ordine q). Sia $\pi \in S_n$ una permutazione dell'insieme $Z_n := \{0, 1, \ldots, n-1\}$ degli indici delle componenti dei vettori di $V_n(q)$; la permutazione π induce una trasformazione lineare $V_n(q) \to V_n(q)$; $x_0 x_1 \ldots x_{n-1} \to x_{\pi(0)} x_{\pi(1)} \ldots x_{\pi(n-1)}$ che indicheremo ancora con π. Questa trasformazione lineare in $V_n(q)$ non è altro che un riordinamento delle componenti di tutti i vettori di $V_n(q)$. Per ogni (n, k)–codice lineare $\mathscr{C} \subset V_n(q)$ il (n, k)-

(*) Lavoro eseguito durante l'attività di visiting professor del C.N.R. in Modena.

(**) Lavoro eseguito nell'ambito dell'attività del G.N.S.A.G.A. del C.N.R., parzialmente finanziato con fondi M.P.I. (40%).

(***) Nella seduta del 28 giugno 1985.

codice lineare $\pi(\mathscr{C})$ è detto equivalente a $\mathscr{C}$. Se $\mathscr{C}$ e $\pi(\mathscr{C})$ coincidono, la permutazione $\pi \in S_n$ sarà chiamata automorfismo del codice $\mathscr{C}$. Questa terminologia, spesso usata nella teoria dei codici, non tiene conto del fatto che - da un punto di vista matematicamente rigoroso - un isomorfismo fra due codici lineari deve essere definito come una biiezione lineare che conserva il peso di Hamming, cioè che lascia invariato il numero delle componenti diverse da zero di ciascun vettore. In [6] è dimostrato che ogni isomorfismo in questo senso può essere descritto come restrizione di una trasformazione monomiale di $V_n(q)$, e che - a parte casi banali - la corrispondenza fra gli isomorfismi e le trasformazioni monomiali è biiettiva. Così la terminologia qui usata risulta giustificata. Trascuriamo solamente quelle trasformazioni monomiali di $GL_n(q)$, che sono descritte da matrici diagonali.

Una importante classe di codici lineari è quella dei codici ciclici; un codice lineare $\mathscr{C} \subset V_n(q)$ si dice ciclico se la traslazione $i \to i - 1$ dell'anello Z_n delle classi resto mod n risulta un automorfismo del codice. Per studiare i codici ciclici è utile identificare lo spazio vettoriale $V_n(q)$ con l'algebra $R_n(q) := F[z]/(z^n - 1)$ dei polinomi su F mod $z^n - 1$. In $R_n(q)$ calcoleremo sempre con rappresentanti di grado minimo; identificheremo così il vettore $a_0 a_1 \ldots a_{n-1} \in V_n(q)$ con la sua funzione generatrice $\sum_{i=0}^{n-1} a_i z^i \in R_n(q)$. I codici ciclici contenuti in $V_n(q)$ coincidono con gli ideali di $R_n(q)$, infatti la permutazione $i \to i - 1$ di Z_n induce la trasformazione lineare $f(z) \to zf(z)$ di $R_n(q)$. Sia u una unità nell'anello Z_n, cioè un numero primo con n. Indichiamo con v l'elemento inverso di u. La permutazione $\pi : Z_n \to Z_n$, $i \to iu$ mod n induce sull'algebra $R_n(q)$ l'automorfismo $\pi : R_n(q) \to R_n(q)$; $\sum_{i=0}^{n-1} a_i z^i \to \sum_{i=0}^{n-1} a_{\pi(i)} z^i$; infatti, la permutazione π è un automorfismo del gruppo additivo dell'anello Z_n. Osserviamo che è $\sum_{i=0}^{n-1} a_{\pi(i)} z^i \equiv \sum_{i=0}^{n-1} a_i z^{iv} \bmod z^n - 1$. Per ogni (n, k)-codice ciclico $\mathscr{C} \subset R_n(q)$ l'immagine $\pi(\mathscr{C})$ è un (n, k)-codice ciclico equivalente a $\mathscr{C}$. In questa nota si caratterizza il codice $\pi(\mathscr{C})$. Questa caratterizzazione è ben nota in letteratura [1, 3, 4, 5] nel caso $(n, q) = 1$, cioè nel caso in cui n e q sono primi fra loro. Il caso $(n, q) > 1$ è parzialmente trattato in [2].

Generalmente nella teoria dei codici ciclici l'ipotesi $(n, q) = 1$ facilita le dimostrazioni, poiché solo in questo caso l'algebra $R_n(q)$ è semisemplice, ma esistono molti codici ciclici interessanti anche nel caso $(n, q) > 1$.

2. Il teorema di equivalenza

Siano n un numero naturale, $q > 1$ una potenza di un numero primo p ed $h \geq 1$ la più grande potenza di p che divide n. Poniamo $t := n/h$. Sia inoltre u una unità nell'anello Z_n, v il reciproco di u in Z_n e π l'automorfismo dell'algebra $R_n(q)$ indotto dalla permutazione $\pi : Z_n \to Z_n$; $i \to iu$ mod n.

Sia ζ una radice primitiva t–esima dell'unità su F. Per $j = 0, 1, 2, \ldots$ indichiamo con $p_j(z)$ il polinomio minimo di ζ^j su F. Indichiamo con CC (j) la classe ciclotomica di j, cioè l'insieme degli elementi $j, jq, jq^2, \ldots$ previa riduzione mod t. Le radici coniugate a ζ^j di $p_j(z)$ su F sono esattamente le radici t–esime dell'unità ζ^l con $l \in$ CC (j). Indicando con R un sistema di rappresentanti delle classi ciclotomiche CC (0), CC (1), ... possiamo scrivere

$$z^t - 1 = \prod_{j \in R} p_j(z) = \prod_{i=0}^{t-1} (z - \zeta^i) \quad \text{e} \quad z^n - 1 = \prod_{j \in R} p_j^h(z) = \prod_{i=0}^{t-1} (z - \zeta^i)^h .$$

Sia ora $\mathscr{C}_\zeta$ un (n, k)–codice ciclico in $R_n(q)$. Il codice $\mathscr{C}_\zeta$ è generato come ideale dal suo cosiddetto polinomio generatore $g_\zeta(z)$, che è il polinomio monico di grado minimo in $\mathscr{C}_\zeta$. Poiché $g_\zeta(z)$ è un divisore di $z^n - 1$ possiamo scrivere $g_\zeta(z) = \prod_{j \in R} p_j^{h(j)}(z)$ dove $h(j) \leq h$ è, per ogni $j \in$ R, un intero non negativo. La radice t–esima dell'unità $\eta := \zeta^u$ è anche primitiva; il suo polinomio minimo su F è il polinomio $p_{\pi(1)}(z) = p_u(z)$. Definiamo un (n, k)–codice $\mathscr{C}_\eta \subset R_n(q)$ mediante il suo polinomio generatore $g_\eta(z) := \prod_{j \in R} p_{\pi(j)}^{h(j)}(z)$ e affermiamo che i polinomi dei codici $\mathscr{C}_\zeta$ e $\mathscr{C}_\eta$ differiscono solo per l'ordinamento dei coefficienti. Più precisamente formuliamo il

TEOREMA DI EQUIVALENZA: $\pi(\mathscr{C}_\zeta) = \mathscr{C}_\eta$.

Dimostrazione. Siano $l \in Z_t$ e $p(z) = \sum_{i=0}^{n-1} a_i z^i = \sum_{i=0}^{n-1} a_{\pi(i)} z^{\pi(i)} \in R_n(q)$.

Si ha:

(i) *La radice t–esima dell'unità η^l è uno zero del polinomio* $\pi(p(z)) = \sum_{i=0}^{n-1} a_{\pi(i)} z^i \in R_n(q)$ *se e solo se* ζ^l *è uno zero di* $p(z)$.

Infatti si ha $\pi(p(\eta^l)) = \sum_{i=0}^{n-1} a_{\pi(i)} \zeta^{uli} = \sum_{i=0}^{n-1} a_{\pi(i)} \zeta^{l\pi(i)} = p(\zeta^l)$.

Scegliamo $j \in$ R e consideriamo il polinomio irriducibile $p_j(z)$.

La radice t–esima dell'unità η^l, $l \in Z_t$, è, per (i), uno zero di $\pi(p_j(z))$ se e solo se $p_j(\zeta^l) = 0$, quindi se e solo se $l \in$ CC (j). Sia I_1 l'ideale generato da $p_j(z)$, I_2 quello generato da $\pi(p_j(z))$, I_3 quello generato da $p_{\pi(j)}(z)$.

Essendo $p_j(z)$ e $p_{\pi(j)}(z)$ divisori di $z^n - 1$ e irriducibili, I_1 e I_3 sono massimali. Per (i) ogni radice di $\pi(p_j(z))$ è radice di $p_{\pi(j)}(z)$, onde, essendo I_3 massimale, è $I_2 \subset I_3$. Ma $\pi(I_1) = I_2$, onde, essendo I_1 massimale, anche I_2 lo è.

Da $I_2 \subset I_3$ segue allora $I_2 = I_3$, onde $\pi(p_j(z)) = e_j(z) p_{\pi(j)}(z)$ dove $e_j(z)$ è una unità di $R_n(q)$.

Così si ha $\pi(g_\zeta(z)) = \prod_{j \in R} (\pi(p_j(z)))^{h(j)} = \prod_{j \in R} e_j^{h(j)}(z) p_{\pi(j)}^{h(j)}(z) = e(z) g_\eta(z)$ dove $e(z) := \prod_{j \in R} e_j^{h(j)}(z)$ è una unità nell'anello $R_n(q)$. I polinomi $\pi(g_\zeta(z))$ e $g_\eta(z)$ generano allora lo stesso ideale $\mathscr{C}_\eta$ di $R_n(q)$, e quindi si ha $\pi(\mathscr{C}_\zeta) = \mathscr{C}_\eta$.

3. Automorfismi

Usiamo ancora la terminologia ed i simboli con il significato attribuito nel precedente n. 2. Se i codici $\mathscr{C}_\zeta$ e $\mathscr{C}_\eta$ coincidono allora la permutazione π di Z_n è un automorfismo di $\mathscr{C}_\zeta$. I codici $\mathscr{C}_\zeta$ e $\mathscr{C}_\eta$ coincidono se e solo se si ha $g_\zeta(z) = g_\eta(z)$. Indichiamo con σ la permutazione di R che associa a $j \in R$ il rappresentante della classe ciclotomica $CC(\pi(j))$. Quindi π è un automorfismo se e solo se si ha $\prod_{j\in R} p_{\sigma(j)}^{h(\sigma(j))}(z) = g_\zeta(z) = g_\eta(z) = \prod_{j\in R} p_{\pi(j)}^{h(j)}(z) = \prod_{j\in R} p_{\sigma(j)}^{h(j)}(z)$, quindi se e solo se si ha $h(j) = h(\sigma(j))$ per ogni $j \in R$: la funzione $h : R \to N_0$ deve essere costante sulle orbite della permutazione σ di R. Questo è in particolare il caso in cui $\pi(1)$ appartiene a $CC(1)$, cioè il caso in cui $u \equiv 1, q, q^2, \ldots \bmod t$. In questo caso la permutazione π di Z_n è un automorfismo di ogni codice ciclico $\mathscr{C} \subset R_n(q)$.

Indichiamo con G il gruppo di questi automorfismi « universali ». Sia m l'ordine moltiplicativo di q mod t. È noto che m è la cardinalità di $CC(1)$ e quindi anche la dimensione del campo di riducibilità completa $GF(q^m)$ del polinomio $z^t - 1$ su $F = GF(q)$. Nel caso $h = 1$ il gruppo G è isomorfo al sottogruppo $CC(1)$ del gruppo Z_t^* delle unità di Z_t. Calcoliamo ora l'ordine di G nel caso $h > 1$. Indichiamo con f l'omomorfismo che assegna ad ogni unità $u \in Z_n^*$ l'unità u mod t di Z_t^*. Il gruppo G è isomorfo al sottogruppo $H := f^{-1}(CC(1))$ di Z_n^*.

Indicando con φ la funzione di Eulero, si ottiene $|Z_n^*| = \varphi(n) = \varphi(t)\varphi(h) = \varphi(t)\, h(p-1)/p$. Ognuna delle $\varphi(t)$ unità di Z_t^* ha $h(p-1)/p$ retroimmagini rispetto ad f.

Quindi risulta $|G| = |H| = mh(p-1)/p$.

BIBLIOGRAFIA

[1] I.F. BLAKE-R.C. MULLIN (1975) – *The Mathematical Theory of Coding*, Acad. Press New York *et al.*, 45.

[2] W. HEISE (1982) – *The full equivalence theorem for cyclic codes*, Atti del Convegno di Geometria Combinatoria, Passo Mendola, 4-11 luglio 1982.

[3] W. HEISE e P. QUATTROCCHI (1983) – *Informations- und Codierungstheorie*, Springer, Heidelberg *et al.*, 286.

[4] J.H. VAN LINT (1975) – *Coding Theory*, « Lecture Notes in Math. », *201*, Springer, Berlin *et al.*, 48.

[5] F.J. MACWILLIAMS e N.J.A. SLOANE (1977) – *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam *et al.*, 234.

[6] P. FILIP e W. HEISE (1984) – *Monomial code-isomorphisms*, to appear in the proceedings of the congress Combinatorics '84, Sept. 24-29, Bari-Italy.