La Matematica nella Società e nella Cultura

Rivista dell'Unione Matematica Italiana

Alberto Picone

Automorfismi di codici algebrico-geometrici generalizzati

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **1** (2008), n.2 (Fascicolo Tesi di Dottorato), p. 327–330.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2008_1_1_2_327_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, 327-330

Automorfismi di codici algebrico-geometrici generalizzati

ALBERTO PICONE

1. – Introduzione.

Nel 1981 Goppa [2] propose un nuovo modo di costruire dei codici lineari a partire dai posti razionali di un campo di funzioni algebriche. Tali codici sono conosciuti come codici algebrico-geometrici o codici di Goppa. La costruzione di Goppa diede nuovo vigore alla ricerca nell'ambito della teoria dei codici correttori in quanto fu possibile costruire successioni di codici lineari che miglioravano il limite di Gilbert-Varshamov. Comunque essa richiede l'uso di molti posti razionali in quanto la lunghezza del codice è pari al numero dei posti razionali presi in considerazione. Purtroppo, campi di funzione su campi con pochi elementi hanno pochi posti razionali comparati col loro genere.

Per risolvere tale problema, una nuova costruzione di codici lineari, detti *codici algebrico geometrici generalizzati*, fu introdotta da Xing, Niederreiter e Lam [4]. Tale costruzione fa uso di posti di grado qualsiasi e per tale motivo, almeno teoricamente, non vi è alcun limite sulla possibilità di costruire codici sufficientemente lunghi. Comunque l'introduzione di questa classe di codici ha permesso di dare nuovi codici migliorando la tabella di Brouwer [1].

In questa tesi si prende in considerazione una sottoclasse di tali codici (vedi [3]) e se ne studiano gli automorfismi nel caso di campi di funzione razionali, ellittici o iperellittici.

2. – Codici GAG e loro automorfismi.

Sia $F|\mathbb{F}_q$ un campo di funzioni algebriche di genere g. Un $\phi - posto$ di $F|\mathbb{F}_q$ è una coppia (P, ϕ_P) con P posto di grado n di $F|\mathbb{F}_q$ e ϕ_P un $\mathbb{F}_q-$isomorfismo tra il campo delle classi residue F_p di P e $\mathbb{F}_{q^n}$.

Se (P, ϕ_P) è un $\phi-$posto di F e $z \in F$ e regolare a P poniamo $z(P, \phi_P) := \phi_P(z(P))$. Un $\phi - divisore$ è un elemento del gruppo libero generato dai $\phi-$posti ovvero è una somma formale

$$\Phi = \sum_{P \in \mathbb{P}_F} n_P \, (P, \phi_P)$$

con $n_P \in \mathbb{Z}$ e $n_P \neq 0$ solo per un numero finito di posti.

Sia $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$ e (P, ϕ_P) un $\phi-$posto. Si definisce un'azione di $\mathrm{Aut}(F|\mathbb{F}_q)$ sul-

l'insieme dei $\phi-$posti ponendo

$$\sigma(P,\phi_P) := (\sigma(P),\phi_P\sigma^{-1}). \tag{1}$$

(in (1) indichiamo con σ anche l'$\mathbb{F}_q-$isomorfismo da F_P in $F_{\sigma(P)}$ che esso induce e definito da $\sigma(x(P)) := \sigma(x)(\sigma(P))$. Tale azione può essere estesa ai $\phi-$divisori in modo ovvio:

$$\sigma\left(\sum_{P\in\mathbb{P}_F} n_P(P,\phi_P)\right) := \sum_{P\in\mathbb{P}_F} n_P(\sigma(P),\phi_P\sigma^{-1}\Big). \tag{2}$$

Sia $\Phi = \sum_{i=1}^{N}(P_i,\phi_i)$ un $\phi-$divisore di $F|\mathbb{F}_q$ con i P_i posti distinti tutti di grado $n>1$. Sia G un divisore tale che $P_i \notin \operatorname{supp} G$ per ciascun $i=1,2,\dots,N$. Si definisce *codice algebrico geometrico generalizzato* (o semplicemente GAG-codice) il codice

$$C(\Phi;G;n) := \{\,(z(P_1,\phi_1),z(P_2,\phi_2),\dots,z(P_N,\phi_N))\,|\,z\in\mathcal{L}(G)\,\} \tag{3}$$

Si definisce *gruppo degli n-automorfismi* di un GAG-codice $C(\Phi;G;n)$ il gruppo $\mathcal{H}(\Phi;G;n)$ di tutti gli automorfismi $\pi\in S_N$ tali che

$$\pi(z(P_1,\phi_1),\dots,z(P_N,\phi_N)) := (z(P_{\pi(1)},\phi_{\pi(1)}),\dots,z(P_{\pi(N)},\phi_{\pi(N)}))$$

è ancora una parola del codice.

Considerato il seguente sottogruppo di $\operatorname{Aut}(F|\mathbb{F}_q)$

$$\operatorname{Aut}(F|\mathbb{F}_q,\Phi,G) := \{\,\sigma\in\operatorname{Aut}(F|\mathbb{F}_q)\,|\,\sigma(\Phi)=\Phi \text{ e } \sigma(G)\sim_\Phi G\}$$

(dove $G\sim_\Phi G'$ se e solo se esiste $z\in F, z\neq 0$, tale che $G=G'+(z)$ e $z(P_i,\phi_i)=1$ per ogni $i=1,2,\dots,N$), si ha che

TEOREMA 1 (Spera [3]). – *Sia $F|\mathbb{F}_q$ un campo di funzioni di genere g. Siano $\Phi=\sum_{i=1}^{N}(P_i,\phi_i)$, essendo i P_i posti distinti di grado $n>1$, e G tali che $\operatorname{supp} G\cap\{P_1,P_2,\dots,P_N\}=\emptyset$. Sia $C(\Phi;G;n)$ il GAG-codice associato a Φ e G. Allora*

1. *Ogni automorfismo $\sigma\in\operatorname{Aut}(F|\mathbb{F}_q,\Phi,G)$ induce un $n-$automorfismo di $C(\Phi;G;n)$ se definiamo*

$$\sigma(x(P_1,\phi_1),\dots,x(P_N,\phi_N)) := (x(\sigma(P_1,\phi_1)),\dots,x(\sigma(P_N,\phi_N)))$$

   per ogni $x\in\mathcal{L}(G)$.

2. *$\operatorname{Aut}(C(\Phi;G;n))$ contiene un sottogruppo isomorfo a $\operatorname{Aut}(F|\mathbb{F}_q,\Phi,G)$ se una delle seguenti condizioni è verificata*

   a) $N-1>\dfrac{16(g+1)^2}{n}$;

   b) $F|\mathbb{F}_q$ ha qualche posto razionale e $N\geq\dfrac{4g+3}{n}$;

Dunque è possibile pensare $\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$ come sottogruppo del gruppo degli n-automorfismi di un GAG-codice. Nella presente tesi si sono determinate condizioni affinchè $\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$ sia esattamente isomorfo a $\mathcal{H}(\Phi; G; n)$ nel caso di campi di funzioni razionali, ellittici o iperellittici.

TEOREMA 2. – *Sia $\mathbb{F}_q(x)|\mathbb{F}_q$ un campo di funzioni razionali. Sia $\Phi = \sum_{i=1}^{N} (P_i, \phi_i)$ un ϕ–divisore con i P_i posti distinti di grado n. Sia*

$$G = rP_\infty + \sum_{i=1}^{m} r_i P_{a_i}$$

con $r > 0$, $r_i \geq 0$ e P_{a_i} posti razionali. Sia $C(\Phi; G; n)$ il GAG-codice associato a Φ e G. Se $\deg G < \dfrac{nN}{2}$ e $nN \geq 3$, allora

$$\mathcal{H}(\Phi; G; n) \cong \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)_{\Phi,G}.$$

Il seguente lemma permette di descrivere in maniera più semplice i ϕ–posti di un campo di funzione razionale. Grazie ad esso, si potrà descrivere esplicitamente $\mathcal{H}(n; \Phi; G)$ nel caso in cui G verifichi le condizioni del Teorema 2.

LEMMA 1. – *Sia (P, ϕ) un ϕ–posto of $\mathbb{F}_q(x)|\mathbb{F}_q$. Se $\deg P = n > 1$, allora esiste $a \in \mathbb{F}_{q^n}$ tale che $(P, \phi) = (P_{[a]}, \phi_a)$ con $P_{[a]} := P_{(x-a)(x-a^q)\cdots(x-a^{q^{n-1}})}$ e $\phi_a\left(\dfrac{u(x)}{v(x)}(P_{[a]})\right) = \dfrac{u(a)}{v(a)}$.*

PROPOSIZIONE 1. – *Sia $\mathbb{F}_q(x)|\mathbb{F}_q$ un campo di funzioni razionali e $C(\Phi; G; n)$ un GAG-codice associato a $\Phi = \sum_{i=1}^{N} (P_{[a_i]}, \phi_{a_i})$ e $G = rP_\infty$. Se $r < \dfrac{nN}{2}$, allora $\mathcal{H}(n; \Phi; G)$ è isomorfo al gruppo delle affinità della retta $\mathbb{F}_q$ che permutano le radici a_i.*

Sia $F|\mathbb{F}_q$ un campo di funzioni ellittico o iperellittico di genere g. Supponiamo $\mathrm{char}\,\mathbb{F}_q \neq 2$. Sia D_∞ la somma dei posti che giacciano sul polo P_∞ di x in $\mathbb{F}_q(x)$ e $H(\mathbb{F}_q) := \mathbb{P}_F^{(1)} \cup \mathrm{supp}(D_\infty)$ essendo $\mathbb{P}_F^{(1)}$ l'insieme dei posti razionali.

TEOREMA 3. – *Sia $J \subseteq H(\mathbb{F}_q) \setminus \mathrm{supp}\,((x)_\infty)$ e sia*

$$G = n_\infty D_\infty + \sum_{Q \in J} n_Q Q$$

un divisore di $F|\mathbb{F}_q$ con $n_\infty \geq \begin{cases} 2g+2 & \text{se } d \equiv 1 \pmod 2 \\ g+1 & \text{se } d \equiv 0 \pmod 2 \end{cases}$ e $n_Q \geq 1$ per ogni $Q \in J$. Inoltre si supponga che $\Phi = \sum_{i=1}^{N} (P_i, \phi_i)$ sia un ϕ–divisore con i P_i posti distinti di grado $n > 1$. Se $\deg G < \dfrac{nN}{2}$ e una delle seguenti condizioni è verificata

1. $nN > 16(g+1)^2 + n$;
2. *$F|\mathbb{F}_q$ ha qualche posto razionale e* $nN \geq 4g+3$;

allora

$$\mathcal{H}(\Phi; G; n) \cong \mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,G}.$$

Anche nel caso ellittico e/o iperellittico, procederemo ad una descrizione semplificata dei ϕ−posti in modo da poter determinare esplicitamente $\mathcal{H}(\Phi; G; n)$.

LEMMA 2. – *Ogni ϕ−posto che non giace su $(P_{[\infty]}, id)$ di un campo di funzioni iperellittiche $F|\mathbb{F}_q$ è del tipo $(P_{[a,\beta]}, \phi_{a,\beta})$ con*

$$P_{[a,\beta]} = \left\{ \frac{u(x,y)}{v(x,y)} \in F \,|\, u(a,\beta) = 0 \text{ e } v(a,\beta) \neq 0 \right\} \text{ e } \phi_{a,\beta}\left(\frac{u(x,y)}{v(x,y)} P_{[a,\beta]}\right) = \frac{u(a,\beta)}{v(a,\beta)}.$$

PROPOSIZIONE 2. – *Sia $F|\mathbb{F}_q$ un campo di funzioni iperellittiche con modello piano $\mathcal{C} : Y^2 = \prod_{\gamma \in \mathbb{F}_q} (X - \gamma)$. Se $C(\Phi; G; n)$ è un GAG-codice associato a $\Phi = \sum_{i=1}^{N} (P_{[a_i,\beta_i]}, \phi_{a_i,\beta_i})$ e $G = rD_\infty$ e se $2g + 2 < r < \frac{nN}{2}$ e $nN \geq 4g + 3$, allora $\mathcal{H}(n; \Phi; G)$ è il gruppo delle trasformazioni $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$, dove $\sigma(x) = ax + b$ e $\sigma(y) = \varepsilon y$ con $\varepsilon^2 = a$, tali che σ fissa l'insieme $\{(a_i, \beta_i) \,|\, i = 1, 2, \ldots, N\}$.*

BIBLIOGRAFIA

[1] BROUWER A.E., *Bounds on minimum distance of linar codes*, [Online], available at http://www.win.tue.nl/∼aeb/voorlincod.html.

[2] GOPPA V.D., *Codes on Algebraic Curves*, Soviet Math. Dokl., **24** (1981), 170-172.

[3] SPERA A.G., *On Automorphisms of generalized Algebraic-Geometry Codes*, J. Pure Appl. Algebra, **210**, (2007), 837-845.

[4] XING C.P., NIEDERREITER H. and LAM K.Y., *A Generalization of Algebraic-Geometric Codes*, IEEE Trans. Inform. Theory, **45** (1999), 2438-2501).

Dipartimento di Matematica e Applicazioni, Palermo
e-mail: picone@math.unipa.it
Dottorato di ricerca in Matematica (sede amministrativa: Università di Palermo) - Ciclo XVIII
Direttore di ricerca: Prof. Antonino Giorgio Spera