Codici di Reed–Solomon

18 Novembre 2009

Sia $q = p^\nu$ una potenza di primo e α un elemento primitivo di $\mathrm{GF}(q)$, di modo che le successive potenze

$$\alpha^0, \alpha^1, \ldots, \alpha^{q-2}$$

sono tutti gli elementi di $\mathrm{GF}(q)^\star$.

Definizione 1. *Sia* $n = q - 1$ *e* $k \leq n$. *Si dice* codice di Reed–Solomon q*–ario di lunghezza* n *e dimensione* k *il sottoinsieme di* $\mathrm{GF}(q)^n$ *dato da*

$$\mathrm{RS}(n,k) = \left\{ \left(f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{n-1}) \right) : f(x) \in \mathrm{GF}(q)[x], \deg f(x) < k \right\}.$$

1 Parametri dei codici di Reed–Solomon

Teorema 2. *Il codice* $\mathrm{RS}(n,k)$ *è lineare, di lunghezza* n*, dimensione* k.

Dimostrazione. Sia $\Theta : \mathrm{GF}(q)[x] \to \mathrm{GF}(q)^n$ l'applicazione che associa ad ogni polinomio $f(x) \in \mathrm{GF}(q)$ il vettore

$$f(x) \to \left(f(\alpha^0), f(\alpha), \ldots, f(\alpha^{n-1}) \right).$$

L'insieme $\mathrm{RS}(n,k)$ è l'immagine del sottospazio vettoriale

$$M_k = \{ p(x) \in \mathrm{GF}(q)[x] : \deg p(x) < k \}$$

di $\mathrm{GF}(q)[x]$ secondo Θ. Mostriamo che:

(1) Θ è lineare; pertanto $\mathrm{RS}(n,k)$ è un codice lineare di lunghezza n;

(2) se $k \leq n$, l'applicazione Θ è iniettiva $M_k \to \mathrm{GF}(q)[x]$; pertanto la dimensione di $\mathrm{RS}(n,k)$ è k.

Per verificare (1) calcoliamo

$$\begin{aligned}\Theta((f+\lambda g)(x)) = \\ ((f+\lambda g)(\alpha^0),(f+\lambda g)(\alpha^1),\dots(f+\lambda g)(\alpha^{n-1})) = \\ (f(\alpha^0)+\lambda g(\alpha^0), f(\alpha^1)+\lambda g(\alpha^1),\dots f(\alpha^{n-1})+\lambda g(\alpha^{n-1})) = \\ (f(\alpha^0), f(\alpha^1),\dots,f(\alpha^{n-1})) + (g(\alpha^0), g(\alpha^1),\dots,g(\alpha^{n-1})) = \\ \Theta(f(x)) + \lambda\Theta(g(x)).\end{aligned}$$

Per la (2), osserviamo che

$$\Theta(f(x)) = \Theta(g(x))$$

se, e solamente se, per ogni $i = 0,\dots,n-1$,

$$f(\alpha^i) = g(\alpha^i),$$

ovvero il polinomio $f(x) - g(x)$ deve annullarsi su tutti gli n possibili elementi α^i. Ci sono due possibilità:

a. $f(x) - g(x)$ è il polinomio nullo;

b. il polinomio

$$(x-\alpha^0)(x-\alpha^1)\cdots(x-\alpha^{n-1}) = \prod_{i=0}^{n-1}(x-\alpha^i) = (x^n-1)$$

divide $f(x) - g(x)$; in questo caso $\deg f(x) - g(x) \geq n$.

D'altro canto, se $\deg f(x), \deg g(x) < k \leq n$, allora $\deg f(x) - g(x) \leq n$, per cui l'eventualità b. non può verificarsi. Ne segue che $\Theta : M_k \to GF(q)^n$ è iniettiva. □

Teorema 3. *La distanza minima di* $RS(n,k)$ *è* $n-k+1$.

Dimostrazione. Usiamo le medesime notazioni adottate nella dimostrazione del Teorema 2. Supponiamo di avere due parole distinte $\mathbf{f}$ e $\mathbf{g}$ in $RS(n,k)$ e indichiamo con $f(x)$ e $g(x)$ i corrispondenti polinomi in M_k, di modo che

$$\mathbf{f} = (f(\alpha^0), f(\alpha^1),\dots,f(\alpha^{n-1})), \quad \mathbf{g} = (g(\alpha^0), g(\alpha^1),\dots,g(\alpha^{n-1})).$$

Ricordando la relazione fra distanza e peso per un codice lineare, si ha

$$d(\mathbf{f},\mathbf{g}) = w(\mathbf{f}-\mathbf{g})$$

In particolare, $w(\mathbf{f}-\mathbf{g})$ corrisponde a $n-t$ ove t è il numero di elementi α^i tali che $f(\alpha^i)-g(\alpha^i)=0$. Questi elementi devono essere radici del polinomio $u(x)=f(x)-g(x)$. Tale polinomio, in particolare, ha grado al più $k-1$ ed è diverso dal polinomio nullo. Ne segue che il numero t delle sue radici è minore o uguale a $k-1$ e dunque

$$d(\mathbf{f},\mathbf{g})=w(\mathbf{f}-\mathbf{g})\geq n-k+1.$$

□

Teorema 4. *Il codice* $\mathrm{RS}(n,k)$ *è ciclico.*

Dimostrazione. Supponiamo

$$\mathbf{c}=(c_0,c_1,\ldots,c_{n-1})\in \mathrm{RS}(n,k).$$

Allora esiste un polinomio $f(x)\in \mathrm{GF}(q)[x]$ con $\deg f(x)<k$ e

$$\mathbf{c}=\left(f(\alpha^0),f(\alpha^1),\ldots,f(\alpha^{n-1})\right).$$

Chiaramente $g(x)=f(\alpha^{n-1}x)\in \mathrm{GF}(q)[x]$ e $\deg g(x)<k$. Osserviamo che

$$\mathbf{c}'=\Theta(g(x))=\left(f(\alpha^{n-1}\alpha),f(\alpha^{n-1}\alpha^2),\ldots f(\alpha^{n-1}\alpha^{n-1})\right)=\left(f(\alpha^{n-1}),f(\alpha^n),\ldots f(\alpha^{2n-2})\right).$$

Tenuto conto che $\alpha^n=\alpha^{q-1}=\alpha^0$, ne segue

$$\mathbf{c}'=\left(f(\alpha^{n-1}),f(\alpha^0),f(\alpha^1),\ldots f(\alpha^{n-1})\right)\in \mathrm{RS}(n,k).$$

Pertanto il codice $\mathrm{RS}(n,k)$ è ciclico. □

2 Codifica e decodifica

Osserviamo che ad ogni elemento $\mathbf{m}=(m_0,m_1,\ldots,m_{k-1})\in \mathrm{GF}(q)^k$ possiamo associare un polinomio

$$m(x)=\sum_{i=0}^{k-1} m_i x^i.$$

La parola corrispondente a $m(x)$ secondo l'omomorfismo Θ introdotto nel paragrafo precedente è un vettore

$$\mathbf{c}=(c_0,c_1,\ldots,c_{n-1})\in \mathrm{RS}(n,k).$$

Pertanto Θ fornisce una codifica

$$\mathbf{m} \to \mathbf{c},$$

ove

$$c_i = \sum_{j=0}^{n-1} m_j \alpha^{ij},$$

supponendo $m_j = 0$ per ogni $j \geq k$. Notiamo comunque che tale codifica non è sistematica; a priori non è possibile determinare un insieme di posizioni in $\mathbf{c}$ in cui compaiano esattamente gli m_i.

Teorema 5 (DFT)**.** *Supponiamo*

$$c_i = \sum_{j=0}^{n-1} m_j \alpha^{ij}; \tag{1}$$

allora,

$$m_k = \frac{1}{n} \sum_{j=0}^{n-1} \alpha^{-jk} c_j. \tag{2}$$

Dimostrazione. Procediamo in due passaggi:

1. Mostriamo dapprima che

$$\sum_{i=0}^{n-1} \alpha^i = \begin{cases} 0 & \text{se } \alpha \neq 1 \\ n & \text{se } \alpha = 1. \end{cases} \tag{3}$$

   Infatti, tenuto conto che $\alpha^n = \alpha^0$ si ha

$$\alpha \sum_{i=0}^{n-1} \alpha^i = \sum_{i=0}^{n-1} \alpha^{i+1} = \sum_{i=1}^{n} \alpha^i = \sum_{i=0}^{n-1} \alpha^i.$$

   Pertanto,

$$\sum_{i=0}^{n-1} \alpha^i - \alpha \sum_{i=0}^{n-1} = 0,$$

   ovvero

$$(1 - \alpha) \sum_{i=0}^{n-1} \alpha^i = 0.$$

Poiché siamo in un campo, vale la legge di annullamento del prodotto e, dunque $(1-\alpha) = 0$ oppure $\sum_{i=0}^{n-1} \alpha^i = 0$. Ne segue che per $\alpha \neq 1$, l'espressione (3) deve essere nulla. Per $\alpha = 1$, la (3) diviene

$$\sum_{i=0}^{n-1} 1 = n.$$

2. Calcoliamo ora

$$\sum_{j=0}^{n-1} \alpha^{-jk} c_j = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} m_i \alpha^{ij} \right) \alpha^{-jk}. \tag{4}$$

Scambiando l'ordine delle sommatorie, la (4) è uguale a

$$\sum_{i=0}^{n-1} m_i \left(\sum_{j=0}^{n-1} \alpha^{j(i-k)} \right).$$

Per quanto verificato nel punto precedente, l'espressione fra parentesi è nulla se $i \neq k$ e pari ad n se $i = k$. Pertanto,

$$\sum_{j=0}^{n-1} \alpha^{-jk} c_j = m_k n.$$

Per concludere, notiamo che $n = q - 1$ è coprimo con q; dunque in $\mathrm{GF}(q)$ è possibile dividere per n. La tesi segue.

□

3 Algoritmo di Welch–Berlekamp

Esiste un algoritmo di decodifica e correzione di errore particolarmente efficiente per i codici di Reed–Solomon.

Premettiamo un'osservazione: sia

$$\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$$

un vettore ricevuto e supponiamo di conoscere un polinomio $p(x)$ con $\deg p(x) < k$ tale che

$$p(\alpha^i) = r_i$$

per ogni i tranne che al più per $t \leq \lfloor \frac{d-1}{2} \rfloor$ valori. Per costruzione dei codici di Reed–Solomon, tale polinomio produce un vettore $\mathbf{r}' = \Theta(p(x)) \in \mathrm{RS}(n, k)$ con

$$d(\mathbf{r}, \mathbf{r}') \leq t \leq \lfloor \frac{d-1}{2} \rfloor$$

Per le proprietà della decodifica dei codici lineari, tale parola di codice è quella alla più piccola distanza possibile da $\mathbf{r}$; pertanto essa corrisponde alla correzione di $\mathbf{r}$.

Mostriamo ora come sia possibile ricavare il polinomio $p(x)$ di cui sopra.

a. Sono dati:

   (a) $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$

   (b) $t \leq \lfloor \frac{d-1}{2} \rfloor$;

   (c) $k \leq n$.

b. Si cerca:

   (a) $p(x)$ con $\deg p(x) < k$ e $p(\alpha^i) = r_i$ per almeno $n - t$ valori di i.

Si procede come segue. Siano

$$E(x) = x^t + \sum_{i=0}^{t-1} e_i x^i, \qquad N(x) = \sum_{i=0}^{k+t-1} n_i x^i$$

due polinomi, $E(x)$ monico di grado t e $N(x)$ di grado al più $k + t - 1$. Vogliamo che per ogni $i = 0, 1, \ldots, n - 1$ valga

$$N(\alpha^i) = r_i E(\alpha^i). \tag{5}$$

Le condizioni in (5), al variare di i, determinano un sistema lineare di n equazioni nelle $(k + t) + t = k + 2t \leq n$ indeterminate

$$e_0, e_1, \ldots, e_{t-1}, n_0, n_1, \ldots n_{k+t-1}.$$

Osserviamo che ogni radice di $E(x)$ è necessariamente radice anche di $N(x)$. Pertanto, il polinomio $E(x)$ divide $N(x)$. Poniamo ora

$$p(x) = \frac{N(x)}{E(x)}.$$

Si noti che:

1. $\deg p(x) = \deg N(x) - \deg E(x) \leq (k + t - 1) - t = k - 1$;
2. ogni qual volta $E(\alpha^i) \neq 0$,

$$p(\alpha^i) = \frac{N(\alpha^i)}{E(\alpha^i)} = r_i;$$

3. il numero di indici per cui $p(\alpha^i) \neq r_i$ è al più $t = \deg E(x)$.

Ne segue che $p(x)$ è proprio il polinomio cercato.

Per concludere, osserviamo che, in generale, il sistema indotto dalle (5) non è detto ammetta un'unica soluzione. D'altro canto se $(E(x), N(x))$ e $(E'(x), N'(x))$ sono due sue soluzioni, allora

$$r_i E(\alpha^i) = N(\alpha^i), \qquad r_i E'(\alpha^i) = N'(\alpha^i);$$

pertanto,

$$r_i E'(\alpha^i) N(\alpha^i) = r_i E(\alpha^i) N'(\alpha^i),$$

da cui

$$p(\alpha^i) = \frac{N(\alpha^i)}{E(\alpha^i)} = \frac{N'(\alpha^i)}{E'(\alpha^i)};$$

il polinomio $p(x)$ è dunque univocamente individuato.