NOTE SUL BOUND DI GILBERT-VARSHAMOV

FIAMMETTA BATTAGLIA

Riferimenti bibliografici utilizzati per queste note: [CSW],[L], [LX]. Altri riferimenti bibliografici utili si trovano nei documenti sopracitati.

1. IL BOUND DI GILBERT-VARSHAMOV

Definiamo $A_q(n,d)$ la massima taglia raggiungibile da un codice q-ario di lunghezza n e distanza di Hamming d.

Definiamo $B_q(n,d)$ la massima taglia raggiungibile da un codice lineare sul campo $\mathbb{F}_q$, di lunghezza n e distanza di Hamming d.

Abbiamo:

- $B_q(n,d) \leq A_q(n,d)$
- $B_q(n,1) = A_q(n,1) = q^n$
- $B_q(n,n) = A_q(n,n) = q$

Denotiamo $B_s(x) \subset \mathbb{F}_q^n$ la palla aperta di centro x e raggio s, ossia

$$B_s(x) = \{y \in \mathbb{F}_q^n \mid d(x,y) < s\}$$

e con $\overline{B_s(x)} \subset \mathbb{F}_q^n$ la palla chiusa di centro x e raggio s, ossia

$$\overline{B_s(x)} = \{y \in \mathbb{F}_q^n \mid d(x,y) \leq s\}.$$

Ricordiamo che, per $s \in \mathbb{N}$, $\#(\overline{B_s(x)}) = \sum_{j=0}^{s} \binom{n}{j}(q-1)^j$. Denotiamo con

$$V_q^n(s) = \#(\overline{B_s(x)})$$

il numero di punti nella palla chiusa di centro un punto in $\mathbb{F}_q^n$ e raggio s, possiamo pensare a questo numero come al volume della palla.

Ricordiamo l'Hamming upper bound:

$$A_q(n,d) \leq \frac{q^n}{V_q^n(\lfloor \frac{d-1}{2} \rfloor)}.$$

Teorema 1.1 (Gilbert-Varshamov lower bound [Gilbert1952, Varshamov1957])**.** *Sia q la potenza di un primo fissata. Siano $d,k,n \in \mathbb{N}$ tali che $2 \leq d \leq n$, $1 \leq k \leq n$ e*

$$V_q^{n-1}(d-2) < q^{n-k}. \tag{1}$$

Allora esiste un codice lineare $[n,k,d']_q$, con $d' \geq d$.

Date: 11 dicembre 2016.

Osservazione 1.2. *Nelle ipotesi del teorema si ha necessariamente $d \leq n-k+1$, ossia i parametri verificano il Singleton bound. Infatti, siano $d, k, n \in \mathbb{N}$ tali che $2 \leq d \leq n$, $1 \leq k \leq n$ e $V_q^{n-1}(d-2) < q^{n-k}$. Supponiamo per assurdo che sia $d \geq n-k+2$. Allora*

$$\begin{aligned} q^{n-k} \leq q^{d-2} &= (1+(q-1))^{d-2} = \\ &\sum_{j=0}^{d-2} \binom{d-2}{j}(q-1)^j \leq \sum_{j=0}^{d-2} \binom{n-1}{j}(q-1)^j \\ &= V_q^{n-1}(d-2). \end{aligned}$$

Infatti $\binom{m}{j} \leq \binom{n}{j}$ per naturali m, n tali che $m \leq n$.

Dimostramo adesso il Teorema 1.1.

Dimostrazione. Abbiamo già osservato che $d \leq n-k+1$, quindi $d \geq 2$ implica $k \leq n-1$. Costruiamo la matrice di controllo di parità H di un codice C in modo tale che C abbia i parametri richiesti. Si denotino le colonne di H nel modo seguente:

$$H = \begin{bmatrix} | & & | \\ C_1 & \dots & C_n \\ | & & | \end{bmatrix} \in \mathbb{F}_q^{(n-k)\times n}.$$

Vogliamo scegliere le colonne di H in modo tale che

(a) rango$(H) = n-k$;
(b) ogni $(d-1)$ colonne di H sono linearmente indipendenti.

Poniamo le prime $n-k$ colonne uguali agli $n-k$ vettori della base canonica di $\mathbb{F}_q^{n-k}$, ossia $C_i = e_i$ per $i = 1, \cdots, n-k$. Queste soddisfano senz'altro le condizioni (a) e (b). Ricordiamo che $d-2 \leq n-k$ e contiamo tutte le combinazioni lineari di $(d-2)$ colonne in

$$H_{n-k} = \begin{bmatrix} | & & | \\ C_1 & \dots & C_{n-k} \\ | & & | \end{bmatrix} \tag{2}$$

Devo contare le combinazioni lineari di $n-k$ colonne con 0 coefficienti diversi da 0, 1 coefficiente diverso da 0, 2 coefficienti diversi da 0 e così via fino a $d-2$ coefficienti diversi da zero. Ottengo

$$\sum_{j=0}^{d-2} \binom{n-k}{j}(q-1)^j \leq \sum_{j=0}^{d-2} \binom{n-1}{j}(q-1)^j = V_q^{n-1}(d-2) < q^{n-k}.$$

Quindi esiste $C_{n-k+1} \in \mathbb{F}_q^{n-k}$ tale che C_{n-k+1} non appartiene ad alcuna combinazione lineare di $d-2$ colonne di (2). Proseguendo in questo modo ottengo la matrice

$$H_{n-k+h} = \begin{bmatrix} | & & | \\ C_1 & \dots & C_{n-k+h} \\ | & & | \end{bmatrix} \tag{3}$$

con $1 \leq h \leq k-1$. Come prima conto le combinazioni lineari di ogni $(d-2)$ colonne in H_{n-k+h}. Ottengo

$$\sum_{j=0}^{d-2} \binom{n-k+h}{j}(q-1)^j \leq \sum_{j=0}^{d-2} \binom{n-1}{j}(q-1)^j = V_q^{n-1}(d-2) < q^{n-k}.$$

Posso quindi scegliere una colonna C_{h+1} non appartenente ad alcuna combinazione lineare di $d-2$ colonne di (3). Determino in questo modo, per $0 \leq h \leq k-1$, ossia in k passi, una matrice H con le caratteristiche (a) e (b). Il codice $C = \mathrm{Ker}(H)$ è un codice con parametri $[n, k, d']$, $d' \geq d$ come richiesto. □

Lemma 1.3. *Siano $a, q \in \mathbb{N}$ tali che $a \geq 1, q \geq 2$, allora $\lceil log_q(a+1) \rceil \leq log_q(a) + 1$.*

Dimostrazione. La funzione $log_q(x)$ assume valori interi quando $x = q^{m+1}$ con $m \in \mathbb{N}$. Quindi, per ogni $m \in \mathbb{N}$, e per ogni $q^m < x \leq q^{m+1}$ si ha $\lceil log_q(x) \rceil = m+1$. Sia $a \in \mathbb{N}$ e sia $m \in \mathbb{N}$ l'unico m tale che tale che $q^m < a+1 \leq q^{m+1}$, allora $\lceil log_q(a+1) \rceil = m+1$. Poiché a è intero $q^m - 1 < a$ implica $q^m \leq a$ e quindi $m \leq log_q(a)$, da cui la tesi. Notare che la tesi non e' vera per valori non interi: esempio $q = 2$, $a = 3/2$. □

Corollario 1.4. *Sia q la potenza di un primo fissata. Siano $d, n \in \mathbb{N}$ tali che $2 \leq d \leq n$. Allora*

$$B_q(n,d) \geq q^{n-\lceil log_q\left(V_q^{n-1}(d-2)+1\right)\rceil} \geq \frac{q^{n-1}}{V_q^{n-1}(d-2)}.$$

Dimostrazione. Poniamo $k = n - \lceil log_q\left(V_q^{n-1}(d-2)+1\right)\rceil$. Allora

$$q^{n-k} = q^{\lceil log_q\left(V_q^{n-1}(d-2)+1\right)\rceil} \geq V_q^{n-1}(d-2) + 1.$$

Le ipotesi del teorema 1.1 sono dunque verificate dai parametri d, k, n, quindi esiste un codice lineare $[n, k, d']_q$, con $d' \geq d$, possiamo quindi costruire un codice $[n, k, d]_q$. Quindi

$$B_q(n,d) \geq q^{n-\lceil log_q\left(V_q^{n-1}(d-2)+1\right)\rceil}.$$

La rimanente disuguaglianza

$$q^{n-\lceil log_q\left(V_q^{n-1}(d-2)+1\right)\rceil} \geq \frac{q^{n-1}}{V_q^{n-1}(d-2)}$$

è una conseguenza del Lemma 1.3. □

2. Bound asintotici e versione asintotica del bound di Gilbert-Varshamov

Dato un codice lineare C di tipo $[n, k, d]_q$, definiamo *information rate* di C

$$R(C) = \frac{k}{n}$$

e *distanza relativa*

$$\delta(C) = \frac{d-1}{n}.$$

Un punto (δ, R) si dice *asintoticamente raggiungibile* se esiste una successione di codici C_i con n_i crescenti, tali che

$$lim_{i\to+\infty}\delta(C_i) = \delta$$

$$lim_{i\to+\infty}R(C_i) = R$$

Notiamo che i punti raggiungibili appartengono necessariamente a $[0,1]^2$. Esempi: $C_i = \mathbb{F}_q^i$ dà $\delta = 0, R = 1$, mentre $C_i = [i,1,i]_q$ dà $\delta = 1, R = 0$. Definiamo la funzione

$$\alpha_q(\delta) = \max\{R \mid (\delta, R) \text{ è asintoticamente raggiungibile}\}.$$

Sono risultati noti: la funzione α_q è continua su $[0,1]$ [Manin1981]; $\alpha_q(0) = 1$ (vedi esempio sopra); $\alpha_q(\delta) = 0$ per $\frac{q-1}{q} \leq \delta \leq 1$. Non si conosce il valore di α_q per alcun $\delta \in (0, \frac{q-1}{q})$, per alcun q [CSW]. Si conoscono solo limiti inferiori e superiori.

Il miglior limite inferiore noto è quello dato dalla versione asintotica del bound di Gilbert-Varshamov:

Proposizione 2.1 (Versione asintotica del bound di Gilbert e Varshamov)**.** *Sia q la potenza di un primo fissata, sia $\delta \in (0, \frac{q-1}{q})$, allora*

$$\alpha_q \geq 1 - h_q(\delta)$$

dove

$$h_q(\delta) = -\delta log_q(\delta) - (1-\delta)log_q(1-\delta) + \delta log_q(q-1)$$

La funzione h_q è detta *funzione di entropia q-aria*. La nozione di entropia nella teoria dell'informazione fu introdotta da C. Shannon in [Shannon48].

Fino al 1982 si congetturava che il bound di Gilbert-Varshamov fosse esatto, ossia che si avesse $\alpha_q = 1 - h_q(\delta)$. Nel 1982 Goppa introdusse un nuovo tipo di codici, sfruttando la geometria delle curve algebriche su campi finiti [Goppa1982]; Tsfasmann, Vladut e Zink costruirono poi, per ogni q fissato sufficientemente grande, una famiglia di codici che supera il bound di Gilbert-Varshamov [TVZ1982], dando inoltre una costruzione di tali codici in tempo polinomiale, poi molto semplificata in [GS].

Il problema per $q = 2$ è ancora aperto.

Dimostreremo la Proposizione 2.1 nel caso $q = 2$. Ci occorrono i seguenti:

Lemma 2.2. *Sia $\delta = \frac{d-1}{n} \leq \frac{1}{2}$ allora*

$$2^{nh_2(\delta)} \geq V_2^n(n\delta).$$

Dimostrazione. Si osservi che

$$2^{-nh_2(\delta)} = \Big(\frac{\delta}{1-\delta}\Big)^{n\delta}(1-\delta)^n$$

$$2^{nh_2(\delta)}\Big(\frac{\delta}{1-\delta}\Big)^{n\delta}(1-\delta)^n = 1 \tag{4}$$

Si scriva ora

$$\begin{aligned} 1 \;=\; & (\delta+(1-\delta))^n = \textstyle\sum_{j=0}^{n}\binom{n}{j}\delta^j(1-\delta)^{n-j} \geq \\ & \textstyle\sum_{j=0}^{\delta n}\binom{n}{j}\delta^j(1-\delta)^{n-j} = \\ & \textstyle\sum_{j=0}^{\delta n}\binom{n}{j}\Big(\frac{\delta}{1-\delta}\Big)^{j}(1-\delta)^n \geq \\ & \textstyle\sum_{j=0}^{\delta n}\binom{n}{j}\Big(\frac{\delta}{1-\delta}\Big)^{n\delta}(1-\delta)^n. \end{aligned} \tag{5}$$

Dove l'ultima disuguaglianza vale perchè $\frac{\delta}{1-\delta} < 1$. Combinando (4) e (5) si ottiene

$$2^{nh_2(\delta)} \geq \sum_{j=0}^{\delta n}\binom{n}{j} = V_2^n(\delta n).$$

□

Lemma 2.3. *Siano n, k, d numeri naturali tali che $k \leq n$, $2 \leq d \leq n$. Siano $R = \frac{k}{n}$ e $\delta = \frac{d-1}{n}$. Se $\delta < \frac{1}{2}$ e*

$$R \leq 1 - h_2(\delta)$$

esiste un codice lineare con parametri $[n, k, d]_2$.

Dimostrazione. Ricordiamo che $q = 2$. Osserviamo che $R \leq 1-h_2(\delta)$ implica $nh_2(\delta) \leq n - k$. quindi, per il Lemma 2.2,

$$2^{nh_2(\delta)} \geq V_2^n(n\delta).$$

Si ottiene quindi

$$2^{n-k} \geq 2^{nh_2(\delta)} \geq V_2^n(n\delta) = V_2^n(d-1) > V_2^{n-1}(d-2).$$

Il teorema 1.1 assicura l'esistenza, per ogni n sufficientemente grande, di un codice lineare con parametri $[n, k, d]$. □

Dimostrazione della Proposizione 2.1

Dimostrazione. Vogliamo dimostrare che il punto $(\delta, 1 - h_2(\delta))$, con $0 < \delta < \frac{q-1}{q} = \frac{1}{2}$ è asintoticamente raggiungibile. Per approssimare il punto $(\delta, 1 - h_2(\delta))$ applichiamo il Lemma 2.3 a una successione di parametri opportunamente costruita. Si osservi che, per ogni n fissato, l'intervallo $[0, 1)$ è unione disgiunta di n intervalli di ampiezza $\frac{1}{n}$:

$$\sqcup_{h=0}^{n-1}\left[\frac{h}{n}, \frac{h+1}{n}\right).$$

Si consideri adesso δ. Sia $N \in \mathbb{N}$ tale che $\delta \geq \frac{1}{N}$. Allora per ogni $n \in \mathbb{N}, n \geq N$, esiste un unico naturale d'_n tale che $1 \leq d'_n \leq n-1$ e

$$\delta \in \left[\frac{d'_n}{n}, \frac{d'_n+1}{n}\right),$$

quindi

$$\delta - \frac{1}{n} \leq \frac{d'_n}{n} \leq \delta.$$

Si consideri adesso $1 - h_2(\frac{d'_n}{n}) \in [0, 1)$. Esiste un unico naturale k_n tale che $1 \leq k_n \leq n - 1$ e

$$1 - h_2(\frac{d'_n}{n}) \in \left[\frac{k_n}{n}, \frac{k_n + 1}{n}\right).$$

Da cui

$$1 - h_2(\frac{d'_n}{n}) - \frac{1}{n} \leq \frac{k_n}{n} \leq 1 - h_2(\frac{d'_n + 1}{n}).$$

Quindi

$$\lim_{n \to +\infty} \frac{d'_n}{n} = \delta,$$

$$\lim_{n \to +\infty} \frac{k_n}{n} = 1 - h_2(\delta).$$

Per continuità della funzione di entropia. Si considerino adesso i parametri interi $d_n = d'_n + 1$ e k_n. Osserviamo che $2 \leq d_n \leq n$, $k_n \leq n$ e

$$\frac{k_n}{n} \leq 1 - h_2(\frac{d_n - 1}{n}).$$

Notiamo inoltre che per n sufficientemente grande $\delta_n < \frac{1}{2}$. Il Lemma 2.3 assicura l'esistenza, per ogni n sufficientemente grande, di un codice lineare con parametri $[n, k_n, d_n]_2$. Abbiamo così dimostrato l'esistenza di una successione di codici lineari con le caratteristiche asintotiche richieste. □

RIFERIMENTI BIBLIOGRAFICI

[CSW] Mahdi Cheraghchi, Amin Shokrollahi, Avi Wigderson, Computational Hardness and Explicit Constructions of Error Correcting Codes, 44th Allerton Conference on Communication, Control and Computing, Allerton House, IL, USA, 2006. Published in: Allerton 2006. Disponibile alla pagina `http://www.math.ias.edu/~avi/PUBLICATIONS/MYPAPERS/CSW06/CSW06.pdf`

[GS] A. Garcia, H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, Invent. Math., vol. 121, pp. 211-222, 1995.

[Gilbert1952] E. N. Gilbert, A comparison of signaling alphabets, Bell System Technical Journal, vol. 31, pp. 504-522, 1952.

[Goppa1982] V. Goppa, Codes on algebraic curves, Sov. Math. Dokl., vol. 24, pp. 170-172, 1981.

[L] Yehuda Lindell, Introduction to Coding Theory, Lecture Notes, (2010), disponibile alla pagina `http://u.cs.biu.ac.il/~lindell/89-662/main-89-662.html`.

[LX] San Ling, Chaoping Xing, Coding Theory: A First Course, Cambridge University Press (2004).

[Manin1981] Y. Manin, What is the maximum number of points on a curve over F2?, J. Fac. Sci. Tokio, vol. 28, pp. 715-720 (1981).

[Shannon48] Claude E. Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal, Vol. 27, pp. 379-423, 623-656, July, October, 1948. Disponibile alla pagina `http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf`

[TVZ1982] M. Tsfasman, S. Vlădut, T. Zink, Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound, Math. Nachrichten, vol. 109, pp. 21-28, 1982.

[Varshamov1957] R. R. Varshamov, Estimate of the number of signals in error correcting codes, Doklady Akademii Nauk SSSR, vol. 117, pp. 739-741, 1957.