On the Information Function of an Error-Correcting Code

Author: Tor Helleseth, Senior Member, IEEE
Torleiv Klove, Senior Member, IEEE
Vladimir I. Levenshtein, Member, IEEE
From: IEEE Transations On Information Theory, Vol.43, No.2, March 1997

No:u8913527
Reporter:交大電信所蘇英凱

1

Abstract

- The information function e_h of a code is the average amount of information contained in h positions of the codewords
- Upper and lower bounds on the information function of binary linear codes are given

2

Notations and Background Information

- S_h : the subset of $\{1, 2, \cdots, n\}$ of size h
- $X = \{i_1, i_2, \cdots, i_h\} \in S_h$ where $1 \le i_1 < i_2 < \cdots < i_h \le n$
- $c = (c_1, c_2, \cdots, c_n)$ $c_x = (c_{i1}, c_{i2}, \cdots, c_{ih})$
- Define $C_x = \{c_x \mid c \in C\}$
- For $y \in C_x$, let $N_x(y) = |\{c \in C \mid c_x = y\}|$
- $\sum_{y \in C_x} N_x = |C|$

3

Notations and Background Information

- Let C be a [n,k] linear code and the support of a vector c given by $\chi(c) \equiv \{i : \exists (x_1, x_2, \cdots, x_n) \in c, x_i \neq 0\}$
- D is the subcode of C and the support of D ,denoted $\chi(D)$, is the set of not-always-zero bit positions of D

$$\chi(D) = \bigcup_{c \in D} \chi(c)$$

- The support weight of D is $w_s = |\chi(D)|$
- any r , where $1 \le r \le k$,the rth minimum support weight denoted

$d_r = d_r(C) = \min\{w_s(D) \mid D$ an [n,r] subcode of $C\}$

4

Notations and Background Information

- If all codewords are equally probable , and the intruder observes a vector y in the positions in X , then he obtains

$$\log \frac{|C|}{N_x(y)} \quad \text{bits of information}$$

- The expected(average)information in *h* positions is

$$e_h = e_h(c) = \frac{1}{\binom{n}{h}} \sum_{X \in S_h} \frac{1}{|C_x|} \sum_{y \in C_x} \log \frac{|C|}{N_x(y)}$$

- By convexity of the logarithm ,

$$e_h \geq \frac{1}{\binom{n}{h}} \sum_{X \in S_h} \log |C_x|$$

5

Lower Bound

- Let C be an [n,k] code generated by $(I_k \mid P)$ and let p= rank P . If $1 \leq h \leq n$

$$e_h \geq \frac{p\binom{n-1}{h-1} + k\binom{n-1}{h-1} - p\binom{n-2}{h-2}}{\binom{n}{h}} = \frac{hk}{n} + \frac{hp(n-h)}{n(n-1)}$$

Special case , P is a k- by-$(n-k)$ zero matrix then $e_h = \frac{hk}{n}$

6

Relation between e_{h+1} and e_h

$$e_{h+1} \geq e_h + \frac{k}{n-h} - \frac{e_h}{n-h}$$

Equality holds if the generator is $(I_k \mid 0)$

7

Upper Bound

- Let $1 \leq r \leq k$ and $0 \leq h \leq n$,then

$$e_h \leq k - r + \frac{h}{n} d_r$$

8

Further Problems and Conclusion

- Besides bounding the information function of a code , we must also add the ability of correcting to a code
- In order to protect our information from intruding , We can use above conditions to design a code against intruding

9