The Main Coding Theory Problem

Your name

Sažetak

Linear codes with good parameters can be constructed from algebraic curves over finite fields. Since Goppas orginal paper [1] in 1981, there has been a constant flow of research on (1) asympototic properties of these codes, (2) behaviour of these codes on different types of curves, (3) efficient decoding. Here g is the genus of the curve and m is a positive integer satisfying $n > m > 2g - 2$. An important consequence is that d satisfies $n - k + 1 \geq d \geq n - k + 1 - g$. These results are shown in Theorem 2.1 and Corollary 2.2

1 Introduction

The main definitions are briefly recalled. A linear q-ary $[n, k, d]$ code or an $[n, k, d]_q$ code C is subspace of $(F_q)^n$, where the dimension of C is

$$\dim C = k$$

and the minimum distance is

$$d(C) = d = \min_{x \in C \setminus \{0\}} \omega(x) = \min_{x \neq y} d(x, y),$$

where $\omega(x)$ is the weight of the word x and $d(x, y)$ is the Hamming distance between the words x and y. The information rate is

$$R = \frac{k}{n}$$

and the relative distance is

$$\delta = \frac{d}{n}$$

The Main Coding Theory Problem is to find good codes, those which maximise both R and δ. Let

$$A_q(n, d) = \max\{k | \text{ there exists a } q\text{-ary } [n, k, d] \text{ code}\}.$$

Also, let

$$\begin{aligned}\alpha(\delta) &= \limsup_{n\to\infty} n^{-1} A_q(n, [\delta n]) \\ &= \limsup R \text{ for codes with fixed } \delta\end{aligned}$$

Lema 1.1

$$\limsup_{n\to\infty} n^{-1} \log_q \left(\sum_{i=0}^{\lfloor \delta n \rfloor} \binom{n}{i} (q-1)^i \right) = H_q(\delta) \tag{1}$$

where H_q is an entrophy function given by

$$\begin{aligned}&H_q(0) = 0,\\ &H_q(t) = t\log_q(q-1) - t\log_q t - (1-t).\end{aligned}$$

Teorema 1.1 *(Gilbert-Varshamov)*

$$\alpha_q(\delta) \geq 1 - H_q(\delta).$$

For many years,1.1 was conjectured to be correct lower bound.

Definicija 1.1 *(1) A generator matrix G for C is a $k \times n$ matrix whose rows form basis for C*

(2) A parity check matrix H is an $(n-k) \times n$ matrix whose rowes form a basis for the dual code $C^{\perp}$; that is, $Hx^* = 0$ for all $x \in C$, where x^* denotes the transpose of x.

Then d can calculated from the next result.

Propozicija 1.1 *Every $d-1$ columns of H are linearly independent but some d columns are dependent*

Corollary 1.1 *The minimum distance d satisfies $d \leq n-k+1$*

Proof 1.1 From the proposition, $\operatorname{rank}(H) \geq d-1$. But, by definition, $\operatorname{rank}(H) = n-k$, whence the result. □

When equality is attained in this corollary, the code is /textitmaximum distance separable (MDS). A geometric view of of a code is given by considering the generator matrix G. Let $P^{k-1} = PG(k-1,q)$ be $(k-1)-$dimensional projective space over $F_q = GF(q)$. A projective $[n,k]-$system is a family of n