A new bound on the size of linear codes

Dott. Emanuele Bellini Prof. Massimiliano Sala [1]
Dott.sa Eleonora Guerrini [2]

1 - Università degli Studi di Trento, Lab di Matematica Industriale e Crittografia

2 - Ecole Normale Superieure de Lyon

12 Marzo 2012

Preliminary notions: a code C

Definition

Let $C \subseteq \mathbb{F}_q^n$, $C \neq \emptyset$. We say that C is an (n, q) **code**. Any $c \in C$ is a **word**.
Let $\phi : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$ be an injective function and let $C = \mathrm{Im}(\phi)$. We say that C is an (n, k, q) **systematic code**.
If C is a vector subspace of $(\mathbb{F}_q)^n$, then C is an (n, k, q) **linear** code.
$\mathbb{F} = \mathbb{F}_q$.

In a systematic code C any $c \in C$ can be seen as $c = (a, F(a))$ for (exactly) one $a \in \mathbb{F}^k$ and for an injective function $F : \mathbb{F}^k \to \mathbb{F}^{n-k}$.

Preliminary notions: distance of a code

Definition

We denote with d a number such that $1 \leq d \leq n$ to indicate the **hamming distance** of a code, which is the minimum number of elements which are different considering any possible combination of two different words in C.

Example

The whole $\mathbb{F}^n$ has distance 1.
$d = n$ in a systematic code is possible only if $k = 1$.

Preliminary notions: spheres

Definition

Let $l, m \in \mathbb{N}$ such that $l \leq m$. In $\mathbb{F}^m$, we denote by $B(l, m)$ the set of vectors with distance from the word 0 less than or equal to l, and we call it the **ball** (or **sphere**) centered in 0 of radius l.

Obviously, $B(l, m)$ is the set of vectors of weight less than or equal to l. So that:

$$|B(l, m)| = \sum_{j=0}^{l} \binom{m}{j} (q-1)^j.$$

The size problem

Definition

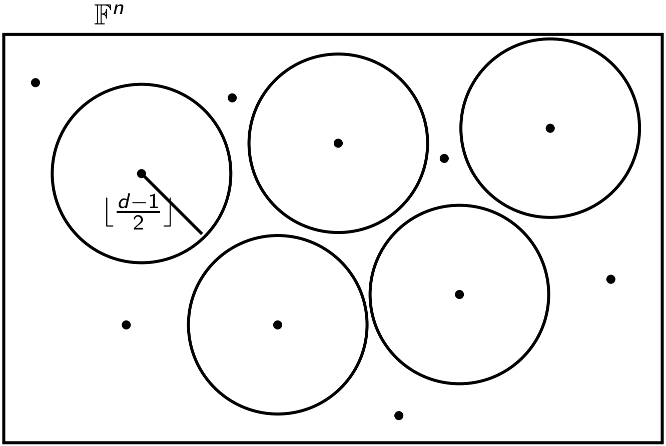
The number $A_q(n,d)$ denotes the maximum number of codewords in a code over $\mathbb{F}_q$ of length n and distance d.

Given parameters q, n, d, what can we say on k or equivalently on $A_q(n,d)$?

Some known bounds for $A_q(n, d)$

Singleton	$\rightarrow$	$A_q(n,d) \leq q^{n-d+1}$
Hamming	$\rightarrow$	$A_q(n,d) \leq \frac{q^n}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k}(q-1)^k}$
if $n(1-q^{-1}) < d$ **Plotkin**	$\rightarrow$	$A_q(n,d) \leq \lfloor \frac{d}{d-n(1-q^{-1})} \rfloor$
Johnson, Levenshtein, Elias,...	$\rightarrow$	more complicated formulas...
Only for linear codes: **Griesmer**	$\rightarrow$	$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$

A picture for the Hamming Bound



Bound A

Theorem

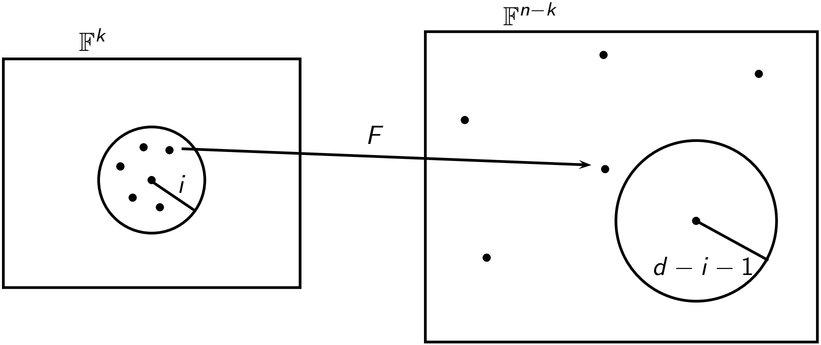
4 Let $d, i \in \mathbb{N}, d \geq 2$. Let n be such that there exists an (n, k, q) systematic code C with distance at least d and $n-1 \geq k \geq 1$. If $1 \leq i \leq \min\{\lfloor \frac{d-1}{2} \rfloor, k\}$, then

$$|B(i,k)| \leq |\mathbb{F}^{n-k} \setminus B(d-i-1, n-k)| + 1$$

that is

$$\sum_{j=0}^{i} \binom{k}{j}(q-1)^j \leq \sum_{j=d-i}^{n-k} \binom{n-k}{j}(q-1)^j + 1$$

Bound A - Sketch of proof



Bound A - Sketch of proof

Two steps:

1. prove that $F(B(i,k) \setminus \{0\}) \subseteq \mathbb{F}^{n-k} \setminus B_0(d-i-1, n-k)$
2. prove that $F' = F_{|_{B(i,k)}}$ is injective

We use that:

1. wlog $0 \in C$
2. if $c \in \mathbb{F}^k$ and $\mathrm{w}(c) \leq i$ then $\mathrm{w}(F(c)) \geq d-i$
3. if $c, c' \in \mathbb{F}^k$ and $\mathrm{w}(c), \mathrm{w}(c') \leq i$ then $\mathrm{d}(F(c), F(c')) \geq d-2i$

Bound B

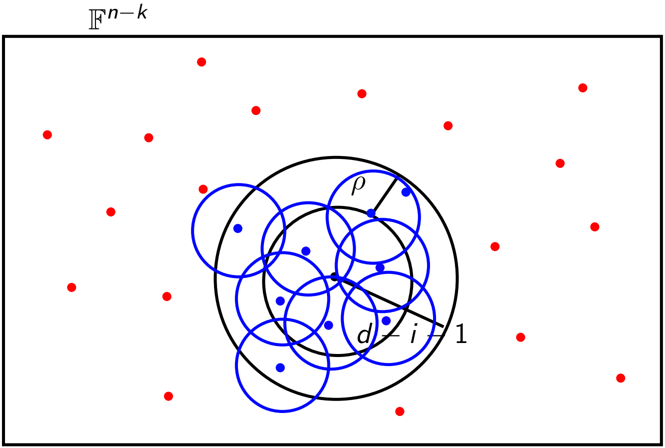
Theorem (Bound $\mathcal{B}$)

Let $n, k, d, i \in \mathbb{N}$. Let n be the smallest integer such that there exists an (n, k, q) systematic code with minimum distance at least d. If $n - 1 \geq k \geq 1$, $1 \leq i \leq \min\{\lfloor \frac{d-1}{2} \rfloor, k\}$, then

$$|B(i,k)| \leq A_q(n-k, d-2i) \setminus \frac{|B(i,n-k)|}{|B(d-2i-1,n-k)|} + 1$$

.

Bound B - Sketch of proof



Bound B - Sketch of proof

Consider the code $\mathcal{F} = F(B(i,k)) \subset \mathbb{F}^{n-k} \setminus B(d-i-1, n-k)$.
$\mathrm{d}(\mathcal{F}) \geq d - 2i$.
Consider the code C, the largest code of distance $d-2i$ in $\mathbb{F}^{n-k} \setminus B(d-i-1, n-k)$.
Consider the code $\bar{C}$, the largest code of distance $d-2i$ in $\mathbb{F}^{n-k}$ such that $C \subseteq \bar{C}$. Then:

$$|\mathcal{F}| \leq |C| \leq |\bar{C}| \leq A_q(n-k, d-2i)$$

We have:

$$C = \bar{C} \setminus \bar{C} \cap B(d-i-1, n-k)$$

So we can bound $|\bar{C}|$ from above using $A_q(n-k, d-2i)$, and $|\bar{C} \cap B(d-i-1, n-k)|$ from below, counting how many words of $\bar{C}$ are captured in the sphere.

Bound C - Conjecture

Theorem (Bound $\mathcal{C}$)

Let $n, k, d, i \in \mathbb{N}$. Let n be the smallest integer such that there exists an (n, k, q) systematic code with minimum distance at least d. If $n-1 \geq k \geq 1$, $1 \leq i \leq \min\{\lfloor \frac{d-1}{2} \rfloor, k\}$, then

$$|B(i,k)| \leq A_q(n-k, d-2i)\frac{|\mathbb{F}^{n-k} \setminus B(d-i-1, n-k)|}{|\mathbb{F}^{n-k}|} + 1$$

or, equivalently:

$$\sum_{j=0}^{i} \binom{k}{j}(q-1)^j \leq A_q(n-k, d-2i)\frac{\sum_{j=d-i}^{n-k} \binom{n-k}{j}(q-1)^j}{2^{n-k}} + 1$$

Some interesting results

	BB	BA	Jq	J2	Ha	Gr	Le	El	Pl
n = 19 d = 7	8	10	8	8	8	9	9	10	x
n = 20 d = 8	8	11	8	8	9	9	8	9	x
n = 27 d = 11	8	14	10	9	10	9	9	10	x
n = 28 d = 11	9	15	10	10	11	10	10	11	x

Grazie per l'attenzione!