Codes and Representation Theory

Ghid Maatouk
Joint work with Bertrand Meyer

ALGO Workshop
Jan 15, 2010

GV Bound for Linear Codes of Rate 1/2

Theorem (GV Bound for Linear Codes of Rate 1/2)

Let $B_{2n}(d)$ denotes the set of nonzero vectors of length $2n$ and weight at most d.
Then for every positive integer n there exists a linear code of parameters $[2n, n, d]$ satisfying

$$|B_{2n}(d)| \geq 2^n.$$

GV Bound for Linear Codes of Rate 1/2

Proof.

- Create an $n \times 2n$ check matrix uniformly at random to define a code C_{rand}.
- $X(w) = |\{x \in C_{rand}, wgt(x) \leq w\}| = \sum_{x \in B_{2n}(w)} X_x$.
- Can show that

$$\Pr[X(w) > 0] \leq E[X(w)] = |B_{2n}(w)| \frac{1}{2^n}.$$

- If $|B_{2n}(w)| < 2^n$, there exists a $[2n, n, d > w]$-code.

Improved Bound for Linear Codes of Rate 1/2

Theorem

[GZ08] There exists a positive constant b and an infinite sequence of integers n and $[2n, n, d]$ linear codes satisfying

$$|B_{2n}(d)| \geq bn2^n.$$

Double Circulant Codes

- Idea: do better by letting C_{rand} be a **double circulant code**.
- Check matrix:

$$H = [I_n|A] = \left[\begin{array}{ccccc|cccc} 1 & & & & & a_0 & a_{n-1} & \cdots & a_1 \\ & 1 & & & & a_1 & a_0 & \cdots & a_2 \\ & & \ddots & & & \vdots & & & \vdots \\ & & & & 1 & a_{n-1} & a_{n-2} & \cdots & a_0 \end{array}\right].$$

- Pick $a = (a_0, \cdots, a_{n-1})$ uniformly at random.

Double Circulant Codes

- Observation:

$$x = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) \in C_{rand}$$

$$\iff j.x = (x_{n-j+1}, \ldots, x_{n-j}, x_{2n-j+1}, \ldots, x_{2n-j}) \in C_{rand} \quad \forall j$$

- Can count over orbit representatives!

Upper Bounding the Probability of the Bad Event

- Let $B'_{2n}(w)$ be a set of representatives of the orbits of the elements of $B_{2n}(w)$.
- $X'(w) := \sum_{x \in B'_{2n}(w)} X_x = \sum_{x \in B_{2n}(w)} \frac{X_x}{l(x)}$.

Upper Bounding the Probability of the Bad Event

- Better bound on $\Pr[X(w) > 0]$.

$$\begin{aligned}\Pr[X(w) > 0] &= \Pr[X'(w) > 0] \\ &\leq E[X'(w)] \\ &= \sum_{d|n} \sum_{\substack{wgt(x)\leq w \\ l(x)=d}} \frac{E[X_x]}{d}.\end{aligned}$$

If n is prime,

$$\Pr[X(w) > 0] \leq \frac{E[X(w)]}{n}.$$

Improved Lower Bound in a Special Case

Theorem

[1] If n is prime and 2 is primitive modulo n, then there exist double circulant codes of parameters $[2n, n, d > w]$ for any positive w such that

$$2|B_{2n}(w)| < n2^n.$$

Proof Idea For a given word $x = (x_L, x_R)$, calculate $\Pr[x \in C_{rand}]$ by looking at the cyclic code generated by x_R.

Looking at Things Differently

- n prime, 2 primitive modulo n.
- Consider the action of the cyclic shift operator

$$L = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$ on the vectors of $\mathbb{F}_2^n$.

- L diagonalizable over Galois field $\mathbb{F}_2(\omega) \simeq \mathbb{F}_{2^{n-1}}$ where ω is an nth root of 1.

Eigenvectors:

$$x_0 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}, x_1 = \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{n-1} \end{pmatrix}, x_2 = \begin{pmatrix} 1 \\ \omega^2 \\ \omega^4 \\ \vdots \\ \omega^{2(n-1)} \end{pmatrix} \dots$$

$$x_{n-1} = \begin{pmatrix} 1 \\ \omega^{n-1} \\ \vdots \\ \omega^{(n-1)(n-1)} \end{pmatrix}$$

Diagonal Action

- Consider the action of the double cyclic shift operator

$$\begin{bmatrix} L & 0 \\ 0 & L \end{bmatrix}$$

on the vectors of $\mathbb{F}_2^{2n}$.

- Eigenvectors over $\mathbb{F}_{2^{n-1}}$ are of the form $\begin{pmatrix} x_i \\ 0 \end{pmatrix}$ or $\begin{pmatrix} 0 \\ x_i \end{pmatrix}$.
- Basis for $\mathbb{F}_{2^{n-1}}^{2n}$:

$$\left\{ \begin{pmatrix} x_0 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} x_{n-1} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x_0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ x_{n-1} \end{pmatrix} \right\}.$$

Goal:describe double circulant codes of length $2n$ over $\mathbb{F}_2$, i.e.,

- Subspaces of $\mathbb{F}_{2^{n}-1}^{2n}$ with basis of the form $[I_n|A]$, A circulant matrix
- Invariant under the Frobenius map

$$\sigma : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1^2 \\ \vdots \\ x_n^2 \end{pmatrix}.$$

- Solve for B in

$$B \begin{bmatrix} F & 0 \\ 0 & F \end{bmatrix} = [I_n | A], \text{ with } A \text{ circulant.}$$

- Get

$$B = \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & \alpha & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & \beta & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & \beta^2 & \cdots & 0 \\ & & & \ddots & & & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & \beta^{n-1} \end{array}\right],$$

$$\alpha \in \mathbb{F}_2, \beta \in \mathbb{F}_{2^{n-1}}.$$

- 2^n subspaces invariant under circular shift.
- Taking conjugates of β ensures invariance under Frobenius.

Modules

Action of a group G on a vector space V : define a multiplication between a group element g and a vector v such that

- $vg \in V$
- $v(gh) = (vg)h$
- $v1 = v$
- $(\lambda v)g = \lambda(vg)$
- $(u + v)g = ug + vg$.

V is a G-**module.**

Modules

Our case:

- $G =< \sigma, \sigma^n = 1 >$ generated by

$$\sigma : \mathbb{F}_2^{2n} \longrightarrow \mathbb{F}_2^{2n}$$

$$(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) \mapsto (x_n, x_1, \ldots, x_{n-1}, x_{2n}, x_{n+1}, \ldots, x_{2n-1})$$

- Acts on $\mathbb{F}_2^{2n}$.

Modules

- G-Modules:

$$M_\beta = \left\langle \begin{pmatrix} x_1 \\ \beta x_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ \beta^2 x_2 \end{pmatrix}, \ldots, \begin{pmatrix} x_{n-1} \\ \beta^{n-1} x_{n-1} \end{pmatrix} \right\rangle$$

- **Irreducible** modules: contain no nontrivial proper submodules.

Back to Counting Argument

- n prime, 2 primitive modulo n.
- $G =< \sigma, \sigma^n = 1 >$ acts on $\mathbb{F}_2^{2n}$
- $M_1, \ldots, M_L$ irreducible G-modules of $\mathbb{F}_2^{2n}$, $L = 2^{n-1}$.

Theorem

If w is such that

$$|B_{2n}(w)| < nL,$$

then there exists an i such that M_i does not contain nonzero words of weight w or less.

Back to Counting Argument

Proof.

- M_i irreducible for all i: $M_i \cap M_j = \{0\}$ for all $i \neq j$.
- Double circulant property: if $x \in M_i$, then all of $\mathrm{orb}(x) \subseteq M_i$.
- $|\mathrm{orb}(x)| = n$.

If every M_i contains an element of $B_{2n}(w)$, then every M_i contains $\geq n$ elements of $B_{2n}(w)$. But then

$$|B_{2n}(w)| \geq L.n.$$

Ingredients

- G finite group acting on $\mathbb{F}_q^n$.
- Action of G must be weight-preserving!
- $G \leq GL_n(\mathbb{F}_q)$, elements of G are permutation matrices acting on $\{1, \ldots, n\}$.

Diagonal Action

- Let G act diagonally on $\mathbb{F}_q^n \oplus \mathbb{F}_q^n$.
- $M_1, \ldots, M_L$ distinct irreducible G-modules of dimension k.

Theorem

If

$$\sum_{x \in B_{2n}(w)} \frac{1}{|orb(x)|} < L,$$

then there exists a $[2m, k, d > w]_q$*- code.*

Proof.

Counting argument. □

Centralizer

- Interested in the diagonal action of G on two copies of a module M.
- Introducing diversity: let $\phi \in GL_n(\mathbb{F}_q)$.
- $M_\phi = \{(\mu, \phi(\mu)), \mu \in M\}$ is a G-module if ϕ commutes with the action of G.
- Interested in groups with large centralizers.

2-transitive action

Definition

G acting on V. The action of G is **transitive** if $\forall a, b \in V$, there is a group element g such that $g(a) = b$.
The action of G is **2-transitive** if $\forall a_1 \neq a_2, b_1 \neq b_2 \in V$, there is a group element g such that $g(a_1) = b_1, g(a_2) = b_2$.

- Can we consider groups whose action is 2-transitive?

2-transitive action

- Let $A = (a_{ij}) \in C(G)$. Then for any $\Pi \in G$,

$$\Pi^{-1} A \Pi = A.$$

- Equivalent to

$$a_{\pi(i)\pi(j)} = a_{ij} \ \forall i, j.$$

- Action of G is 2-transitive: for all $i \neq j, l \neq k$, there exists a π such that $\pi(i) = l, \pi(j) = k$, so must have $a_{ij} = a_{lk}$.
- Action of G is transitive: on the diagonal, must have $a_{ii} = a_{jj}$ for all i, j.
- $|C(G)| < q^2$.

Counting Codes

- G finite group acting on V. Have finitely many types of irreducible modules M_i.
- $V = \bigoplus_{i=1}^{t} M_i^{\alpha_i}$
- Given $\beta_i \leq \alpha_i$, in how many ways can $N = \bigoplus_{i=1}^{t} M_i^{\beta_i}$ be mapped into V?

Counting Codes

- Schur's lemma:
  - If there exists a homomorphism between two irreducible G-modules, it is either trivial or an isomorphism
  - Isomorphism between irreducible G-modules can only be $\lambda \times Id$.
- Thus can only map $M_i^{\beta_i}$ to $M_i^{\alpha_i}$. In how many ways?

$$\frac{(q^{\alpha_i}-1)(q^{\alpha_i}-q)\cdots(q^{\alpha_i}-q^{\beta_i-1})}{(q^{\beta_i}-1)\cdots(q^{\beta_i}-q^{\beta_i-1})}.$$

- Will not give us the exponential factor in n that we are looking for.

Starting with Good Codes

- Start with codes that we already know lie on the GV bound.
  - Goppa Codes
- What can we say about the automorphism group of such codes?
- Goppa codes: consider automorphisms of the form $x \mapsto ax + b$. Can we find many Goppa codes invariant under such automorphisms?

Relaxing Constraints

- Underlying assumption: G acts on $\mathbb{F}_q^n$, q does not divide $|G|$. Then can apply **Maschke's theorem**, which allows us to completely decompose a space into irreducible modules.
- Can we gain something by discarding this assumption?
- May be enough to have $M_i \cap M_j$ small.
- Work with **indecomposable** modules; look at d-wise intersections of such modules.
- Can we upper-bound size of d-wise intersections asymptotically in the dimension of the modules?

P. Gaborit and G. Zémor, "Asymptotic Improvement of the Gilbert-Varshamov Bound for Linear Codes", *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3865-3872, Sept. 2008.