On Perfect Codes in the Johnson Graph

Natalia Silberstein

Tuvi Etzion

Computer Science Department

Technion - Israel Institute of Technology

Outline

- Background
  - Basic definitions
  - t-designs
  - Steiner systems
- 1-perfect codes in $J(n, w)$
  - Necessary conditions
  - Improvement of Roos' bound
- 2-perfect codes in $J(2w, w)$
  - Necessary conditions
  - No 2-perfect codes in $J(2w, w)$ for $w < 1.97\text{x}10^{7655}$

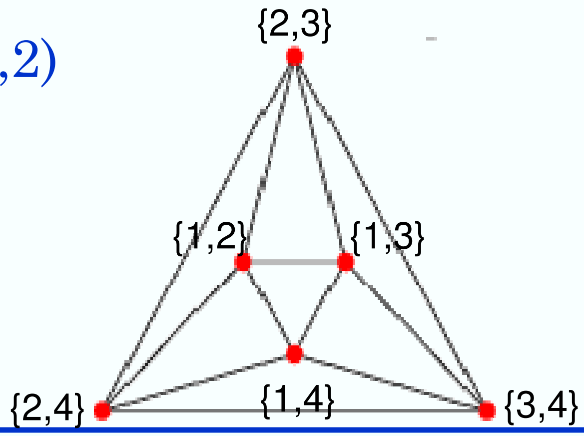
Basic Definitions

- The Johnson space V_w^n, $0 \leq w \leq n$, consists of all w-subsets of a fixed n-set $N = \{1, 2, \ldots, n\}$.
- with the Johnson space we associate the Johnson graph $J(n, w)$:
  - Vertex set: V_w^n
  - Edges set: Two vertices u and v are adjacent if and only if $|u \cap v| = w - 1$

Basic Definitions

- The Johnson space V_w^n, $0 \le w \le n$, consists of all w-subsets of a fixed n-set $N = \{1, 2, \ldots, n\}$.
- with the Johnson space we associate the Johnson graph $J(n, w)$:
  - Vertex set: V_w^n
  - Edges set: Two vertices u and v are adjacent if and only if $|u \cap v| = w - 1$

Example: $J(4,2)$



Basic Definitions

- A code C in $J(n, w)$ is a subset of V_w^n
- A code C in $J(n, w)$ can be described as a binary code of length n and constant weight w
  - From w-subset $S \in V_w^n$ construct a characteristic binary vector of length n and weight w with *ones* in the positions of S and *zeroes* in the positions of $N \setminus S$
- The Johnson distance between two w-subsets is half of the number of coordinates where their characteristic vectors differ.

Perfect Codes in $J(n,w)$

- A code C in $J(n, w)$ is called an e-perfect code if the e-spheres with centers at the codewords of C form a partition of V_w^n.
- The trivial perfect codes in $J(n, w)$ are:
  - V_w^n is 0 - perfect.
  - Any $\{v\}, v \in V_w^n, w \le n - w$, is w - perfect.
  - If $n = 2w$, w odd, any pair of disjoint w - subsets is e - perfect with $e = (w\text{-}1)/2$.
- Delsarte (1973) conjectured that there are no perfect codes in $J(n, w)$, except for trivial perfect codes.

Perfect Codes in $J(n,w)$

- [Roos1983] If there exists an e-perfect code in $J(n, w)$ then $n \le (w-1)\dfrac{2e+1}{e}$.
- [Etzion,Schwartz2004] There are no nontrivial
  2-perfect codes in $J(n, w)$ for all $n < 40000$;
  3-perfect, 7-perfect, 8-perfect codes in $J(n, w)$.
- [Etzion,Schwartz2004] There are no perfect codes in :
  - $J(2w+p^i, w)$, p is a prime and $i \ge 1$
  - $J(2w+pq, w)$, p and q primes, $q < p$, and $p \ne 2q-1$
- [Gordon2006] There are no 1- perfect codes in $J(n, w)$ for all $n < 2^{250}$.

Codes in $J(n,w)$ and Block Designs

Let t, n, w, λ be integers with $n > w \geq t$, and $\lambda > 0$

- A $t-(n, w, \lambda)$ design is a collection C of w-subsets, called blocks, of N, such that each t-subset of N is contained in exactly λ blocks of C.
- Such C is a code in $J(n, w)$.
- The largest t for which a code C in $J(n, w)$ is a t-design is called the strength of the code.
- A necessary condition for a $t-(n, w, \lambda)$ design to exist is that the numbers $\lambda \binom{n-i}{t-i} / \binom{w-i}{t-i}$ must be integers, $0 \leq i \leq t$.

Codes in $J(n,w)$ and Block Designs

- The complement of an e-perfect code in $J(n, w)$ is an e-perfect code in $J(n,n\text{-}w)$.
- Then we assume that $n \geq 2w$ or $n = 2w+a$.
- If the code C has strength φ, then for each t, $0 \leq t \leq \varphi$, it is a t-$(2w+a, w, \lambda_t)$ design, where $\lambda_t = \binom{2w+a-t}{w-t} / \Phi_e(w,a)$ and $\Phi_e(w,a) = \sum_{i=0}^{e} \binom{w}{i}\binom{w+a}{i}$ is the size of an e-sphere.

Codes in $J(n,w)$ and Block Designs

- Define the polynomial

$$\sigma_e(w,a,t)=\sum_{i=0}^{e}(-1)^i\binom{t}{i}\sum_{j=0}^{e-i}\binom{w-i}{j}\binom{w+a-t+i}{i+j}$$

- ***Theorem*** [Etzion, Schwartz, 2004] If there is an e-perfect code C in $J(2w+a, w)$ with strength φ, then φ is the smallest positive integer for which $\sigma_e(w, a, \varphi+1)=0$.

Codes in $J(n,w)$ and Steiner Systems

- t - (n, w, λ) design with $\lambda = 1$ is called Steiner system S(t, w, n).
- [Etzion, 1996] If an e-perfect code exists in $J(n, w)$, then the following Steiner systems must exist:
  - $S(2, e+2, w+2)$
  - $S(2, e+2, \text{n-}w+2)$
  - $S(2, e+2, w-e+1)$
  - $S(2, e+2, n-w-e+1)$
  - $S(e+1, 2e+1, w)$
  - $S(e+1, 2e+1, n-w)$

1-perfect codes in $J(n,w)$. New results

- ***Theorem 1.*** Assume there exists an 1-perfect code C in $J(2w + a, w)$ with strength $\varphi = w - d$ for some $d \geq 0$. Then
  - $d > 1$, $d \equiv 0$ or $1 \pmod 3$,
  - $a = \dfrac{w - d^2 + d - 1}{d - 1}$,
  - and $\dfrac{\prod_{i=0}^{d-2} (wd - (d + i(d-1)))}{(d-1)!(d-1)^{d-1} d(w - d + 1)} \in \mathbb{Z}$

1-perfect codes in $J(n,w)$ Improvement of Roos' bound

- Roos' bound for 1-perfect codes:

$$n = 2w + a \le 3(w - 1) \Rightarrow a \le w - 3.$$

we improve this bound:

- ***Theorem 2.*** If an 1-perfect code exists in $J(2w + a, w)$, then $a < \frac{w}{11}$.

Proof of Theorem 2: $a < w/11$

- Let C be an 1-perfect code in $J(2w+a, w)$ with strength w-d. Then by Theorem 1 we have $d > 1$, $d \equiv 0$ or $1 \pmod 3$, and

$$a = \frac{w - d^2 + d - 1}{d - 1} \ (*), \qquad \frac{\prod_{i=0}^{d-2}(wd - (d + i(d-1)))}{(d-1)!\,(d-1)^{d-1}\, d\,(w - d + 1)} \in \mathbb{Z} \ (**)$$

- Assume $d = 3$. Then by (**) $\frac{(w-1)(3w-5)}{8(w-2)} \in Z$, which is impossible since gcd(w-1, w-2) = gcd(3w-5, w-2) = 1. Hence $d > 3$.

- Assume $d = 4$. Then by (**) $\frac{4(w-1)(4w-7)2(2w-5)}{3!3^3 4(w-3)} \in \mathbb{Z}$.

Since gcd(w -3, w -1) ∈ {1, 2}, gcd(w - 3, 4w -7) ∈ {1, 5}, and gcd(w -3, 2w -5) = 1, it follows that $w - 3 \leq 2 \cdot 5$.
But by (*), $a = (w - 13) / 3$, hence $w > 13$. Thus $d > 4$.

Proof of Theorem 2: $a < w/11$

- Similarly we obtain contradiction for $d = 6$, $d = 7$, $d = 9$, and $d = 10$. Since $d \equiv 0, 1 \pmod 3$ then $d \geq 12$, and thus by (*)

$$a \leq \frac{w - 12^2 + 12 - 1}{11} = \frac{w - 133}{11} < \frac{w}{11}. \quad \square$$

- As the value of d is growing, considering the divisibility condition becomes more complicated.
- The same method can be used for further improving the Roos' bound.

2-perfect codes in $J(2w,w)$

Theorem 3. If a 2 – perfect code C exists in $J(2w, w)$, then there is an integer $m \geq 0$ such that

- (c.1) $w = \dfrac{(1+\sqrt{2})^{2m+1} + (1-\sqrt{2})^{2m+1} + 6}{4}$, and
- (c.2) $\gamma := \sqrt{2}((1+\sqrt{2})^{2m} - (1-\sqrt{2})^{2m}) + 1$ is a square of some integer

- *Proof:* We find the roots of the polynomial

$$\sigma_e(w,a,t) = \sum_{i=0}^{e} (-1)^i \binom{t}{i} \sum_{j=0}^{e-i} \binom{w-i}{j} \binom{w+a-t+i}{i+j}$$

for $e = 2$ and $a = 0$ and by this obtain the strength of C:

2-perfect codes in $J(2w,w)$
Proof of Theorem 3.

- The strength of a 2-perfect code in $J(2w, w)$ is

$$\frac{1}{2}\left(-1+2w-\sqrt{8w-11\pm 4\sqrt{5-6w+2w^2}}\right)$$

- We have two constraints:
  - $\sqrt{5-6w+2w^2} \in \mathbb{Z}$
  - $\sqrt{8w-11\pm 4\sqrt{5-6w+2w^2}} \in \mathbb{Z}$

2-perfect codes in $J(2w,w)$. Proof. of Theorem 3.

- The first constraint is $\sqrt{5-6w+2w^2} \in \mathbb{Z}$, then $\exists y \in \mathbb{Z}$, $y^2 = 5-6w+2w^2 \Rightarrow (2w-3)^2 - 2y^2 = -1$.

  Let $x = 2w - 3$. Then we get Pell equation $x^2 - 2y^2 = -1$ with a family of solutions:

  $$x = \frac{(1+\sqrt{2})^{2m+1} + (1-\sqrt{2})^{2m+1}}{2} \text{ and } y = \frac{(1+\sqrt{2})^{2m+1} - (1-\sqrt{2})^{2m+1}}{2\sqrt{2}}$$

  for some integer $m \geq 0$.

  Then $$w = \frac{(1+\sqrt{2})^{2m+1} + (1-\sqrt{2})^{2m+1} + 6}{4} \quad \text{(c.1)}$$

2-perfect codes in $J(2w,w)$. Proof. of Theorem 3.

- The second constraint is $\sqrt{8w-11\pm 4\sqrt{5-6w+2w^2}}\in\mathbb{Z}$

$$+:\quad \exists\alpha\in\mathbb{Z},\alpha^2=8w-11+4y=4(x+y)+1.$$
$$-:\quad \exists\beta\in\mathbb{Z},\beta^2=8w-11-4y=4(x-y)+1$$

since $x=\dfrac{(1+\sqrt{2})^{2m+1}+(1-\sqrt{2})^{2m+1}}{2}$ and $y=\dfrac{(1+\sqrt{2})^{2m+1}-(1-\sqrt{2})^{2m+1}}{2\sqrt{2}}$

we obtain

$$\alpha^2=\sqrt{2}((1+\sqrt{2})^{2m+2}-(1-\sqrt{2})^{2m+2})+1,$$
$$\beta^2=\sqrt{2}((1+\sqrt{2})^{2m}-(1-\sqrt{2})^{2m})+1$$

that proves (c.2). □

2-perfect codes in $J(2w,w)$

We examine the conditions of Theorem 3 for $1 \le m \le 10000$. The only values of m which satisfy (c.2) are 0, 1, and 2, where the corresponding values of w are 2, 5, 22, respectively.

It was proved by Etzion and Schwartz (2004) that there are no 2-perfect codes in $J(n, w)$ for all $n \le 40000$.

Thus for $w \le 1.97 \times 10^{7655}$ (considering $m = 10000$), there is no 2-perfect code in $J(2w, w)$.

Conclusion

- 1-perfect codes in $J(n,w)$
- 2-perfect codes in $J(2w,w)$
- Another techniques:
  - Regularity of perfect codes

    [W.J. Martin, "Completely regular subsets", Ph.D. dissertation, 1992;
    T. Etzion and M. Schwartz,"Perfect Constant-Weight Codes", IEEE Trans.on Inform. Theory, 2004]
  - Configuration distribution

    [T. Etzion, " Configuration Distribution and Designs of Codes in the Johnson Scheme", Journal of Combinatorial Designs, 2006]
  - Moments

    [T. Etzion, " Configuration Distribution and Designs of Codes in the Johnson Scheme", Journal of Combinatorial Designs, 2006;
    N.Silberstein, "Properties of Codes in the Johnson Scheme," M.Sc. Thesis, 2007]

Thank you!