SOME CONNECTIONS BETWEEN SELF-DUAL CODES, COMBINATORIAL DESIGNS AND SECRET-SHARING SCHEMES

Stefka Bouyuklieva, Zlatko Varbanov

Department of Mathematics and Informatics

Veliko Tarnovo University, Bulgaria

Algebraic Combinatorics and Applications 2010

Thurnau, April 11–18, 2010

INTRODUCTION

Secret sharing is an important topic in cryptography and has applications in information security.

The age-old way to share a secret, such as the 3-digit combination 17-14-92 (combination with 100 positions) is to give part of the secret to each user: 17 to Andrew, 14 to Bryan, and 92 to Chris.

Shamir (1979) and Blakely (1979) – (S, T) *threshold schemes for secret sharing*

A secret is transformed into a list of S shares in such manner that:

(P1) knowledge of any T shares reveals the secret, but

(P2) knowledge of T-1 or fewer shares gives no information whatsoever about the secret.

McEliece and Sarwate (1981) – a formulation of (S, T) threshold schemes in terms of q-ary MDS codes of block length $n = S + 1$ with q^k codewords.

SECRET-SHARING

Secret sharing scheme – sharing a secret among a finite set of people or entities such that only some distinguished subsets of these have access to the secret.

Example:

$$S = \{s_1, s_2, \ldots, s_n\}, \quad U = \{u_1, u_2, \ldots, u_p\}, \quad p > n$$

$$U^* = \{u_{s_1}, u_{s_2}, \ldots, u_{s_n}\}$$

Access structure – the collection of all such distinguished subsets that have access to the secret.

ACCESS STRUCTURE

If $\mathcal{P}$ is the set of parties involved in the secret-sharing, then

$$\Gamma = \{A \subset \mathcal{P} : \ A \text{ can uncover the secret}\}$$

$A \in \Gamma$ - **minimum access group** if

$$B \in \Gamma \text{ and } B \subseteq A \text{ implies } B = A$$

$$\overline{\Gamma} = \{A \mid A \text{ is a minimum access group}\}$$

$\overline{\Gamma}$ - the **minimum access structure**.

In general, determining the minimum access structure is a difficult problem.

BINARY LINEAR CODES

$GF(2)$ – a field with 2 elements.

Binary linear $[n, k]$ **code** C **of length n** – k-dimensional linear subspace of $GF(2)^n$.

Weight of a codeword $c \in C$ $(wt(c))$ – the number of nonzero components of c.

Minimum weight (distance):
$d = d(C) = min\{wt(c) | c \in C, c \neq 0\} \rightarrow [n, k, d]$ code.

Generator matrix of C – $k \times n$ matrix with entries in $GF(2)$ whose rows are a basis of C.

Weight enumerator of C: $C(y) = \sum_{i=0}^{n} A_i y^i$

SELF-DUAL CODES

- **Inner product** – $x.y = \sum_{i=1}^{n} x_i y_i, \quad x, y \in GF(2)^n$
- **Dual code** – $C^{\perp} = \{x \in GF(2)^n \mid x.c = 0,\ \forall c \in C\}$
- C – **self-orthogonal** code if $C \subseteq C^{\perp}$
- C – **self-dual** code if $C = C^{\perp}$ $(k = n/2)$
- All codewords in a binary self-orthogonal code have even weights
- **Doubly-even** code – all its weights are divisible by 4
- **Singly-even** self-dual code – contains a codeword of weight $w \equiv 2 \pmod 4$

EXTREMAL SELF-DUAL CODES

If C is a binary self-dual $[n, n/2, d]$ code then

$$d \leq 4[n/24] + 4$$

except when $n \equiv 22 \pmod{24}$ when

$$d \leq 4[n/24] + 6$$

When n is a multiple of 24, any code meeting the bound must be doubly-even.

THE SHADOW OF A SINGLY EVEN CODE

C - singly even self-dual $[n, k = n/2, d]$ code

C_0 - its doubly even subcode:

$$C_0 = \{v \in C \mid wt(v) \equiv 0 \pmod 4\}$$

$$dim C_0 = k - 1$$

$$C_2 = \{v \in C \mid wt(v) \equiv 2 \pmod 4\}$$

$$C = C_0 \cup C_2$$

$$\Rightarrow C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$$

$S = C_0^{\perp} \setminus C = C_1 \cup C_3$ - the shadow of C

$t-(v,k,\lambda)$ DESIGNS

A $t-(v,k,\lambda)$ **design** is:

- a set of v points $\mathcal{P}$;
- a family of blocks $\mathcal{B}=\{B\subset\mathcal{P},|B|=k\}$;
- an incidence relation between them such that $v=|\mathcal{P}|$, every block is incident with precisely k points, and every t distinct points are incident with λ blocks.

Any t-design is also a $s-(v,k,\lambda_s)$ design for $s\le t$:

$$\lambda_s=\frac{(v-s)}{(k-s)}\lambda_{s+1}(s=1,\ldots,t-1),\;\;\lambda_t=\lambda$$

Assmus-Mattson Theorem

Binary case:

- C – $[n, k, d]$ binary linear code;

- $C^{\perp}$ – its orthogonal $[n, n-k, d^{\perp}]$ code;

- t – an integer, $0 < t < d$, such that $C^{\perp}$ has not more than $d - t$ nonzero weights $w \leq n - t$.

Then:

- the supports of all codewords in C of weight u form a t-design;

- the supports of all codewords in $C^{\perp}$ of weight w, $d^{\perp} \leq w \leq n - t$, form a t-design.

SECRET-SHARING ($n-1$ PARTIES)

- $s \in GF(q)$ - the secret;
- $G = (G_0 G_1 \ldots G_{n-1})$ - a generator matrix of a code C of length n;
- $z \in GF(q)^k$ - the information vector, $zG_0 = s$;
- $u = zG$;
- to each party we assign $u_i, i = 1, \ldots, n-1$;

A scheme is said to be *perfect* if a group of shares either determines the secret or gives no information about the secret.

COMPUTING THE SECRET

s is determined by the set of shares $\{u_{i_1}, u_{i_2}, \ldots, u_{i_m}\}$

$$\Longleftrightarrow G_0 = \sum_{j=1}^{m} x_j G_{i_j},\ 1 \leq i_1 < \cdots < i_m \leq n-1$$

$$\Longleftrightarrow \exists (1, 0, ..., 0, c_{i_1}, 0, ..., 0, c_{i_m}, 0.., 0) \in C^{\perp},\ (c_{i_1}, \ldots, c_{i_m}) \neq 0$$

So by solving this linear equation, we find x_j and from then on the secret by

$$s = zG_0 = \sum_{j=1}^{m} x_j z G_{i_j} = \sum_{j=1}^{m} x_j u_{i_j}$$

.

Secret-sharing based on an SD code

Dougherty, Mesnager, Sole, 2008

D_i - the 1-design formed from the vectors of weight i

$$\Gamma = \{A \mid A \text{ is the support of a vector } v \in C \text{ with } v_0 = 1\}.$$

- Any group of size less than $d-1$ cannot recover the secret.
- There are $\lambda_1(D_i)$ groups of size $i-1$ that can recover the secret.
- It is perfect, which means that a group of shares either determines the secret or gives no information about the secret.
- When the parties come together $\lfloor \frac{d-1}{2} \rfloor$ cheaters can be found.

Secret-sharing based on an SD code

Bouyuklieva, Varbanov, 2009

C - a singly-even SD $[n, n/2, d]$ code with $wt(S) = 1$. Then, the vectors in C_2 (up to equivalence) are in the form $(1, c_1, c_2, \ldots, c_{n-1})$.

- Any group of size less than $d - 1$ cannot recover the secret.
- There are A_i groups of size $i - 1$ that can recover the secret ($i \equiv 2 \ (mod\ 4)$).
- It is perfect, which means that a group of shares either determines the secret or gives no information about the secret.
- When the parties come together $\lfloor \frac{d-1}{2} \rfloor$ cheaters can be found.

TWO-PART SECRET SHARING

Bouyuklieva, Varbanov, 2009

- $s' \in GF(q)$ - the second part of the secret;
- $z \in GF(q)^k$, $s' = s + zG_1 + zG_2 = z(G_0 + G_1 + G_2)$;
- $u = zG$, to each party we assign $u_i, i = 1, \dots, n-1$;

s' is determined by the set of shares $\{u_{i_3}, u_{i_4}, \dots, u_{i_m}\}$

$$\Longleftrightarrow G_2 = G_0 + G_1 + \sum_{j=3}^{m} x_j G_{i_j},\ 1 \le i_1 < \cdots < i_m \le n-1$$

$$\Longleftrightarrow \exists(1,1,1,0,...,0,c_{i_3},0,...,0,c_{i_m},0..,0) \in C^{\perp},\ (c_{i_3},\dots,c_{i_m}) \neq 0$$

TWO-PART SECRET SHARING

Bouyuklieva, Varbanov, 2009

Let C be a binary singly-even SD $[n, n/2, d]$ code with the properties:

- $wt(S) = 1$;
- the set of codewords of weight i in C_0 without the common zero coordinate holds a 2-design.

Then the access structure of the two parts are:

$$\Gamma_1 = \{A \mid A \text{ is the support of a vector } v \in C_2 \ (v_0 = 1)\}.$$

$$\Gamma_2 = \{A \mid A \text{ is the support of a vector } v \in C_2$$
$$\text{with } v_0 = v_1 = v_2 = 1\}.$$

TWO-PART SECRET SHARING

Let C be a binary doubly-even SD $[n, n/2, d]$ code with the property that the set of codewords of weight i in C holds a $3-(v, k, \lambda)$ design where $v = n$ and $k = i$.

Then the access structure of the two parts are:

$$\Gamma_1 = \{A \mid A \text{ is the support of a vector } v \in C \quad \text{with } v_0 = 1\}.$$

$$\Gamma_2 = \{A \mid A \text{ is the support of a vector } v \in C$$
$$\text{with } v_0 = v_1 = v_2 = 1\}.$$

Lets mention, that if a group of participants can recover the second part, to recover then the first part they need the participants 1 and 2, in general. But there are groups which can recover only the first part but not the second.

RESULTS (ONE-PART)

Let C be singly-even SD code with parameters:

- $[24m+18, 12m+9, 4m+4]$ or
- $[24m+10, 12m+5, 4m+2]$ or
- $[24m+2, 12m+1, 4m+2]$

In these cases there exist codes with $wt(S) = 1$.

$$\Gamma = \{A \mid A \text{ is the support of a vector } v \in C_2\}.$$

Example: C is $[42, 21, 8]$ code with $wt(S) = 1$ and weight enumerator $1 + 164y^8 + 697y^{10} + \ldots + 164y^{34} + y^{42}$.

The access structure contains 164 groups of size 7, 697 groups of size 9, etc.

RESULTS (TWO-PART)

Let C be singly-even SD $[24m+2, 12m+1, 4m+2]$ code with $wt(S) = 1$. In this case the set of codewords of weight i in C_2 (without the common all-one coordinate) holds a 2-design.

Example: C – singly-even SD $[50, 25, 10]$ code with $wt(S) = 1$ and weight enumerator $1 + 196y^{10} + 11368y^{12} + \ldots + y^{50}$.

- For the first part of the secret, the access structure contains 196 groups of size 9.
- For the second part we take these 36 blocks of D that have 1 in the first position. Without the first point, the blocks of D hold $1-(48, 8, 6)$ design D_1.
- We take these 6 blocks of D_1 that have 1 in the first position. Then, for the second part of the secret, the access structure consists of 6 groups of size 7.

RESULTS (TWO-PART)

- To recover the two-part secret should first be used the groups of size 7. They recover the second part of the secret.
- After that to recover the other part of the secret we use these groups (they are of size 8 already) and the other 30 groups of size 8. We add a new participant that has ones in these 36 groups (the other entries are 0).
- At last, we use the obtained 36 groups of size 9, and the other 160 groups of size 9 to recover the first part of the secret.

RESULTS (TWO-PART)

Let C be doubly-even extremal SD $[24m+8, 12m+4, 4m+4]$ code. In this case the set of codewords of weight i in C holds a 3-design.

Example: C – doubly-even extremal SD $[32, 16, 8]$ code with weight enumerator $1 + 620y^8 + 13888y^{12} + \ldots + y^{32}$. The set of the codewords of weight 8 holds $3-(32, 8, 7)$ design D.

- There are 155 blocks with 1 in the first position. Then, for the first part of the secret, the access structure contains 155 groups of size 7. These blocks without first point hold $2-(31, 7, 7)$ design D'.
- For the second part we take these 35 blocks of D' that have 1 in the first position. Without the first point, these blocks hold $1-(30, 6, 7)$ design D''.
- We take these 7 blocks of D'' that have 1 in the first position. Then, for the second part of the secret, the access structure consists of 7 groups of size 5.

RESULTS (TWO-PART)

- To recover the two-part secret should first be used the groups of size 5. They recover the second part of the secret.

- After that to recover the other part of the secret we use these groups (they are of size 6 already) and the other 28 groups of size 6. We add a new participant that has ones in these 35 groups (the other entries are 0).

- At last, we use the obtained 35 groups of size 7, and the other 120 groups of size 7 to recover the first part of the secret.

References

[1] R. J. McEliece, D. V. Sarwate, ”On sharing secrets and Reed-Solomon codes”, Comm. ACM 24 (1981), no.9, pp.583–584.

[2] J. L. Massey, ”Some applications of coding theory in cryptography”, Codes and Ciphers, Cryptography and Coding IV (1995), Formara Lt, Esses, England, pp.33–47.

[3] S. T. Dougherty, S. Mesnager, P. Sole, ”Secret sharing schemes based on self–dual codes”, Proc. IEEE Inf. Theory Workshop, ITW 2008, Porto, Portugal.

THANKS FOR YOUR ATTENTION!