

Some Applications of Bounds for Designs to the Cryptography

Svetla Nikova* Ventsislav Nikov
Department of Mathematics and Informatics
Veliko Tarnovo University
5000 Veliko Tarnovo, Bulgaria
e-mail: svetla_yenci@hotmail.com

Abstract

Recent years have seen numerous examples when designs play an important role in the study of such topics in cryptography as secrecy and authentication codes, secret sharing schemes, correlation-immune and resilient functions. In this paper we give applications of some methods and results from the design theory, especially bounding the optimal size of the designs and codes, to cryptography. We give a new bound for the parameter t , when (n, T, t) -resilient function and correlation-immune function of order t exist. In the last section we present analogous bound for the parameter N of T -wise independent t -resilient function.

1 Introduction

Let \mathcal{M} be a metric space with distance $d(x, y)$ and a normalized measure μ , $\mu(\mathcal{M}) = 1$. Any finite subset (*code* or *design*) C , $C \subset \mathcal{M}$ is characterized by its *minimal distance* $d(C) = \min_{x, y \in C, x \neq y} d(x, y)$. For any $C \subset \mathcal{M}$, let $\Delta(C)$ denote the set of values of $d(x, y)$ when $x, y \in C$ i.e. the distance distribution of C . For any code C the parameter $s(C) = |\Delta(C) \setminus \{0\}|$ characterizes the number of distinct distances between distinct points of C . The diameter of the whole space \mathcal{M} can be defined as $D(\mathcal{M}) = \max(\Delta(\mathcal{M}) \setminus \{0\})$. We will define a τ -design by means of the strictly decreasing real function (substitution) $\sigma(d)$ considered on the interval $[0, D(\mathcal{M})]$.

Definition 1.1 *A set C will be referred to as a τ -design in \mathcal{M} with respect to the substitution $\sigma(d)$ if for any polynomial $f(t)$ in a real t of degree at most τ ,*

$$\int_{\mathcal{M}} \int_{\mathcal{M}} f(\sigma(d(x, y))) d\mu(x) d\mu(y) = \frac{1}{|C|^2} \sum_{x, y \in C} f(\sigma(d(x, y))). \quad (1)$$

*Supported by a junior research fellowship of the Katholieke Universiteit Leuven, Belgium.

The maximum integer τ ($\tau \leq s(\mathcal{M})$) such that a set C is a τ -design is called the strength of C and denoted by $\tau(C)$. Suppose \mathcal{M} is finite and $\Delta(C) = \{d_0, d_1, \dots, d_n\}$, is the *distance distribution* of C . The *dual distance distribution* (so called MacWilliams transform [15, p.137]) of C is defined to be $\Delta'(C) = \{d'_0, d'_1, \dots, d'_n\}$. The *dual distance* of the code C is the smallest i , $i = 1, \dots, n$, such that $d'_i \neq 0$; the *external distance* $s'(C)$ of C is the number of i , $i = 1, \dots, n$, such that $d'_i \neq 0$. It is proved in [3] that $\tau(C) + 1 = d'(C)$.

In this paper we are interested in applications of some methods and results of design theory, especially bounding the optimal size of the designs and codes, to cryptography. A function $f(x_1, \dots, x_n)$, where $x_i \in Z_v = \{0, 1, \dots, v-1\}$ $v \geq 2$ and $f(x_1, \dots, x_n) \in Z_w$ ($w \geq 2$) can be considered as a random variable provided that the input variables x_i , $i = 1, \dots, n$, are independent and uniformly distributed random variables. Then f is characterized by probabilities $p(b)$ to take a value $b \in Z_w$. The function f is called correlation-immune of order t ($t = 0, 1, \dots, n$) if any function in $n-t$ variables, obtained from f by a substitution of any constants from Z_v for any t input variables, has the same probability $p(b)$, $b \in Z_w$. If $w = v^T$ ($T = 1, 2, \dots$) and all probabilities $p(b)$, $b \in Z_w$, are equal, then any f can be considered as a system of T functions $f_1(x_1, \dots, x_n), \dots, f_T(x_1, \dots, x_n)$ of the form $Z_v^n \rightarrow Z_v$, which are independent and uniformly distributed random variables (we call such systems of T functions in n variables *balanced*). If f is correlation-immune function of order t , then the system of T function preserves the property to be balanced system under a substitution of any constants of Z_v for any t input variables. Such balanced system of T functions is called (n, T, t) -*resilient*, (or simply resilient of order t).

Another interesting application is the designs in product association schemes. Let (Y, \mathcal{A}) ¹ be an association scheme with primitive idempotents E_0, E_1, \dots, E_d . For $\mathcal{T} \subseteq \{1, \dots, d\}$ a Delsarte \mathcal{T} -design in (Y, \mathcal{A}) is a subset D of Y whose characteristic vector is annihilated by the idempotents E_j ($j \in \mathcal{T}$). The most studied case is that in which (Y, \mathcal{A}) is Q -polynomial and $\mathcal{T} = \{1, \dots, t\}$. For $1 \leq i \leq m$, let (Y_i, \mathcal{A}_i) be Q -polynomial association schemes. Assume that Delsarte t -designs in each (Y_i, \mathcal{A}_i) are characterized as poset t -designs in a Q -poset \mathcal{P}_i attached to that scheme. With these assumption, we consider the product association scheme $(\times Y_i, \mathcal{A})$ and the corresponding linear programming bound and the Delsarte bound on size of degree of such a \mathcal{T} -design analogous to Delsarte's bound for t -designs in Q -polynomial association schemes.

The paper is organized as follows. In the first part we present some preliminary results about τ -designs in Hamming and Johnson space. We give briefly our previous investigations, which give necessary and sufficient conditions for improving the Delsarte bound for designs. We present also the analytical form of the extremal polynomials and the analytical form of the new bound for non-antipodal spaces. The results in this section are valid for all PMS, in particular for Hamming and Johnson space. The proofs of the theorems can be found in [10, 11, 12]. In Section 3 we are interested in correlation-immune and resilient

¹Here and in Section 4 we will follow the notations used in [9]

functions and the connection with the designs theory. As a direct application we give a new bound for the parameter t , when (n, T, t) -resilient function and correlation-immune function of order t exist. In the last section we present analogous bound for the parameter N of T -wise independent t -resilient function.

2 Improvement of the Delsarte bound for orthogonal arrays and combinatorial designs

The basic problem of the coding theory is the construction of the maximum (on cardinality) σ -code. Together with this problem there exists another one of constructing the minimum (on cardinality) τ -design (or equivalently a code with dual distance $d' = \tau + 1$). As it is proved in [5, 2] this two problems are dual.

Following the notations in [7] we will consider **polynomial metric space** (PMS) with a given substitution $\sigma(d)$ and a system of orthogonal (with respect to the measure $\nu(z)$) polynomials $Q_i(z)$ of degree i , $i = 0, 1, \dots, s(\mathcal{M})$, the so called *zonal spherical functions* (ZSF). A polynomial metric space \mathcal{M} is called **antipodal** if for every point $x \in \mathcal{M}$ there exists a point $\bar{x} \in \mathcal{M}$ such that for any point $y \in \mathcal{M}$ we have $\sigma(d(x, y)) + \sigma(d(\bar{x}, y)) = 0$. A code for which $\sigma(d(x, y)) \leq \sigma(d)$, where d is the minimum distance of C we call an $(M, |C|, \sigma)$ -code. When \mathcal{M} is finite the measure $\nu(z)$ is left continuous function and has $s + 1$ steps at the point $z_i = \sigma(d_i)$ with positive step sizes w_i , $i = 0, 1, \dots, s(\mathcal{M})$, $\sum_{i=0}^s w_i = 1$.

For arbitrary $a, b \in \{0, 1\}$ can be defined the so called **adjacent** system of orthogonal polynomials $Q_k^{a,b}(z)$ (with respect to the measure $(1-z)^a(1+z)^b\nu(z)$) in a real z of degree k , $k = 0, 1, \dots, s(\mathcal{M}) - \delta_{a,1} - \delta_{b,1}$, positive constant $c^{a,b}$ and $r_k^{a,b}$ [7]. The ZSF satisfy the recurrence formula $(z + m_i + c_i - 1)Q_i(z) = m_i Q_{i+1}(z) + c_i Q_{i-1}(z)$, for $i \geq 0$, where $r_{-1} = m_{-1} = 0$, $m_i = \frac{a_{i,i}}{a_{i+1,i+1}}$, $c_i = \frac{r_{i-1}m_{i-1}}{r_i}$ and $Q_{-1}(z) \equiv 0$, $Q_0(z) \equiv 1$. Denote by $z_k^{a,b}$ the greatest zero of the polynomial $Q_k^{a,b}(z)$. We will introduce the notations $Q_k^{a,b}(z) = \sum_{i=0}^k a_{k,i}^{a,b} z^i$, $n_i^{a,b} = \frac{a_{i,i-1}^{a,b}}{a_{i,i}^{a,b}}$, $\tilde{n}_i^{a,b} = \frac{a_{i,i-2}^{a,b}}{a_{i,i}^{a,b}}$, $u_i^{a,b} = \frac{a_{i,i}^{a,b}}{a_{i,i}^{a,b}}$.

The linear programming bounds for codes and designs was obtained by using the following theorem [15].

Theorem 2.1 *Let $C \subset \mathcal{M}$ be an $(\mathcal{M}, |C|, \sigma)$ -code (reps. τ -design) and let $f(z)$ be a real non-zero polynomial such that*

(A1) $f(z) \leq 0$, for $-1 \leq z \leq \sigma$, (resp. (B1) $f(z) \geq 0$, for $-1 \leq z \leq 1$),

(A2) the coefficients in the ZSF expansion $f(z) = \sum_{i=0}^k f_i Q_i(z)$ satisfy $f_0 > 0$, $f_i \geq 0$ for $i = 1, \dots, k$. (resp. (B2) the coefficients in the ZSF expansion $f(z) = \sum_{i=0}^k f_i Q_i(z)$ satisfy $f_0 > 0$, $f_i \leq 0$ for $i = \tau + 1, \dots, k$.)

Then, $|C| \leq f(1)/f_0 = \Omega(f)$ (resp. $|C| \geq f(1)/f_0$).

We denote by $B_{\mathcal{M},\tau}$ the set of real polynomials which satisfy the conditions **(B1)** and **(B2)** and $B(\mathcal{M},\tau) = \max\{\Omega(f) : f(t) \in B_{\mathcal{M},\tau}\}$. A polynomial $f(z) \in B_{\mathcal{M},\tau}$ is called $B_{\mathcal{M},\tau}$ -extremal if $\Omega(f) = \max\{\Omega(g) : g(z) \in B_{\mathcal{M},\tau}, \deg(g) \leq \deg(f)\}$.

Many authors obtained various pairs of bounds [15] for the cardinality of codes and designs in finite PMS which follow from Theorem 2.1. For our investigations the most important ones will be the Levenshtein bound $L_{2k-1+\varepsilon}(\mathcal{M},\sigma)$ for codes and the Delsarte bound $D(\mathcal{M},\tau)$ for τ -designs which can be presented as follows [7, 3]: $|C| \leq L_{2k-1+\varepsilon}(\mathcal{M},\sigma) = (1 - \frac{Q_k^{1,0}}{Q_k^{0,\varepsilon}(\sigma)}) \sum_{i=0}^{k-1+\varepsilon} r_i$, where $\varepsilon = 0$ if $z_{k-1}^{1,1} \leq \sigma < z_k^{1,0}$ and $\varepsilon = 1$ if $z_k^{1,0} \leq \sigma < z_k^{1,1}$, resp. $|C| \geq D(\mathcal{M},\tau) = 2^\theta c^{0,\theta} \sum_{i=0}^k r_i^{0,\theta}$, where $\theta \in \{0,1\}$ and $\tau = 2k + \theta$. This two bounds can be obtained by the polynomials $f^{(\sigma)}(z) = (z - \sigma)(z + 1)^\varepsilon (\sum_{i=0}^{k-1} r_i^{1,\varepsilon} Q_i^{1,\varepsilon}(z) Q_i^{1,\varepsilon}(\sigma))^2$, and $f^{(\tau)}(z) = (z + 1)^\theta ((Q_k^{1,\theta}(z))^2)$, respectively, in the Theorem 2.1.

PMS are finite metric spaces represented by P- and Q- polynomial association schemes as well as infinite metric spaces. The most famous examples of the finite spaces are the Hamming, Johnson, Grassmann space. We will consider only Hamming and Johnson spaces, presented by Q-polynomial association schemes. In these spaces τ -designs are known as orthogonal arrays and combinatorial designs, respectively. Analogously the Delsarte bound is in fact the Rao bound for orthogonal arrays and the Ray-Chaudhuri/Wilson bound for the combinatorial t-designs.

We consider the following linear functional $G_\tau(\mathcal{M}, f) = \frac{f(1)}{D(\mathcal{M},\tau)} + \sum_{i=1}^{k+\theta} \rho_i^{(\tau)} f(\alpha_i)$, where α_i are the zeros of $Q_k^{1,\theta}(t)$, and $\rho_i^{(\tau)}$ are positive constants. This linear functional maps the set of real polynomials to the set of real numbers. Now we will give necessary and sufficient conditions for improvement of the Delsarte bound.

Theorem 2.2 [10, 11] *The bound $D(\mathcal{M},\tau)$ can be improved by a polynomial $f(z) \in B_{\mathcal{M},\tau}$ of degree at least $\tau + 1$, if and only if $G_\tau(\mathcal{M}, Q_j) < 0$ for some $j \geq \tau + 1$. Moreover, if $G_\tau(\mathcal{M}, Q_j) < 0$ for some $j \geq \tau + 1$, then $D(\mathcal{M},\tau)$ can be improved by a polynomial in $B_{\mathcal{M},\tau}$ of degree j .*

Theorem 2.3 [11] *Let \mathcal{M} be non-antipodal PMS. Then, any $B_{\mathcal{M},\tau}$ -extremal polynomial of degree $\tau + 2$ ($\tau = 2k + \theta$) has the form*

$$f^{(\tau)}(z; \tau + 2) = (1 + z)^{1-\theta} [q(z + 1) + (1 - z)][\eta Q_{k-1+\theta}^{1,1-\theta}(z) + Q_{k+\theta}^{1,1-\theta}(z)]^2$$

where q and η are suitable constants.

Let us introduce the following notations: for $\tau = 2k$

$$B_1 = \frac{u_k^{1,1}(n_{\tau+2} - 2n_k^{1,1})}{2u_{k-1}^{1,1}m_{k-1}c^{1,1}r_{k-1}^{1,1}}, \quad B_2 = \frac{1}{(c^{1,1})^2 r_{k-1}^{1,1} r_k^{1,1}}, \quad S_1 = \frac{4}{r_{k+1}} + \frac{4}{r_k}$$

$$S_2 = \frac{4(2n_{k+1} - n_{\tau+2})}{u_k^{1,1}u_{k-1}^{1,1}m_{k-1}m_k^2} - \frac{8}{u_k^{1,1}u_{k-1}^{1,1}m_{k-1}m_k}, \quad S_3 = \frac{4}{r_{k+1}r_k}$$

$$S_4 = \frac{4(2n_{k+1} - n_{\tau+2})}{u_k^{1,1} u_{k-1}^{1,1} (m_k)^2 m_{k-1} r_k}, \quad S_5 = \frac{-4}{(u_k^{1,1} u_{k-1}^{1,1} m_k m_{k-1})^2}$$

and for $\tau = 2k + 1$

$$B_1 = \frac{u_{k+1}^{1,0} (1 + n_{\tau+2} - 2n_{k+1}^{1,0})}{4u_k^{1,0} m_k c^{1,0} r_k^{1,0}}, \quad B_2 = \frac{1}{(2c^{1,0})^2 r_k^{1,0} r_{k+1}^{1,0}}, \quad S_5 = \frac{-4(u_{k+1}^{0,1} u_k^{0,1})^2}{(u_{k+1}^{1,0} u_k^{1,0})^2}$$

$$S_1 = \frac{2}{c^{0,1} r_{k+1}^{0,1}} + \frac{2}{c^{0,1} r_k^{0,1}} \quad S_2 = \frac{4(u_{k+1}^{0,1})^2 (1 + 2n_{k+1}^{0,1} - n_{\tau+2})}{u_{k+1}^{1,0} u_k^{1,0} m_k} - \frac{8u_{k+1}^{0,1} u_k^{0,1}}{u_{k+1}^{1,0} u_k^{1,0}},$$

$$S_3 = \frac{1}{(c^{0,1})^2 r_{k+1}^{0,1} r_k^{0,1}} \quad S_4 = \frac{2(u_{k+1}^{0,1})^2 (1 + 2n_{k+1}^{0,1} - n_{\tau+2})}{c^{0,1} u_{k+1}^{1,0} u_k^{1,0} m_k r_k^{0,1}}.$$

Now taking into account that $S(\mathcal{M}, \tau) = \Omega(f^{(\tau)}(z; \tau+2))$ and using the notations above we obtain the following analytical form of the bound $S(\mathcal{M}, \tau)$.

Lemma 2.4 [11] *Let \mathcal{M} be a non-antipodal PMS. Then the bound $S(\mathcal{M}, \tau)$ is equal to*

$$\frac{S_1 + (B_1 + \sqrt{B_1^2 + B_2})S_2}{S_3 + (B_1 + \sqrt{B_1^2 + B_2})S_4 + (B_1 + \sqrt{B_1^2 + B_2})^2 S_5} + D(\mathcal{M}, \tau - 2)$$

Corollary 2.5 [11] *Let \mathcal{M} be a non-antipodal PMS and let τ be an integer. Then*

- a) $B(\mathcal{M}, \tau) \geq S(\mathcal{M}, \tau) = \Omega(f^{(\tau)}(z; \tau + 2))$.
- b) $S(\mathcal{M}, \tau) > D(\mathcal{M}, \tau)$ if and only if $G_\tau(\mathcal{M}, Q_{\tau+2}) < 0$.

Theorem 2.6 [11] *Let \mathcal{M} be antipodal PMS. Then, any $B_{\mathcal{M}, \tau}$ -extremal polynomial of degree $\tau + 3$ ($\tau = 2k + \theta$) has the form*

$$f^{(\tau)}(z; \tau + 3) = (1 + z)^\theta [q(z + 1) + (1 - z)][\eta_1 Q_{k-1}^{1,\theta}(z) + \eta_2 Q_k^{1,\theta}(z) + Q_{k+1}^{1,\theta}(z)]^2$$

where q , η_1 and η_2 are suitable constants.

Corollary 2.7 [11] *Let \mathcal{M} be an antipodal PMS and let τ be an integer. Then*

$$B(\mathcal{M}, \tau) \geq S(\mathcal{M}, \tau) = \Omega(f^{(\tau)}(z; \tau + 3)).$$

Let us consider the Hamming space $\mathcal{M} = H_v^n$ ($n, v = 2, 3, \dots$). The orthogonal arrays are commonly denoted by $OA_\lambda(\tau, n, v)$ and their cardinality satisfy $|C| = \lambda v^\tau$. The ZSF for the Hamming space are the Krawtchouk polynomials $K_k^{n,v}(z)$. A stronger version of the Theorem 2.1 is the following:

Theorem 2.8 [5] Let $C \subset \mathcal{M}$ be an d -code (resp. τ -design) and let $f(z) = \sum_{i=0}^n f_i K_i^{n,v}(z)$ be a real non-zero polynomial such that

(C1) $f(0) > 0, f(i) \leq 0$, for $i = d, \dots, n$,
 (resp. (D1) $f(0) > 0, f(i) \geq 0$, for $i = 1, 2, \dots, n$),

(C2) $f_0 > 0, f_i \geq 0$ for $i = 1, \dots, n$.
 (resp. (D2) $f_0 > 0, f_i \leq 0$ for $i = d + 1, \dots, n$.)

Then, $|C| \leq \min \Omega(f)$ (resp. $|C| \geq \max \Omega(f)$), where $\Omega(f) = f(0)/f_0$.

Let us denote by $A_v^*(n, d) = \min\{\Omega(f)\}$ for polynomials f satisfying the conditions (C1), (C2); $B_v^*(n, d) = \max\{\Omega(f)\}$ for polynomials f satisfying the conditions (D1), (D2); and $B_v^{**}(n, d) = \max\{\Omega(f)\}$: for polynomials f satisfying the conditions (D1), (D2) and $\deg f \leq d$.

Theorem 2.9 [2, 5] For any integers n, d, v ($1 \leq d \leq n + 1, v \geq 2$),

$$A_v^*(n, d)B_v^*(n, d - 1) = v^n \quad (2)$$

Here we will present well known pairs of universal bounds, i.e. inequalities which are valid for all codes $C \subseteq H_v^n$. The first pair is the **Singleton bound** [15] for a code $C \subseteq H_v^n$

$$v^\tau \leq |C| \leq v^{n-d+1},$$

where any of the bounds is attained if and only if $d + d' = n + 2$, ($d' - 1 = \tau$). The second pair of bounds is formed by **Rao** and **Hamming** [15] bounds for a code $C \subseteq H_v^n$.

$$D(H_v^n, \tau) \leq |C| \leq \frac{v^n}{D(H_v^n, d - 1)} \quad (3)$$

Codes, which cardinality is equal to the left-hand side or the right-hand side of (3) are called *tight* designs and *perfect* codes, respectively.

The third pair universal bounds for any code $C \subseteq H_v^n$ is the **Levenshtein** bound [5].

$$\frac{v^n}{L(H_v^n, \sigma(\tau + 1))} \leq |C| \leq L(H_v^n, \sigma(d))$$

First two pairs of bounds are obtained by means of combinatorial methods, but all of them can be obtained using Theorem 2.1 or Theorem 2.8. Applying Theorem 2.9 for our bound we have

Theorem 2.10 [12] For any code $C \subseteq H_v^n$

$$S(H_v^n, \tau) \leq |C| \leq \frac{v^n}{S(H_v^n, d - 1)} \quad (4)$$

In the Johnson space $X = J_w^n$ ($n = 2, 3, \dots$; $w = 1, \dots, \lfloor n/2 \rfloor$) designs are the classical $t - (v, k, \lambda)$ and codes are called constant weight codes. The ZSF are the Hahn polynomials $J_k^{n,w}(z)$. For J_w^n an analog of the Theorem 2.8 is also valid and there are known several pairs of bounds.

Theorem 2.11 [12] *For any design $C \subseteq J_w^n$*

$$S(J_w^n, \tau) \leq |C| \quad (5)$$

3 Resilient and Correlation-immune functions

In [14] Stinson gave the connection between correlation-immune function, resilient function and orthogonal arrays.

Theorem 3.1 [1] *A function $f : Z_v^n \rightarrow Z_w$ is correlation-immune of order t if and only if Z_v^n is partitioned into w orthogonal arrays $OA_\lambda(t, n, v)$.*

Theorem 3.2 [1] *A function $f : Z_v^n \rightarrow Z_v^T$ is resilient of order t if and only if Z_v^n is partitioned into v^T orthogonal arrays $OA_{v^{n-T-t}}(t, n, v)$.*

Note that in the first theorem λ need not be identical. A large set of orthogonal arrays $LOA_\lambda(t, n, v)$ is a set of v^{n-t}/λ simple arrays $OA_\lambda(t, n, v)$ such that all have the same λ value.

Corollary 3.3 [1] *There exists a function $f : Z_v^n \rightarrow Z_v^T$ that is resilient of order t if and only if there exists an $LOA_{v^{n-T-t}}(t, n, v)$.*

A necessary condition for the existence of a correlation-immune function of order t and for existence of a (n, T, t) -resilient function are as follows:

$$w \leq \frac{v^n}{B_v^*(n, t)} = A_v^*(n, t + 1), \quad \log_v(B_v^*(n, t)) \leq n - T. \quad (6)$$

One is concerned with developing upper bounds for the optimum value of t for a given n and T . It is easy to see that $n \geq T + t$ and so the trivial upper bound is $t \leq n - T$. If we substitute the Delsarte bound instead of $B_v^*(n, t)$ we obtain another upper bound for t [1]. The upper bounds based on the Delsarte (Rao) bound for orthogonal arrays are stronger than the ones obtained using the trivial bound. We can improve this bound using our previous result in Theorem 2.10.

Theorem 3.4 *Suppose there exists an correlation-immune function of order t . Then $w \leq \frac{v^n}{S(H_v^n, t)}$.*

Theorem 3.5 *Suppose there exists a (n, T, t) -resilient function. Then*

$$\log_v(S(H_v^n, t)) \leq n - T$$

However, we can often do better by using Delsarte's linear programming bound. Let $W(n, t)$ be the optimal solution to the linear programming problem Theorem 2.8. In view of the equation (6), this implies that $\log_v(W(n, t) + 1) \leq n - T$. For large values of t , the orthogonal array bounds obtained by the linear programming technique are usually much better than the Delsarte (Rao) bound and our new bound $S(H_v^n, t)$. The disadvantage of this method is that one needs to solve a different linear program for every parameter situation. Thus it is of interest to derive explicit bounds as corollaries of the linear programming bound. In the cases $v = 2, t + 1 < n < 2t + 2$ and $v = 2, t + 1 < n < 2t + 3$ the most important bounds are as follows :

Theorem 3.6 [1, 4] *Suppose there exists a (n, T, t) -resilient function and $v = 2$. Then*

$$t \leq \lfloor \frac{2^{T-1}n}{2^{T-1}} \rfloor - 1, \quad t \leq 2 \lfloor \frac{2^{T-2}(n+1)}{2^{T-1}} \rfloor - 1.$$

4 Designs in product association schemes. Maximum independent resilient system of functions.

Let (\mathcal{P}, \preceq) be a partially ordered set (*poset*). If there exist constants $\lambda_0, \dots, \lambda_t$ such that, for $0 \leq i \leq t$ and $\forall x \in \mathcal{P}^i, |\{y \in D : x \preceq y\}| = \lambda_i$ then the set $D \subseteq \mathcal{P}^d$ is called a *poset t -design* in (\mathcal{P}, \preceq) . For $1 \leq i \leq m$, let (Y_i, \mathcal{A}_i) be a d_i -class association scheme with adjacency matrices \mathcal{A}_i . The *direct product* of these schemes is the association scheme $(X, \mathcal{A}) = (Y_1, \mathcal{A}_1) \otimes \dots \otimes (Y_m, \mathcal{A}_m)$ defined by $X = Y_1 \times \dots \times Y_m$ and $\mathcal{A} = \{\otimes_{i=1}^m \mathcal{M}_i : \mathcal{M}_i \in \mathcal{A}_i, 1 \leq i \leq m\}$ where $\otimes_{i=1}^m \mathcal{M}_i$ is the m -fold Kronecker product of matrices. Assume that each component scheme (Y_i, \mathcal{A}_i) has an attached Q -poset $(\mathcal{P}_i, \preceq_i)$. Consider the Delsarte \mathcal{T}^* -design ($\mathcal{T}^* = \mathcal{T} - \{0\}$) in $(\times Y_i, \mathcal{A})$ as poset designs in the product poset $\times \mathcal{P}_i$ where \mathcal{T} is any downset in the product chains \mathcal{C} . Let (X, \mathcal{A}) be the product of Q -polynomial association schemes $(Y_i, \mathcal{A}_i), (1 \leq i \leq m)$. Each matrix $M \in \mathcal{A}$ may be expanded in the form $M = v \sum_{\underline{j} \in \mathcal{C}} \beta_{\underline{j}} E_{\underline{j}}$. If we change the bases, we have $M = \sum_{\underline{i} \in \mathcal{C}} \alpha_{\underline{i}} A_{\underline{i}}$, where $\alpha_{\underline{i}} = \sum_{\underline{j} \in \mathcal{C}} Q_{\underline{i}\underline{j}} \beta_{\underline{j}}, (\underline{i} \in \mathcal{C})$. For $\underline{j} \in \mathcal{C}$, let $f_{\underline{j}} = \text{rank} E_{\underline{j}}$.

Theorem 4.1 [9] *Let (X, \mathcal{A}) be the product of Q -polynomial association schemes $(Y_i, \mathcal{A}_i), (1 \leq i \leq m)$. Let \mathcal{T} be a downset in \mathcal{C} and let $D \subseteq X$ be a Delsarte \mathcal{T}^* -design. Consider the matrices M satisfying the conditions*

- (i) M is non-negative matrix;
- (ii) $\beta_{\underline{j}} \leq 0$ for $\underline{j} \notin \mathcal{T}$;
- (iii) $\beta_{\underline{0}} = 1$.

Then, the lower bound on the size of a \mathcal{T} -design is $|D| \geq \alpha_{\underline{0}}$.

Theorem 4.2 (Delsarte bound)[9] *Let (X, \mathcal{A}) be the product of Q -polynomial association schemes (Y_i, \mathcal{A}_i) , $(1 \leq i \leq m)$. Let \mathcal{T} be a downset in \mathcal{C} and let $D \subseteq X$ be a Delsarte \mathcal{T}^* -design. If $\mathcal{E} \subseteq \mathcal{C}$ satisfies $(\mathcal{E} + \mathcal{E}) \cap \mathcal{C} \subseteq \mathcal{T}$, then $|D| \geq \sum_{j \in \mathcal{E}} f_j$.*

Here are some examples from [9].

- *Mixed-level orthogonal arrays* $OA(M, q_1^{n_1} \cdots q_m^{n_m}, t)$ of strength t are studied by Sloane and Stufken in [13]. This object is equivalent to the Delsarte \mathcal{T}^* -design in the scheme $H(n_1, q_1) \otimes \cdots \otimes H(n_m, q_m)$, where $\mathcal{T} = \{j : \sum j_i \leq t\}$.
- *Mixed t -designs* [8] is the product of Johnson schemes $J(v_1, k_1) \otimes J(v_2, k_2)$, which is the Delsarte \mathcal{T}^* -design for $\mathcal{T} = \{(i_1, i_2) : i_1 + i_2 \leq t\}$.
- *Fused orthogonal array design* of strength t can be considered as a product scheme of the form $H(n, q) \otimes J(v, k)$.
- *Split orthogonal arrays* $SOA_\lambda(t, n; T, N; v)$ are introduced by Levenshtein [6]. The cardinality of $SOA_\lambda(t, n; T, N; v)$ is λv^{t+T} . Given q, n, N, t, T we wish to find an $M \times (n + N)$ array with entries in $Z_q = \{0, \dots, q - 1\}$ such that, upon choosing any t columns from among the first n columns and any T columns from among the last N columns, all $(t + T)$ -tuples over the alphabet Z_q occur equally often. This is equivalent to a \mathcal{T} -design in the product scheme $H(n_1, q) \otimes H(n_2, q)$ where $\mathcal{T} = \{(i_1, i_2) : 0 \leq i_1 \leq t_1, 0 \leq i_2 \leq t_2\}$. For such objects, the Delsarte linear programming bound is equivalent to the following: let $f(z) = 1 + \sum_{i=1}^n f_i K_i^{n,v}(z)$ and $g(z) = 1 + \sum_{j=1}^N g_j K_j^{N,v}(z)$ be polynomials satisfying the condition **(D1)** and $f_i g_j \leq 0$ for $i \geq t + 1$ or $j \geq T + 1$ then $|D| \geq f(0)g(0)$.

Theorem 4.3 [6] *If D is split orthogonal array then*

$$|D| \geq \max(B_v^*(n, t)B_v^{**}(N, T), B_v^{**}(n, t)B_v^*(N, T))$$

Hence we have the following bound $|D| \geq D(H_v^n, t)D(H_v^N, T)$. Using again Theorem 2.10 we obtain the next statement.

Theorem 4.4 *If D is split orthogonal array then*

$$|D| \geq \max(S(H_v^n, t)D(H_v^N, T), D(H_v^n, t)S(H_v^N, T))$$

A system of N functions in n variables over Z_v is called *T -wise independent t -resilient* if any subset of T functions of the system forms a t -resilient system. Our goal is to find the maximum number N , such that there exists a T -wise independent t -resilient system. The connection between this cryptographic objects and the orthogonal arrays was studied by Levenshtein in [6].

Theorem 4.5 [6] *The existence of T -wise independent t -resilient system is equivalent to that of split orthogonal array $SOA_\lambda(t, n; T, N; v)$ with $(\lambda = v^{n-t-T})$.*

Corollary 4.6 *We derive the inequality*

$$v^n \geq \max(S(H_v^n, t)D(H_v^N, T), D(H_v^n, t)S(H_v^N, T)).$$

Summarizing the results our bounds (Theorems 3.4, 3.5, 4.4 and Corollary 4.6) give a necessary condition for the existence of the above considered cryptographic objects.

References

- [1] J.Bierbrauer, K.Gopalakrishnan, D.R.Stinson, Orthogonal arrays, resilient functions, error correcting codes and linear programming bounds, *SIAM J.Discrete Math.* 9, 1996, 424-452.
- [2] J.Bierbrauer, K.Gopalakrishnan, D.R.Stinson, A note on the duality of linear programming bounds for orthogonal arrays and codes, *Bulletin of the ICA* 22, 1998, 17-24.
- [3] P.Delsarte, An Algebraic Approach to Association Schemes in Coding Theory, *Philips Research Reports Suppl.*, 10, 1973.
- [4] J.Friedman, On the bit extraction problem. *Proc. 33rd IEEE Symp. on Foundations of Computer Science*, 1992, 314-319.
- [5] V.I.Levenshtein, Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Trans. Inf. Theory* 41, 5, 1995, 1303-1321.
- [6] V.I.Levenshtein, Split orthogonal arrays and maximum independent resilient systems of functions, *Designs, Codes and Cryptography* 12, 1997, 131-160.
- [7] V.I.Levenshtein, Universal bounds for codes and designs, Chapter 6 in *Handbook of Coding Theory*, V.Pless and W.C.Huffman, 1998 Elsevier Science B.V., 449-648.
- [8] W.J. Martin, Mixed block designs, *J. Combin. Designs* 6, 2, 1998, 151-163.
- [9] W.J. Martin, Designs in product association schemes *Designs, Codes and Cryptography* 16, 3, 1999, 271-289.
- [10] S.I. Nikova, Bounds for designs in infinite polynomial metric spaces, Ph.D. Thesis, Eindhoven University of Technology, 1998.
- [11] S.I.Nikova, V.S.Nikov, Improvement of the Delsarte bound for τ -designs when it is not the best bound possible, submitted in *Designs Codes and Cryptography*.
- [12] S.I.Nikova, V.S.Nikov, Improvement of the Delsarte bound for τ -designs in finite polynomial metric space, to be published.
- [13] N.J.A. Sloane, J.Stufken, A linear programming bound for orthogonal arrays with mixed levels, *J. Stat. Plan. Inf* 56, 1996, 295-306.
- [14] D.R.Stinson, Resilient functions and large sets of orthogonal arrays, *Congressus Numer.* 92, 1993, 105-110.
- [15] F.J.MacWilliams, N.J.A.Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.