Split Orthogonal Arrays and Maximum Independent Resilient Systems of Functions

VLADIMIR I. LEVENSHTEIN*
Institute for Applied Mathematics, RAS,
Miusskaya Sq.4, 125047, Moscow

Abstract

A system of (Boolean) functions in n variables is called randomized if the functions preserve the property of their variables to be independent and uniformly distributed random variables. Such a system is referred to as t-resilient if for any substitution of constants for any i variables, where $0 \le i \le t$, the derived system of functions in $n-i$ variables will be also randomized. We investigate the problem of finding the maximum number $N(n,t,T)$ of functions in n variables of which any T form a t-resilient system. This problem is reduced to the minimization of the size of certain combinatorial designs, which we call split orthogonal arrays. We extend some results of design and coding theory, in particular, a duality in bounding the optimal sizes of codes and designs, in order to obtain upper and lower bounds on $N(n,t,T)$. In some cases, these bounds turn out to be very tight. In particular, for some infinite subsequences of integers n they allow us to prove that $N(n,3,3)=\frac{2^{n-2}}{n}$, $N(n,3,5)=\sqrt{\frac{2^{n-1}}{n}}$, $N(n,3,\frac{n}{2}-1)=n$, $N(n,\frac{n}{2}-1,3)=n$, $N(n,\frac{n}{2}-1,5)=\sqrt{2n}$. We also find a connection of the problem considered with the construction of unequal-error-protection codes and superimposed codes for multiple access in the Hamming channel.

Contents

*The results of this paper were presented in part at the 1995 IEEE International Symposium on Information Theory, Whisler, Canada, September 17-22, 1995. The research was partially supported by the Russian Foundation for the Basic Research (grant 95-01-01103) and by the International Science Foundation (grant MEF300).

1. Introduction

The paper is devoted to applications of some ideas, methods, and results of design and coding theory, especially a duality in bounding the optimal sizes of designs and codes, to solve a number of problems connected with correlation-immune and resilient functions. These functions were intensively investigated in recent years in connection with applications in cryptology and complexity theory [1], [2], [6], [7], [8], [14], [16], [26], [35].

A function $f(x_1,\dots,x_n)$, where $x_i \in F_v = \{0,1,\dots,v-1\}$ $(v \geq 2)$ and $f(x_1,\dots,x_n) \in F_w$ $(w \geq 2)$, 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 $p_f(b)$ to take a value $b \in F_w$. The function f is called *correlation-immune of order* t $(t = 0,1,...,n)$ if any function in $n-t$ variables, obtained from f by a substitution of any constants from F_v for any t input variables, has the same probabilities $p_f(b)$, $b \in F_w$. If $w = v^T$ $(T = 1,2,\dots)$ and all probabilities $p_f(b)$, $b \in F_w$, 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 $F_v^n \to F_v$, which are independent and uniformly distributed random variables (we call such systems of T functions in n variables *randomized*). Moreover, if the f is a correlation-immune function of order t, then the system of T functions preserves the property of being randomized under a substitution of any constants of F_v for any t input variables (we call such randomized system of T functions *t-resilient*). This explains a cryptological motivation of a t-resilient system, namely, that an opponent cannot disturb the independence and uniform distribution of the output random variables even if he can substitute at most t input variables for constants. We denote by $T_v(n,t)$ the maximum number of functions in a t-resilient system.

A possibility of nontrivial applications of coding and design theory to correlation-immune and resilient functions based on a result by Stinson [37]. In his work, he proved that the existence of a correlation-immune function $f : F_v^n \to F_w$ of order t (in particular for $w = v^T$, of a t-resilient system of T functions over F_v) is equivalent to the existence of a partition of F_v^n into w orthogonal arrays $OA_{\lambda_i}(t,n;v)$, $i = 0,\dots,w-1$, with $\lambda_i = p_f(i)v^{n-t}$ (an $OA_\lambda(t,n;v)$ is a matrix C with rows from F_v^n such that in any t columns of C every vector of F_v^t occurs exactly λ times). This gives the following necessary condition for the existence of a correlation-immune function $f : F_v^n \to F_w$ of order t and, in particular for

$w = v^T$, of t-resilient system of T functions over F_v :

$$w \leq \frac{v^n}{B_v(n, t+1)}, \tag{1.1}$$

where $B_v(n, t+1)$ is the minimum size of $OA_\lambda(t, n; v)$ over all λ ($\lambda = 1, 2, \ldots$), and allows us to use coding theory [25], [27], [29] and partitions F_v^n into designs (see [39]) to construct the desirable functions.

In this paper, we consider a new problem of finding the maximum number $N_v(n, t, T)$ of functions (of the form $F_v^n \to F_v$), of which any T form a t-resilient system. It is natural to call such systems *T-wise independent t-resilient.* In the case $t = 0$ we call such a system *T-wise independent* and put $N_v(n, T) = N_v(n, 0, T)$. In Section 2, we introduce a concept of a split orthogonal array $\mathrm{SOA}_\lambda(t, n; T, N; v)$. In Section 3, we prove that the condition

$$v^n \geq B_v(n, t+1; N, T+1) \tag{1.2}$$

where $B_v(n, t+1; N, T+1)$ is the minimum size of a $\mathrm{SOA}_\lambda(t, n; T, N; v)$ over all λ ($\lambda = 1, 2, \ldots$), is necessary for the existence of a T-wise independent t-resilient system of N functions of the form $F_v^n \to F_v$.

In order to obtain lower bounds on $B_v(n, t+1)$ and $B_v(n, t+1; N, T+1)$ (and upper bounds on $T_v(n, t)$ and $N_v(n, t, T)$), in preliminary Sections 4-5 we extend some results of Delsarte theory [11] from the case of orthogonal arrays (OAs) to the case of split orthogonal arrays (SOAs). As a rule, we give a short proof of a known result for OAs and remark that the corresponding result for SOAs may be proved by using twice the same argument. In Section 4 we also use a functional description of *binary* (i.e., $v = 2$) OAs to give a simple proof of the following useful identities:

$$T_2(n+1, 2h+1) = T_2(n, 2h),$$

$$N_2(n+1, 2h+1, T) = N_2(n, 2h, T),$$

$$N_2(n+1, 2m+1) = N_2(n, 2m) + 1.$$

In Section 6 we present a linear programming bound for SOAs. Let $A_v(n, d)$ be the maximum size of a set $C \in F_v^n$ with Hamming distance at least d between distinct vectors (i.e., of a d-code $C \in F_v^n$). Let

$$K_k^{n,v}(z) = \sum_{j=0}^{k} (-1)^j (v-1)^{k-j} \binom{z}{j} \binom{n-z}{k-j} \tag{1.3}$$

be the Krawtchouk polynomial [19] of degree k and suppose that for an arbitrary polynomial $f(z) = \sum_{i=0}^n f_i K_i^{n,v}(z)$, $\Omega(f) = f(0)/f_0$. Let us define the following three functions:

$$A_v^*(n,d) = \min \Omega(f),$$

where the minimum is taken over all polynomials $f(z)$ such that $f_0 > 0,\ f_i \geq 0$ if $i = 1, 2, \ldots, n$, and $f(0) > 0,\ f(i) \leq 0$ if $i = d, \ldots, n$;

$$B_v^*(n,d) = \max \Omega(f),$$

where the maximum is taken over all polynomials $f(z)$ such that $f_0 > 0,\ f_i \leq 0$ if $i = d, \ldots, n,\ f(0) > 0,\ f(i) \geq 0$ if $i = 1, 2, \ldots, n$, and

$$B_v^{**}(n,d) = \max \Omega(f),$$

where the maximum is taken over all polynomials $f(z)$ such that $f_0 > 0,\ f_i \geq 0$ if $i = 1, \ldots, d-1,\ f_i = 0$ if $i = d, \ldots, n,\ f(0) > 0,\ f(i) \geq 0$ if $i = 1, 2, \ldots, n$. Then by the Delsarte inequalities,

$$A_v(n,d) \leq A_v^*(n,d),$$

$$B_v(n,d) \geq B_v^*(n,d) \geq B_v^{**}(n,d). \tag{1.4}$$

Using the split distance distribution [27] of a code and generalizing this method we prove that

$$B_v(n, t+1; N, T+1) \geq$$

$$\max(B_v^*(n,t+1)B_v^{**}(N,T+1), B_v^{**}(n,t+1)B_v^*(N,T+1) \tag{1.5}$$

In order to use the bound (1.5) we need to represent the known Singleton [36] and Rao [31] bounds as the following linear programming bounds on $B_v^{**}(n,d)$:

$$B_v^*(n,d) \geq B_v^{**}(n,d) \geq v^{d-1} \tag{1.6}$$

and

$$B_v^*(n,d) \geq B_v^{**}(n,d) \geq R^{n,v}(d), \tag{1.7}$$

where for an integer $d = 2l + 1 + \sigma,\ \sigma \in \{0, 1\}$,

$$R^{n,v}(d) = v^{\sigma} \sum_{i=0}^{l} \binom{n-\sigma}{i} (v-1)^i.$$

Moreover, we get one more lower bound on $B_v^*(n,d)$ with the help of the following important result on duality in bounding the optimal sizes of codes and designs [24]:

$$A_v^*(n,d) B_v^*(n,d) = v^n \tag{1.8}$$

and the following linear programming bound for codes [21], [24]:

$$A_v^*(n,d) \le L^{n,v}(d) = \begin{cases} L_k^{n,v}(d) & \text{if } d_k(n-1) \le d-1 \le d_{k-1}(n-2) \\ vL_k^{n-1,v}(d) & \text{if } d_k(n-2) \le d-1 \le d_k(n-1) \end{cases} \tag{1.9}$$

where $d_k(n) = d_k(n,v)$ is the smallest root of $K_k^{n,v}(z)$ and

$$L_k^{n,v}(z) = \sum_{i=0}^{k-1} \binom{n}{i} (v-1)^i - \binom{n}{k} (v-1)^k \frac{K_{k-1}^{n-1,v}(z-1)}{K_k^{n,v}(z)}.$$

Basic results of the paper are presented in Sections 7 and 8. In Section 7, using (1.1), (1.2), (1.4)-(1.9) we obtain three upper bounds on $T_v(n,t)$ and $N_v(n,T)$ and five more upper bounds on $N_v(n,t,T)$. In Section 8, we describe a construction of independent resilient systems by means of two OAs which shows that all the above-mentioned upper bounds can be attained for some parameters. In particular, by this construction, the maximum number N such that

$$N \le k_v(n, t+1) + k_v(N, T+1)$$

provides a lower bound on $N_v(n,t,T)$, where $k_v(n,d)$ is the maximal dimension of a systematic linear d-code of length n over the residue-class ring $\mathbf{Z}_v$ or over the finite field $\mathbf{F}_q$ when $v = q$ where q is a power of a prime. The derived lower and upper bounds allow us to find $T_v(n,t)$, $N_v(n,T)$, and $N_v(n,t,T)$ for some infinite families of parameters and obtain some asymptotic results. As an example, note that the maximal 6-wise independent 3-resilient system of Boolean functions in 16 variables consists of 23 (linear) functions and may be constructed by means of the perfect Golay and Hamming codes (in this case $k_2(16,4) = 11$, $k_2(23,7) = 12$, $R^{16,2}(4) = 2^5$, $R^{23,2}(7) = 2^{11}$).

2. Codes, Orthogonal Arrays, and Split Orthogonal Arrays

We consider the Hamming space F_v^n, which consists of vectors $\mathbf{x} = (x_1, \ldots, x_n)$, where all coordinates are contained in a set F_v of v $(v = 2, 3, \ldots)$ elements with metric $d(x,y)$ equal to the number of coordinates in which x and y differ.

An arbitrary matrix C with rows from F_v^n will be called a *code*, a *design* or an *orthogonal array* (OA) in F_v^n . The number of rows of C is called the *size* of C and denoted by $|C|$. The size $|C|$ can be more than the number of distinct rows in C. This last number is denoted by $r(C)$. We shall characterize C by the *minimal distance* $d(C)$ (of a code C) and the *maximal strength* $t(C)$ (of a design or an orthogonal array C), which are defined as follows. We call C a *d-code* $(d = 1, \ldots, n+1)$ if $|C| = r(C)$ and the distance between any two different rows of C is at least d. The value $d(C)$ is the maximum number d such that C is a d-code (thus $d(C) = n+1$ when C has only one row). We call C a *t-design*

$(t = 0, \ldots, n)$ if there exists an integer $\lambda = \lambda_t$ such that every vector of F_v^t occurs in any t columns of C exactly λ times. It is clear that $|C| = \lambda_t v^t$ and for any integer l $(0 \leq l \leq t)$, any t-design is an l-design (we assume that any C is a 0-design with $\lambda_0 = |C|$). A t-design C is usually called an orthogonal array of strength t and of index λ with n factors and v levels and is denoted $OA_\lambda(t, n; v)$. The value $t(C)$ is the maximum number t such that C is a t-design. In particular, $t(C) \geq 1$ if and only if every column of C contains every element of F_v the same number of times (that is, $\lambda_1 = |C|/v$).

The fundamental problems of coding and design theory are to find the maximum size $A_v(n, d)$ of a d-code in F_v^n and the minimum size $B_v(n, t+1)$ of a t-design in F_v^n (the meaning of the last notation will be clear from Section 6 where it is explained that $t(C)+1$ is the so-called dual distance of a code C). It should be noted that all results of the paper (in particular, the lower bounds) are also valid, if $B_v(n, t+1)$ is the minimum number $r(C)$ of distinct rows of a t-design C in F_v^n. Throughout the paper we sometimes omit the lower index v if $v = 2$.

From the definitions of d-code and $(d-1)$-design it follows that

$$A_v(n, d) \leq A_v(n+1, d) \leq v A_v(n, d), \tag{2.1}$$

$$A_v(n+1, d+1) \leq A_v(n, d), \tag{2.2}$$

$$B_v(n+1, d+1) \geq B_v(n, d+1) \geq B_v(n, d), \tag{2.3}$$

$$B_v(n+1, d+1) \geq v B_v(n, d). \tag{2.4}$$

It is significant to note that in the binary case

$$A(n+1, d+1) = A(n, d) \text{ for odd } d, \tag{2.5}$$

$$B(n+1, d+1) = 2B(n, d) \text{ for odd } d. \tag{2.6}$$

(the reverse inequality in (2.4) for $v = 2$ and d odd was proved in [33]; in Section 4 we give its simple proof based on a functional description of OAs).

A code C in F_v^n is called *k-systematic* $(k = 1, \ldots, n)$ if there exists a function $f : F_v^k \to F_v^{n-k}$ such that

$$C = \{|\mathbf{x}|f(\mathbf{x})|, \mathbf{x} \in F_v^k\} \tag{2.7}$$

and hence C consists of v^k rows (throughout the paper we understand $|\mathbf{x}|\mathbf{y}|$ as the concatenation of vectors $\mathbf{x}$ and $\mathbf{y}$ as in [27]). We denote by $\tilde{k}_v(n, d)$ (respectively by $\tilde{l}_v(n, d)$) the maximum (respectively, the minimum) integer k such that there exists a k-systematic d-code (respectively, $(d-1)$-design)) in F_v^n. By the definition,

$$A_v(n, d) \geq v^{\tilde{k}_v(n,d)} \text{ and } B_v(n, d) \leq v^{\tilde{l}_v(n,d)}. \tag{2.8}$$

For constructing codes and designs it is useful to endow F_v with the algebraic structure of the residue-class ring $\mathbf{Z}_v = \{0, \ldots, v-1\}$ or of the finite field $\mathbf{F}_q$ when $v = q$ where q is a power of a prime. In both cases we call a set $C \subseteq F_v^n$ a *linear code* if together with arbitrary vectors it contains any their linear combination over the ring or the field F_v. It is evident that any linear code over $\mathbf{F}_q$ is k-systematic for some k up to a permutation of columns, but it is not true for all linear codes over $\mathbf{Z}_v$ when v is not a prime. Note that for any k-systematic linear code C in F_v^n, there exists a matrix $G = G(C)$ of the size $k \times (n-k)$ such that (cf.(2.7))

$$C = \{|\mathbf{x}|\mathbf{x}G|, \mathbf{x} \in F_v^k\}. \tag{2.9}$$

We also denote by $k_v(n,d)$ (respectively, by $l_v(n,d)$) the maximum (respectively, the minimum) integer k such that there exists a k-systematic linear d-code (respectively, $(d-1)$-design) in F_v^n. Thus, in the case of $v = q$ we evaluate the extrema over codes which are linear over $\mathbf{Z}_q$ or over $\mathbf{F}_q$, though now we do not know codes and designs over rings better than those over fields[1]. It is obvious that

$$\tilde{k}_v(n,d) \geq k_v(n,d) \text{ and } \tilde{l}_v(n,d) \leq l_v(n,d). \tag{2.10}$$

We shall see in Section 6 that for any v and d, $k_v(n,d) + l_v(n,d) = n$ (as in the case of codes over fields).

Let us introduce a definition of *split orthogonal arrays* (SOAs), which plays a key role in the paper. This concept is based on partitioning the set of columns of a matrix into two parts and making different restrictions to them. For any integers t, n, T, N, λ $(0 \leq t \leq n,\ 0 \leq T \leq N)$, we denote by $\mathrm{SOA}_\lambda(t,n;T,N;v)$ a matrix C in F_v^{n+N} such that every vector from F_v^{t+T} occurs exactly λ times in any $t+T$ columns of which t belong to the first n columns of C and T belong to the last N columns. It is clear that for such a SOA C, we have $|C| = \lambda v^{t+T}$. Denote by $B_v(n,t+1;N,T+1)$ the minimum of the parameter $r(C)$ (the number of distinct rows of C) over all C which are $\mathrm{SOA}_\lambda(t,n;T,N;v)$ for some λ, $\lambda = 1,2,\ldots$. Similarly to the case of OA, for any integers l and L, $0 \leq l \leq t$, $0 \leq L \leq N$, any $\mathrm{SOA}_\lambda(t,n;T,N;v)$ is a $\mathrm{SOA}_{\lambda v^{t-l+T-L}}(l,n;L,N;v)$. Moreover, any $OA_\lambda(t+T,n+N;v)$ is a $\mathrm{SOA}_\lambda(t,n;T,N;v)$ and hence

$$B_v(n,t+1;N,T+1) \leq B_v(n+N,t+T+1).$$

We shall see that the first quantity can be much smaller than the second one.

Example 2.1. *We shall prove in Section 8 that the 8-systematic linear code C in F_2^{16} with the matrix*

[1] Indeed, for any linear d-code of length n over $\mathbf{Z}_q$ there exists a linear d-code of length n over $\mathbf{F}_q$ of the same or more size (this was messaged to the author by A.A. Nechaev).

$$G = G(C) = \left\| \begin{array}{cccccccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array} \right\|$$

(see (2.9)) forms a $\mathrm{SOA}_4(8,3;8,3;2)$ of size 2^8. On the other hand, $B_2(16,7) \geq 697$ by the Rao bound (see Section 6).

Since the definitions of k-systematic and linear codes were given for any matrix, we can extend them to SOAs. Moreover, we shall call *systematic* any n-systematic $\mathrm{SOA}_\lambda(t,n;T,N;v)$.

3. Independent Resilient Systems of Functions and Split Orthogonal Arrays

Assume that the variables are taken from $F_v = \{0,\ldots,v-1\}$ and consider functions over F_v. A system of T such functions $f_1(\mathbf{x}),\ldots,f_T(\mathbf{x})$, where $\mathbf{x} = (x_1,\ldots,x_n) \in F_v^n$ is called *t-resilient* and denoted by $(t,n;T;v) - RS$ if for every t-subset $\{i_1,\ldots,i_t\} \subseteq \{1,\ldots,n\}$ and for any choices of $a_j \in F_v$, $j = 1,\ldots,t$, and of $b_h \in F_v$, $h = 1,\ldots,T$, the number of vectors $\mathbf{x}$ such that

$$x_{i_j} = a_j, \ j = 1,\ldots,t,$$

and

$$f_h(x_1,\ldots,x_n) = b_h, \ h = 1,\ldots,T,$$

is equal to v^{n-t-T} (in the paper [37] by Massey and Stinson such t-resilient system is called a t-resilient function and denoted $(n,T,t) - RF$). If we consider $x_1,\ldots,x_n$ as independent and uniformly distributed random variables then from the definition of a t-resilient system it follows that both these functions in n variables and the functions in $n-t$ variables obtained from them after any substitution of constants for any t variables will be random variables with the same properties. The maximum number T such that there exists a $(t,n;T;v) - RS$ is denoted by $T_v(n,t)$; a $(t,n;T;v) - RS$ with $T = T_v(n,t)$ is called *maximal* t-resilient system. Since $v^{n-t-T} \geq 1$, we have

$$T_v(n,t) \leq n - t. \tag{3.1}$$

Thus, the number of functions in any t-resilient system does not exceed the number of variables.

A system of N functions $f_1(\mathbf{x}), \ldots, f_N(\mathbf{x})$ in n variables over F_v is called *T-wise independent t-resilient* and denoted by $(t, n; T, N; v) - IRS$ if any subset of T functions of the system forms a t-resilient system. The maximum number N $(N \geq T \geq 2)$ such that there exists a $(t, n; T, N; v) - IRS$ is denoted by $N_v(n, t, T)$; a $(t, n; T, N; v) - IRS$ with $N = N_v(n, t, T)$ is called *maximal.* We shall see that $N_v(n, t, T)$ for some t and T can grow exponentially with n (cf. (3.1)).

Theorem 3.1. *The existence of a $(t, n; T, N; v) - IRS$ is equivalent to that of a systematic $SOA_\lambda(t, n; T, N; v)$ (with $\lambda = v^{n-t-T}$).*

Proof. There exists a one-to-one correspondence between systems of functions $f_1(\mathbf{x}), \ldots, f_N(\mathbf{x})$ in n variables over F_v and matrices of size $v^n \times (n + N)$ given by

$$(x_1, \ldots, x_n, f_1(\mathbf{x}), \ldots, f_N(\mathbf{x})), \text{ where } \mathbf{x} = (x_1, \ldots, x_n) \text{ runs over } F_v^n. \tag{3.2}$$

Then Theorem follows from the definitions of a systematic $\mathrm{SOA}_\lambda(t, n; T, N; v)$ and $(t, n; T, N; v) - IRS$. ∎

Since for $t = 0$ the existence of a systematic $\mathrm{SOA}_{v^{n-t-T}}(t, n; T, N; v)$ is equivalent to that of an $OA_{v^{n-T}}(T, N; v)$ we have the following special case.

Corollary 3.2. *A T-wise independent system of N functions of the form $F_v^n \to F_v$ exists if and only if there exists an $OA_{v^{n-T}}(T, N; v)$.*

Since for $N = T$ and for any choice of $b_h \in F_v$, $h = 1, \ldots, T$, rows (3.2) with

$$f_h(x_1, \ldots, x_n) = b_h, \ \ h = 1, \ldots, T,$$

form an $OA_\lambda(t, n; v)$ with $\lambda = v^{n-t-T}$, we get Stinson's result [37].

Corollary 3.3. *The existence of a $(t, n; T; v) - RS$ is equivalent to that of a partition of F_v^n into v^T $OA_\lambda(t, n; v)$ (with $\lambda = v^{n-t-T}$).*

Thus the existence of a $\mathrm{SOA}_{v^{n-t-T}}(t, n; T, N; v)$, of an $OA_{v^{n-t-T}}(t, n; v)$, and of an $OA_{v^{n-T}}(T, N; v)$ gives rise to the following necessary conditions

$$v^n \geq B_v(n, t + 1; N, T + 1), \tag{3.3}$$

$$v^n \geq B_v(N, T + 1), \tag{3.4}$$

and

$$v^{n-T} \geq B_v(n, t + 1) \tag{3.5}$$

for the existence of a $(t,n;T,N;v)-IRS$, of a T-wise independent system of N functions of the form $F_v^n \to F_v$, and of a $(t,n;T;v)-RS$, respectively. In particular,

$$v^{T_v(n,t)} \le \frac{v^n}{B_v(n,t+1)}. \tag{3.6}$$

Sufficient conditions for the existence of resilient systems of functions will be considered in Section 8.

4. Functional Description of Split Orthogonal Arrays

In this section, we consider a functional description of orthogonal arrays suggested by Delsarte in [10], [11] and extend it to the case of split orthogonal arrays. This gives rise to another definition of the maximal strength $t(C)$ and will be used to obtain lower bounds for $B_v(n,t+1)$ and $B_v(n,t+1;N,T+1)$.

We consider the Hamming space F_v^n over $F_v = \mathbf{Z}_v$ and denote by $F_v^{n,i}$ the subset of F_v^n consisting of all vectors with i nonzero coordinates.

Let $\mathbf{L}$ be a linear space of complex-valued functions $u(\mathbf{x})$, $\mathbf{x} \in F_v^n$, with the inner product

$$\langle u, w\rangle = v^{-n} \sum_{\mathbf{x}\in F_v^n} u(\mathbf{x})\overline{w(\mathbf{x})}, \tag{4.1}$$

and suppose $\xi = \xi_v$ is a primitive v^{th} degree root of unity. Hence,

$$\sum_{x=0}^{v-1} \xi^{ax} = v\delta_{a,0} \text{ for any } a \in \{0,1,\ldots,v-1\}. \tag{4.2}$$

For any fixed $\mathbf{a} = (a_1,\ldots,a_n) \in F_v^n$, we define a function $u_{\mathbf{a}}(\mathbf{x})$ in $\mathbf{x} = (x_1,\ldots,x_n) \in F_v^n$ as follows:

$$u_{\mathbf{a}}(\mathbf{x}) = \xi^{\mathbf{a}\cdot\mathbf{x}} \text{ , where } \mathbf{a}\cdot\mathbf{x} = \sum_{i=1}^{n} a_i x_i. \tag{4.3}$$

In particular, $u_{\mathbf{a}}(\mathbf{x}) \equiv 1$ if $\mathbf{a} = (0,\ldots,0)$. Since

$$\langle u_{\mathbf{a}}, u_{\mathbf{b}}\rangle = v^{-n} \prod_{i=1}^{n} \sum_{x_i=0}^{v-1} \xi^{(a_i-b_i)x_i} = \delta_{\mathbf{a},\mathbf{b}},$$

$\{u_{\mathbf{a}}(\mathbf{x}), \mathbf{a} \in F_v^n\}$ is an orthonormal (with respect to (4.1)) basis of $\mathbf{L}$. Therefore, for any $\mathbf{b} \neq (0,\ldots,0)$,

$$\sum_{\mathbf{x}\in F_v^n} u_{\mathbf{b}}(\mathbf{x}) = v^n\langle 1, u_{\mathbf{b}}\rangle = 0. \tag{4.4}$$

Theorem 4.1 (Delsarte Theorem). *A code C in F_v^n is a t-design (or $OA_\lambda(t,n;v)$) if and only if*

$$\sum_{\mathbf{x}\in C} u_{\mathbf{a}}(\mathbf{x}) = 0 \text{ for any } \mathbf{a} \in \bigcup_{i=1}^{t} F_v^{n,i}. \tag{4.5}$$

Proof. By the definition, a code C forms a t-design if and only if for any integers h $(1 \le h \le t)$ and $j_1, \ldots, j_h$ $(1 \le j_1 < \ldots < j_h \le n)$ and any $a_j \in \{0, \ldots, v-1\}$ $(j = 1, \ldots, h)$,

$$\sum_{\mathbf{x}=(x_1,\ldots,x_n)\in C} \prod_{j=1}^{h} \delta_{x_{i_j},a_j} = \lambda = v^{-h}|C|. \tag{4.6}$$

For any $i_1, \ldots, i_h$ $(1 \le i_1 < \ldots < i_h \le n)$ and any $b_j \in \{1, \ldots, v-1\}$, $j = 1, \ldots, h$, denote by $\mathbf{e}(i_1, \ldots, i_h; b_1, \ldots, b_h)$ a vector $\mathbf{a} = (a_1, \ldots, a_n) \in F_v^n$ such that $a_{i_j} = b_j$, $j = 1, \ldots, h$, and $a_i = 0$ if $i \notin \{i_1, \ldots, i_h\}$. It is clear that

$$u_{\mathbf{e}(i_1,\ldots,i_h;b_1,\ldots,b_h)}(\mathbf{x}) = \prod_{j=1}^{h} u_{\mathbf{e}(i_j;b_j)}(\mathbf{x}). \tag{4.7}$$

Since by (4.2)

$$\delta_{x_i,a} = v^{-1}(1 + \sum_{b=1}^{v-1} \xi^{(x_i-a)b}) = v^{-1}(1 + \sum_{b=1}^{v-1} \xi^{-ab} u_{\mathbf{e}(i;b)}(\mathbf{x})), \tag{4.8}$$

from (4.7) it follows that (4.5) implies (4.6). On the other hand, for any $h, h = 1, \ldots, t$,

$$u_{\mathbf{e}(i_1,\ldots,i_h;b_1,\ldots,b_h)}(\mathbf{x}) = \sum_{a_1=0}^{v-1} \xi^{b_1 a_1} \cdots \sum_{a_h=0}^{v-1} \xi^{b_h a_h} \prod_{j=1}^{h} \delta_{x_{i_j},a_j}. \tag{4.9}$$

Therefore, using (4.2) we can see that (4.6) implies (4.5). ■

Theorem 4.2. *Let C be formed by the rows $|\mathbf{x}|\mathbf{y}|$, where $\mathbf{x} = (x_1, \ldots, x_n) \in F_v^n$ and $\mathbf{y} = (y_1, \ldots, y_N) \in F_v^N$. Then C is a $SOA_\lambda(t,n;T,N;v)$ if and only if for any $\mathbf{a} \in F_v^{n,i}$ and any $\mathbf{b} \in F_v^{N,j}$ with $0 \le i \le t$, $0 \le j \le T$, $i + j \ge 1$,*

$$\sum_{|\mathbf{x}|\mathbf{y}|\in C} u_{\mathbf{a}}(\mathbf{x}) u_{\mathbf{b}}(\mathbf{y}) = 0. \tag{4.10}$$

Proof. By the definition, a code C in F_v^{n+N} is a $\mathrm{SOA}_\lambda(t,n;T,N;v)$ if and only if for any integers k $(k \le t)$, $i_1, \ldots, i_k$ $(1 \le i_1 < \ldots < i_k \le n)$, l $(l \le T)$, $j_1, \ldots, j_l$ $(1 \le j_1 < \ldots < j_l \le N)$ and any $a_i, b_j \in \{0, 1, \ldots, v-1\}$ $(i = 1, \ldots, k; j = 1, \ldots, l)$,

$$\sum_{|\mathbf{x}|\mathbf{y}|\in C} \prod_{r=1}^{k} \delta_{x_{i_r},a_r} \prod_{s=1}^{l} \delta_{y_{j_s},b_s} = \lambda = v^{-(k+l)}|C|. \tag{4.11}$$

Similarly, to the proof of Theorem 4.1 one can see that by (4.8) and (4.7), Eq. (4.10) implies (4.11), and by (4.9) and (4.2), Eq. (4.11) implies (4.10). ■

The functional description of designs can be used to prove some of their non-trivial properties. For any $\mathbf{x} = (x_1, \ldots, x_n) \in F_2^n$, where $x_i \in \{0,1\}$, we denote by $\bar{\mathbf{x}}$ the vector $(1-x_1, \ldots, 1-x_n)$ and call a binary design C *self-complementary* if C contains $\mathbf{x}$ if and only if it contains $\bar{\mathbf{x}}$. For any binary t-design C by (4.6) with $h = t-1$ the following holds: if $C^{(0)} = \{|0|\mathbf{x}| : \mathbf{x} \in C\}$ and $C^{(1)} = \{|1|\mathbf{x}| : \mathbf{x} \in C\}$, then union of rows of $C^{(0)}$ and $C^{(1)}$ forms a self-complementary t-design.

Corollary 4.3. *Any self-complementary binary $2h$-design (or $OA_\lambda(2h, n; 2)$) is in effect a $(2h+1)$-design [33] (see also [23]). Moreover,*

$$B(n+1, 2h+2) = 2B(n, 2h+1), \tag{4.12}$$

$$B(n+1, 2h+2; N, T) = 2B(n, 2h+1; N, T), \tag{4.13}$$

$$T(n+1, 2h+1) = T(n, 2h), \tag{4.14}$$

$$N(n+1, 2h+1, T) = N(n, 2h, T), \tag{4.15}$$

$$N(n+1, 2m+1) = N(n, 2m) + 1. \tag{4.16}$$

Proof. In the binary case $\xi = -1$, and for any $\mathbf{x} \in F_2^n$, Eq. (4.3) gives that

$$u_{\mathbf{a}}(\mathbf{x}) = (-1)^i u_{\mathbf{a}}(\mathbf{x}) = 0 \text{ if } \mathbf{a} \in F_2^{n,i}. \tag{4.17}$$

In particular, due to Theorem 4.1 this proves the first part of the Corollary. The inequalities $B(n+1, t+2) \geq 2B(n, t+1)$, $B(n+1, t+2; N, T) \geq 2B(n, t+1; N, T)$, $T(n+1, t+1) \leq T(n, t)$, and $N(n+1, t+1, T) \leq N(n, t, T)$ are easily obtained if one removes the first column or variable (out of $n+1$ ones). In order to prove for $t = 2h$ the opposite inequalities we replace each row $\mathbf{x}$ of an $OA_\lambda(2h, n; 2)$ and each row $|\mathbf{x}|\mathbf{y}|$ of a $SOA_\lambda(2h, n; T, N; 2)$, where $\mathbf{x} \in F_2^n$ and $\mathbf{y} \in F_2^N$, by two the rows $|0|\mathbf{x}|$ and $|1|\bar{\mathbf{x}}|$ or $|0|\mathbf{x}|\mathbf{y}|$ and $|1|\bar{\mathbf{x}}|\mathbf{y}|$, respectively. As a result, we obtain a self-complementary $2h$-design of length $n+1$ and, hence, a $(2h+1)$-design (which in the case of SOA consists of prefixes of length $n+1$ of all vectors with arbitrary fixed constants in arbitrary T places of $\mathbf{y}$). This completes the proof of (4.12) and (4.13). The same construction allows us to increase by one the parameters n and $2h$ in a $(n, 2h; T; 2) - RS$ and in a $(n, 2h; T, N; 2) - IRS$. In the last case, we also use Theorem 3.1 and the fact that the construction preserves the property to be a systematic design. This gives (4.14) and (4.15). Since the same construction also shows that the existence of an $OA_{2^{n-2m}}(2m, N; 2)$ is equivalent to that of an $OA_{2^{n-2m}}(2m+1, N+1; 2)$, Corollary 3.2 implies (4.16). Herewith, if $\{f_i(x_1, ..., x_n), i = 1, ..., N\}$ is a $2m$-wise independent system of Boolean functions, then $\{f_i(x_1, ..., x_n) \oplus x_{n+1}, i = 0, 1, ..., N\}$, where $f_0(x_1, ..., x_n) \equiv 0$, is a $(2m+1)$-wise independent system of $N+1$ Boolean functions in $n+1$ variables. ■

5. Krawtchouk Polynomials, Dual Distance, and Split Distance Distribution

Now we discuss some classical results and provide them with short proofs. Similar arguments being applied twice allow us to generalize these results to the case of split orthogonal arrays and split distance distributions. The Krawtchouk polynomials $K_k^{n,v}(z)$ of degree k, $k = 0, \ldots, n$, in a real variable z are defined by (1.3). The main applications of the Krawtchouk polynomials for investigation of d-codes and t-designs in the Hamming space F_v^n are based on the following identity

$$K_k^{n,v}(d(\mathbf{x}, \mathbf{y})) = \sum_{\mathbf{a} \in F_v^{n,k}} u_{\mathbf{a}}(\mathbf{x}) \overline{u_{\mathbf{a}}(\mathbf{y})}, \tag{5.1}$$

which is valid for any $\mathbf{x}, \mathbf{y} \in F_v^n$. Since $\sum_{b=1}^{v-1} \xi^{bx} = -1 + v\delta_{x,0}$ (see (4.2)), Eq. (5.1) immediately follows from the fact that for $\mathbf{a} = \mathbf{e}(i_1, \ldots, i_k; b_1, \ldots, b_k)$, one has

$$u_{\mathbf{a}}(\mathbf{x}) \overline{u_{\mathbf{a}}(\mathbf{y})} = \prod_{j=1}^{k} \xi^{b_j (x_{i_j} - y_{i_j})}.$$

The orthogonality relation

$$\sum_{d=0}^{n} K_i^{n,v}(d) K_j^{n,v}(d) (v-1)^d \binom{n}{d} = v^n (v-1)^i \binom{n}{i} \delta_{i,j} \tag{5.2}$$

follows from (5.1) and the fact the functions $u_{\mathbf{a}}(\mathbf{x})$, $\mathbf{a} \in F_v^n$ are orthonormal with respect to (4.1). Another orthogonality relation, namely,

$$\sum_{d=0}^{n} K_i^{n,v}(d) K_d^{n,v}(j) = v^n \delta_{i,j} \tag{5.3}$$

is a consequence of (5.2) and the equality

$$(v-1)^i \binom{n}{i} K_d^{n,v}(i) = (v-1)^d \binom{n}{d} K_i^{n,v}(d)$$

based on the known properties of binomial coefficients. Let

$$f(z) = \sum_{i=0}^{n} f_i K_i^{n,v}(z) \tag{5.4}$$

be an arbitrary polynomial. Note that due to (5.3),

$$f_i = v^{-n} \sum_{d=0}^{n} f(d) K_d^{n,v}(i). \tag{5.5}$$

Let us introduce the notation

$$\Omega(f) = \frac{f(0)}{f_0}, \text{ if } f_0 \neq 0. \tag{5.6}$$

The polynomial

$$g(z) = \sum_{j=0}^{n} g_j K_j^{n,v}(z), \text{ where } g_j = v^{-n/2} f(j), \tag{5.7}$$

will be referred to as *dual* (to $f(z)$)) and denoted by $\tilde{f}(z)$.

Lemma 5.1. *For an arbitrary polynomial (5.4),*

$$f(z) = \tilde{g}(z) \text{ when } g(z) = \tilde{f}(z)$$

and

$$\Omega(f)\Omega(\tilde{f}) = v^n, \text{ if } f_0 \neq 0 \text{ and } f(0) \neq 0.$$

Proof. By (5.5) and (5.7),

$$v^{-n/2}\tilde{f}(i) = v^{-n} \sum_{j=0}^{n} f(j) K_j^{n,v}(i) = f_i, \tag{5.8}$$

which proves the lemma. ■

Example 5.2. *It is known (see [9, p.285] or [24, p.1308]) that for any l, $l = 0, \ldots, n$, the polynomial*

$$h_l(z) = v^{l/2} \binom{n-z}{l} \tag{5.9}$$

of degree l can be expanded as $h_l(z) = \sum_{j=0}^{n} h_{l,j} K_j^{n,v}(z)$, where

$$h_{l,i} = v^{-n+l/2} \sum_{k=0}^{n} \binom{n-k}{l} K_k^{n,v}(i) = \binom{n-i}{n-l} v^{-l/2}. \tag{5.10}$$

Hence, $\tilde{h}_l(z) = h_{n-l}(z)$ and $\Omega(h_l) = v^l$.

For an arbitrary code C in F_v^n, the vector $\mathbf{B}(C) = (B_0(C), \ldots, B_n(C))$, where

$$B_i(C) = \frac{1}{|C|} |\{(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C,\ d(\mathbf{x}, \mathbf{y}) = i\}|, \tag{5.11}$$

is called the *distance distribution* of C [27]. Note that the minimal distance $d(C)$ of a code C (containing at least two distinct rows) can be defined as the minimum integer i ($i = 1, \ldots, n$) such that $B_i(C) \neq 0$. The dual distance distribution $\mathbf{B}'(C) = (B'_0(C), B'_1(C), \ldots, B'_n(C))$ is defined by using the *MacWilliams transform* [27, p. 137] of $\mathbf{B}(C)$ as follows

$$B'_i(C) = \frac{1}{|C|}\sum_{d=0}^{n} B_d(C)K_i^{n,v}(d), \quad i = 0, 1, \ldots, n. \tag{5.12}$$

Since $K_0^{n,v}(z) \equiv 1$, $B'_0(C) = 1$ by (5.11). The minimum integer i ($i = 1, \ldots, n$) such that $B'_i(C) \neq 0$ is denoted by $d'(C)$ and called the *dual distance* of C (if $B'_i(C) = 0$ for all $i = 1, \ldots, n$, then it is possible to prove that C is a union of some copies of entire F_v^n, and we put $d'(C) = n + 1$ in this case).

Lemma 5.3 (MacWilliams identities). *For any code C in F_v^n and any polynomial (5.4),*

$$\sum_{i=0}^{n} B_i(C)f(i) = |C|\sum_{i=0}^{n} f_i B'_i(C), \tag{5.13}$$

$$\sum_{i=0}^{n} f_i B_i(C) = v^{-n}|C|\sum_{i=0}^{n} B'_i(C)f(i). \tag{5.14}$$

Proof. Eq. (5.13) follows from (5.12), and Eq. (5.14) is obtained by considering (5.12) for the dual polynomial $\tilde{f}(z)$ and using (5.7) and (5.8). ∎

In particular, for $f(z) = K_i^{n,v}(z)$ (5.14) implies that

$$B_i(C) = \frac{|C|}{v^n}\sum_{d=0}^{n} B'_d(C)K_i^{n,v}(d),\; i = 0, 1, \ldots, n. \tag{5.15}$$

From (5.12), (5.11) and (5.1) there follows an important result by Delsarte [10], [11] which explains the functional sense of values $B'_i(C)$ and proves their nonnegativity.

Lemma 5.4. *For any code C in F_v^n and any $i = 0, 1, \ldots, n$,*

$$|C|^2 B'_i(C) = \sum_{\mathbf{x},\mathbf{y}\in C} K_i^{n,v}(d(\mathbf{x},\mathbf{y})) = \sum_{\mathbf{a}\in F_v^{n,i},} |\sum_{\mathbf{x}\in C} u_{\mathbf{a}}(\mathbf{x})|^2 \geq 0. \tag{5.16}$$

By Theorem 4.1, this gives

Theorem 5.5 (Delsarte Theorem). *A code C in F_v^n is a t-design if and only if*

$$|C|^2 B'_i(C) = \sum_{\mathbf{x},\mathbf{y}\in C} K_i^{n,v}(d(\mathbf{x},\mathbf{y})) = 0 \text{ for } i = 1, \ldots, t.$$

Moreover, $d'(C) = t(C) + 1$ for any code C.

Thus, the value $B_v(n,d)$ defined above can be also considered as the minimum size of a code C in F_v^n with $d'(C) \geq d$. A code C' in F_v^n is called *formally dual* to a code C with different rows (i.e., $B_0(C) = 1$), if $\mathbf{B}(C') = \mathbf{B}'(C)$ (by (5.12) and (5.15) for $i = 0$, $B_0(C') = B_0'(C) = 1$, $|C||C'| = v^n$, and this relation is symmetrical). It follows that the dual distance $d'(C)$ of C is the minimal distance $d(C')$ of a formally dual code C', if that exists.

For a linear code C in the Hamming space F_v^n over the ring $\mathbf{Z}_v$ or the field $\mathbf{F}_q$ when $v = q$, one can define a *dual* code

$$C^\perp = \{\mathbf{x} = (x_1, \ldots, x_n) \in F_v^n : \sum_{i=1}^{n} x_i y_i = 0 \text{ for any } \mathbf{y} = (y_1, \ldots, y_n) \in C\}.$$

Theorem 5.6 (MacWilliams Theorem). *For any linear code C the dual code $C^\perp$ is formally dual to C.*

Proof. For a proof of this well-known Theorem it is sufficient to check that

$$\frac{1}{|C|} \sum_{\mathbf{x} \in C} u_{\mathbf{a}}(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{a} \in C^\perp \\ 0 & \text{if } \mathbf{a} \notin C^\perp \end{cases} \tag{5.17}$$

since then by (5.16)

$$B_i'(C) = \frac{1}{|C|^2} \sum_{\mathbf{a} \in F_v^{n,i}} |\sum_{\mathbf{x} \in C} u_{\mathbf{a}}(\mathbf{x})|^2 = |C^\perp \bigcap F_v^{n,i}|. \tag{5.18}$$

If C is linear over $\mathbf{Z}_v$ and $\mathbf{a} \cdot \mathbf{x} \neq 0$, where $\mathbf{x} \in C$, we can factorize the group C by the subgroup formed by multiples of $\mathbf{x}$ and use (4.2) in order to prove (5.17). For linear codes over $\mathbf{F}_q$, $q = p^m$, we assume $u_{\mathbf{a}}(\mathbf{x}) = \xi_p^{Tr(\mathbf{a}\cdot\mathbf{x})}$ (cf. (4.3)), where ζ_p is primitive p^{th} degree root of unity and $Tr(\ )$ is the absolute trace from $\mathbf{F}_q$ to $\mathbf{F}_p$. Then Eqs. (5.1), (5.17) and (5.18) are still valid. ■

Theorems 5.5 and 5.6 allow us to construct linear t-designs by using dual codes with minimal distance $t+1$. Note that for a systematic linear code C, defined by (2.9) there exists a formally dual systematic linear code, obtained from the dual code $C^\perp = \{|\mathbf{x}G^T|\mathbf{x}|,\ \mathbf{x} \in F_v^{n-k}\}$, where G^T is the transpose of G, by a permutation of columns. Therefore

$$k_v(n,d) + l_v(n,d) = n \tag{5.19}$$

and

$$B_v(n,d) \leq v^{n-k_v(n,d)}.$$

For an arbitrary code C consisting of rows $|\mathbf{x}|\mathbf{y}|$, where $\mathbf{x} \in F_v^n$ and $\mathbf{y} \in F_v^N$, we consider the set of $(n+1)(N+1)$ numbers

$$B_{i,j}(C) = \frac{1}{|C|}|\{(|\mathbf{x}|\mathbf{y}|, |\mathbf{u}|\mathbf{v}|) : |\mathbf{x}|\mathbf{y}|, |\mathbf{u}|\mathbf{v}| \in C,\ d(\mathbf{x},\mathbf{u}) = i,\ d(\mathbf{y},\mathbf{v}) = j\}|$$

$i = 0,\dots,n$, $j = 0,\dots,N$, which is called the *split distance distribution* of C ([27, p. 149]). We define the numbers $B'_{k,l}(C)$, $k = 0,\dots,n$, $l = 0,\dots,N$, as follows:

$$B'_{k,l}(C) = \frac{1}{|C|}\sum_{k=0}^{n}\sum_{l=0}^{N} B_{i,j}(C)K_k^{n,v}(i)K_l^{N,v}(j). \tag{5.20}$$

Similarly to Lemmas 5.3 and 5.4, we get the following statements.

Lemma 5.7. *For any code C in F_v^{n+N} and any polynomials $f(z) = \sum_{i=0}^{n} f_i K_i^{n,v}(z)$ and $g(z) = \sum_{j=0}^{N} g_j K_j^{N,v}(z)$,*

$$\sum_{i=0}^{n}\sum_{j=0}^{N} B_{i,j}(C)f(i)g(j) = |C|\sum_{i=0}^{n}\sum_{j=0}^{N} f_i g_j B'_{i,j}(C), \tag{5.21}$$

$$\sum_{i=0}^{n}\sum_{j=0}^{N} f_i g_j B_{i,j}(C) = v^{-(n+N)}|C|\sum_{i=0}^{n}\sum_{j=0}^{N} B'_{i,j}(C)f(i)g(j). \tag{5.22}$$

In particular,

$$B_{k,l}(C) = v^{-(n+N)}|C|\sum_{i=0}^{n}\sum_{j=0}^{N} B'_{i,j}(C)K_k^{n,v}(i)K_l^{N,v}(j). \tag{5.23}$$

Lemma 5.8. *For any code C in F_v^{n+N} and any k, $k = 0,1,\dots,n$, and l, $l = 0,\dots,N$,*

$$|C|^2 B'_{k,l}(C) = \sum_{|\mathbf{x}|\mathbf{y}|\in C}\ \sum_{|\mathbf{u}|\mathbf{v}|\in C} K_k^{n,v}(d(\mathbf{x},\mathbf{u}))K_l^{N,v}(d(\mathbf{y},\mathbf{v})) =$$

$$= \sum_{\mathbf{a}\in F_v^{n,k}}\ \sum_{\mathbf{b}\in F_v^{N,l}} \Big|\sum_{|\mathbf{x}|\mathbf{y}|\in C} u_{\mathbf{a}}(\mathbf{x})u_{\mathbf{b}}(\mathbf{y})\Big|^2 \geq 0. \tag{5.24}$$

By Theorem 4.2, this gives

Theorem 5.9. *Let C be formed by rows $|\mathbf{x}|\mathbf{y}|$, where $\mathbf{x} = (x_1,\dots,x_n) \in F_v^n$ and $\mathbf{y} = (y_1,\dots,y_N) \in F_v^N$. Then C is a $SOA_\lambda(t,n;T,N;v)$ if and only if for any i and j, where $0 \leq i \leq t$, $0 \leq j \leq T$, $i + j \geq 1$,*

$$|C|^2 B'_{i,j}(C) = \sum_{|\mathbf{x}|\mathbf{y}|\in C} \sum_{|\mathbf{u}|\mathbf{v}|\in C} K_i^{n,v}(d(\mathbf{x},\mathbf{u})) K_j^{N,v}(d(\mathbf{y},\mathbf{v})) = 0. \tag{5.25}$$

For a code C in F_v^{n+N} with $B_{0,0}(C) = 1$, we call a code C' in F_v^{n+N} *formally split-dual* to C if $B_{k,l}(C') = B'_{k,l}(C)$ for any $k = 0, \ldots, n$, $l = 0, \ldots, N$ (by (5.20) and (5.23) for $k = l = 0$, $B_{0,0}(C') = B'_{0,0}(C) = 1$, $|C||C'| = v^{n+N}$ and this relation is symmetrical).

Theorem 5.10. *For any linear code C in F_v^{n+N}, a dual code $C^\perp$ is formally split-dual to C.*

Proof. It is based on (5.1), (5.17), (5.24) and the fact that for linear codes over both the ring $\mathbf{Z}_v$ and the field $\mathbf{F}_q$, $u_{\mathbf{a}}(\mathbf{x})u_{\mathbf{b}}(\mathbf{y}) = u_{|\mathbf{a}|\mathbf{b}|}(|\mathbf{x}|\mathbf{y}|)$. ■

6. Linear Programming Bound for Split Orthogonal Arrays. The Known Universal Bounds

We shall say that a polynomial $f(z) = \sum_{i=0}^{n} f_i K_i^{n,v}(z)$ has the property $\mathcal{A}_d = \mathcal{A}_d^{n,v}$, where $d = 1, \ldots, n+1$, if

$$f_0 > 0, \quad f_i \geq 0 \quad \text{if} \quad i = 1, 2, \ldots, n, \tag{6.1}$$

$$f(0) > 0, \quad f(i) \leq 0 \quad \text{if} \quad i = d, \ldots, n, \tag{6.2}$$

and has the property $\mathcal{B}_d = \mathcal{B}_d^{n,v}$, where $d = 1, \ldots, n+1$, if

$$f_0 > 0, \quad f_i \leq 0 \quad \text{if} \quad i = d, \ldots, n, \tag{6.3}$$

$$f(0) > 0, \quad f(i) \geq 0 \quad \text{if} \quad i = 1, 2, \ldots, n. \tag{6.4}$$

Recall that $\Omega(f) = \frac{f(0)}{f_0}$ and define

$$A_v^*(n,d) = \min \Omega(f) \tag{6.5}$$

where the minimum is taken over all polynomials $f(z)$ with $\mathcal{A}_d$, and

$$B_v^*(n,d) = \max \Omega(f) \tag{6.6}$$

where the maximum is taken over all polynomials $f(z)$ with $\mathcal{B}_d$.

The following statement is due to Delsarte [9]. However, it should be noted that the lower linear programming bound on the size of designs is proved below for the number of distinct rows of an orthogonal array which might be less than its size.

Theorem 6.1. *For any integers n, d, v $(1 \le d \le n+1,\ v \ge 2)$,*

$$A_v(n,d) \le A_v^*(n,d), \tag{6.7}$$

$$B_v(n,d) \ge B_v^*(n,d). \tag{6.8}$$

Proof. For a code C with $d(C) \ge 1$, $B_0(C) = 1$, $B_0'(C) = 1$ and by Lemma 5.4, all the values $B_i'(C)$ (together with the values $B_i(C)$) are nonnegative. Using a polynomial $f(z)$ that has the property $\mathcal{A}_d$ in (5.13), we obtain $f(0) \ge |C| f_0$, which leads to (6.7). Suppose now that a $(d-1)$-design C has rows of r distinct patterns (i.e., $r(C) = r$) and every pattern j $(j = 1, \dots, r)$ occurs m_j times. Then $|C| = \sum_{j=1}^r m_j$, $|C| B_0(C) = \sum_{j=1}^r m_j^2$, and $B_0'(C) = 1$. Taking account of Theorem 5.5 and using a polynomial $f(z)$ with the property $\mathcal{B}_d$ in (5.13), we obtain

$$f(0) \sum_{j=1}^r m_j^2 \le f_0 \left(\sum_{j=1}^r m_j \right)^2$$

and hence $f(0) \le f_0 r$, that leads to (6.8). ■

Theorem 6.2 ([24]). *For any integers n, d, v $(1 \le d \le n+1,\ v \ge 2)$,*

$$A_v^*(n,d) B_v^*(n,d) = v^n. \tag{6.9}$$

Proof. From the definitions of a dual polynomial and the properties $\mathcal{A}_d$ and $\mathcal{B}_d$ it follows that a polynomial has the property $\mathcal{A}_d$ if and only if the dual polynomial has the property $\mathcal{B}_d$. Therefore, Lemma 5.1 implies (6.9). ■

In order to estimate the size of SOAs we also use the value

$$B_v^{**}(n,d) = \max \Omega(f)$$

where the maximum is taken over all polynomials $f(z) = \sum_{i=0}^n f_i K_i^{n,v}(z)$ having the following property $\bar{\mathcal{B}}_d = \bar{\mathcal{B}}_d^{n,v}$:

$$f_0 > 0, f_i \ge 0 \quad \text{if} \quad i = 1, \dots, d-1, \quad f_i = 0 \quad \text{if} \quad i = d, \dots, n, \tag{6.10}$$

$$f(0) > 0, \quad f(i) \ge 0 \quad \text{if} \quad i = 1, 2, \dots, n.$$

Since condition (6.10) is stronger than (6.3), we have

$$B_v(n,d) \ge B_v^*(n,d) \ge B_v^{**}(n,d). \tag{6.11}$$

Theorem 6.3. *For any integers t, n, T, N, v $(0 \le t \le n,\ 0 \le T \le N,\ v \ge 2)$,*

$$B_v(n,t{+}1;N,T{+}1) \geq \max\left(B_v^*(n,t+1)B_v^{**}(N,T+1), B_v^{**}(n,t+1)B_v^*(N,T+1)\right)$$

Proof. Let $f(z) = \sum_{i=0}^{n} f_i K_i^{n,v}(z)$ and $g(z) = \sum_{j=0}^{N} g_j K_j^{N,v}(z)$ be polynomials having the properties $\mathcal{B}_{t+1}^{n,v}$ and $\mathcal{B}_{T+1}^{N,v}$ respectively. We also assume that $f(z)$ has the property $\bar{\mathcal{B}}_{t+1}^{n,v}$ or $g(z)$ has the property $\bar{\mathcal{B}}_{T+1}^{N,v}$, and hence $f_i g_j \leq 0$ if $i \geq t+1$ or $j \geq T+1$. Suppose that an arbitrary $\mathrm{SOA}_\lambda(t,n;T,N;v)$ C has rows of r distinct patterns (i.e., $r(C) = r$) and every pattern j ($j = 1,\ldots,r$) occurs m_j times. Then $|C| = \sum_{j=1}^{r} m_j$, $|C|B_{0,0}(C) = \sum_{j=1}^{r} m_j^2$ and $B'_{0,0}(C) = 1$. Taking account of Lemma 5.8 and Theorem 5.9 and using the polynomials $f(z)$ and $g(z)$ in (5.21), we obtain

$$f(0)g(0)\sum_{j=1}^{r} m_j^2 \leq f_0 g_0 \left(\sum_{j=1}^{r} m_j\right)^2$$

and hence $f(0)g(0) \leq f_0 g_0 r$, which leads to (6.11). ∎

The problems of finding $A_v^*(n,d)$ and $B_v^*(n,d)$ and optimal polynomials $f(z)$ that give the corresponding extrema for all d and n are so far open. It is not likely that such complete solutions of these problems will be found. However, any polynomial $f(z)$ that has property $\mathcal{A}_d$ or $\mathcal{B}_d$, respectively, gives rise to the bounds

$$A_v(n,d) \leq A_v^*(n,d) \leq \Omega(f), \tag{6.12}$$

$$B_v(n,d) \geq B_v^*(n,d) \geq \Omega(f). \tag{6.13}$$

Now we describe three families of polynomials which turn out to be optimal under a certain strengthening of the property $\mathcal{A}_d^{n,v}$ or $\mathcal{B}_d^{n,v}$. Due to Theorem 6.1 and (6.12)-(6.13) they lead to three pairs of universal (i.e., valid for all v, n and d) bounds on the size of d-codes and $(d-1)$-designs. The first pair is good when v is more than $n-2$, the other two are good when d is sufficiently small or large, respectively. For some parameters v, n and d these polynomials give rise to the equalities $A_v(n,d) = \Omega(f)$ or $B_v(n,d) = \Omega(f)$ and hence also determine the values $A_v^*(n,d)$ and $B_v^*(n,d)$. All the proofs of the results mentioned below in this section, and necessary and sufficient conditions for the attainability of the corresponding bounds can be found in [24].

1. First, for any d, $d = 1,\ldots,n+1$, we consider the polynomial

$$h_{d-1}(z) = v^{(d-1)/2}\binom{n-z}{d-1}$$

of degree $d-1$ (see (5.9)). Due to (5.10), $h_{d-1}(z)$ has the property $\bar{\mathcal{B}}_d = \bar{\mathcal{B}}_d^{n,v}$ and $\Omega(h_{d-1}) = v^{d-1}$. Hence by (6.13) and (6.9),

$$B_v(n,d) \geq B_v^*(n,d) \geq B_v^{**}(n,d) \geq v^{d-1}, \tag{6.14}$$

$$A_v(n,d) \le A_v^*(n,d) = \frac{v^n}{B_v^*(n,d)} \le v^{n-d+1}. \tag{6.15}$$

Bound (6.14) on the size of OA is trivial and bound (6.15) is the well-known Singleton bound [36]. Both these bounds are met by $[n,k,d=n-k+1]_q$ Reed-Solomon codes, which exist when $n \le q+1$ (see [27]).

2. For any integer d, there exists a unique integer $l = l(d)$ and a unique $\sigma = \sigma(d) \in \{0,1\}$ such that $d = 2l + \sigma + 1$ (it is clear that $l(d) = \lfloor \frac{d-1}{2} \rfloor$ and $\sigma(d) = d - 1 - 2\lfloor \frac{d-1}{2} \rfloor$). Define a function $R^{n,v}(d)$, $d = 1, \ldots, 2n+1$, as follows

$$R^{n,v}(d) = v^{\sigma(d)} \sum_{i=0}^{l(d)} \binom{n-\sigma(d)}{i} (v-1)^i. \tag{6.16}$$

The function $R^{n,v}(d)$ is increasing in d for the fixed n and v, and $R^{n,v}(d)$ and $v^n/R^{n,v}(d)$ are increasing in n for the fixed d ($d \ge 3$) and v. Furthermore, $R^{n,2}(n) = 2^{n-1}$ and for odd n, $R^{n,2}(n+1) = 2^n$.

Theorem 6.4. *For any d, $d = 1, \ldots, n+1$, the polynomial*

$$g^{d,n}(z) = (n-z)^{\sigma(d)} (K_{l(d)}^{n-1-\sigma(d),v}(z-1))^2 \tag{6.17}$$

of degree $d-1$ has the property $\bar{\mathcal{B}}_d^{n,v}$ and

$$\Omega(g^{d,n}) = R^{n,v}(d).$$

Hence,

$$B_v(n,d) \ge B_v^*(n,d) \ge B_v^{**}(n,d) \ge R^{n,v}(d), \tag{6.18}$$

$$A_v(n,d) \le A_v^*(n,d) = \frac{v^n}{B_v^*(n,d)} \le \frac{v^n}{R^{n,v}(d)}. \tag{6.19}$$

Moreover,

$$R^{n,v}(d) = \max \Omega(f), \tag{6.20}$$

where the maximum is taken over the polynomials $f(z) = \sum_{i=0}^n f_i K_i^{n,v}(z)$ of degree at most $d-1$ such that $f_0 > 0$ and $f(z) \ge 0$ for $0 \le z \le n$.

The inequality $B_v(n,d) \ge R^{n,v}(d)$ is due to Rao [31] (1947) and the inequality $A_v(n,d) \le v^n/R^{n,v}(d)$ is in effect the well-known Hamming bound [17] (1950). The fact that these bounds can be proved by the linear programming method was established by Delsarte [9]. The proof of (6.20) was accomplished by Dunkl [12] who used a result by Schoenberg and Szego [32]. It should be noted that in the binary case, the lower bound $R^{n,2}(d)$ on the quantity $B_2(n,d)$, together with $B_2(n,d)$ itself (see (2.6)), satisfies the functional equation

$$F(n+1, 2h+2) = 2F(n, 2h+1), \tag{6.21}$$

and the upper bound $2^n/R^{n,2}(d)$ to $A_2(n,d)$, together with $A_2(n,d)$ itself (see (2.5)), satisfies the functional equation

$$F(n+1, 2h+2) = F(n, 2h+1). \tag{6.22}$$

3. Denote by $d_k(n) = d_k(n,v)$ the smallest root of $K_k^{n,v}(z)$, $k = 1, \dots, n$, and let $d_0(n) = n+1$, $d_{n+1}(n) = 0$. In particular,

$$d_1(n) = \frac{(v-1)n}{v}, \; d_2(n) = \frac{2(v-1)n - v + 2 - \sqrt{4(v-1)n + (v-2)^2}}{2v}.$$

It is known that

$$d_k(n-2) < d_k(n-1) < d_{k-1}(n-2), \; k = 1, \dots, n-1.$$

Therefore for any real z, $1 < z \le n$, there exists a unique integer $k = k(z)$, $1 \le k \le n-1$, such that either

$$d_k(n-1) + 1 < z \le d_{k-1}(n-2) + 1 \tag{6.23}$$

or

$$d_k(n-2) + 1 < z \le d_k(n-1) + 1. \tag{6.24}$$

Let us put $\varepsilon(z) = 0$ ($\varepsilon(z) = 1$) if z lies in the domain defined in (6.23) and (6.24), respectively, and assume that $k(1) = n$, $\varepsilon(1) = 0$. For any k, $k = 1, \dots, n$, and any real z, let us introduce the notation

$$L_k^{n,v}(z) = \sum_{i=0}^{k-1} \binom{n}{i} (v-1)^i - \binom{n}{k} (v-1)^k \frac{K_{k-1}^{n-1,v}(z-1)}{K_k^{n,v}(z)}$$

and for $1 \le z \le n$, the notation

$$L^{n,v}(z) = v^{\varepsilon(z)} L_{k(z)}^{n-\varepsilon(z),v}(z). \tag{6.25}$$

The function $L^{n,v}(z)$ is continuous and positive, it decreases with z, and for $\varepsilon \in \{0,1\}$ and any k, $k = 0, 1, \dots, n-\varepsilon$, has the following property:

$$L^{n,v}(d_k(n-1-\varepsilon)+1) = R^{n,v}(2k+\varepsilon+1).$$

In particular, for any $\varepsilon \in \{0,1\}$, $L^{n,v}(n-\varepsilon+1) = R^{n,v}(1+\varepsilon) = v^\varepsilon$ and

$$L^{n,v}(\frac{(v-1)(n-\varepsilon)+1}{v}) = R^{n,v}(3+\varepsilon) = v^\varepsilon((v-1)(n-\varepsilon)+1). \tag{6.26}$$

Equation (6.25) defines $L^{n,v}(z)$ in $2n-1$ distinct intervals similar to as (6.16) does $R^{n,v}(d)$ for $2n+1$ values of d. For the first three intervals, $L^{n,v}(z)$ can be found in [24, p.1312].

For any d, $d=1,\ldots,n$, we denote by $f^{d,n}(z)$ the polynomial

$$(d-z)(n-z)^{\varepsilon(d)}\left(\sum_{i=0}^{k(d)-1}\frac{K_i^{n-1-\varepsilon(d),v}(z-1)K_i^{n-1-\varepsilon(d),v}(d-1)}{\binom{n-1-\varepsilon(d)}{i}(v-1)^i}\right)^2 \tag{6.27}$$

of degree

$$h(d)=2k(d)-1+\varepsilon(d). \tag{6.28}$$

Note that if the degree of a polynomial $F(z)$ is more than n and (see (5.5))

$$f_i=v^{-n}\sum_{d=0}^{n}F(d)K_i^{n,v}(d),\ i=0,\ldots,n,$$

then $F(z)=f(z) \pmod{z(z-1)\ldots(z-n)}$ where $f(z)=\sum_{i=0}^{n}f_iK_i^{n,v}(z)$. Since $F(j)=f(j)$ for $j=0,\ldots,n$, we can say that $F(z)$ has the property $\mathcal{A}_d$ or $\mathcal{B}_d$ if so does $f(z)$, and generalize (6.12) and (6.13) to the case of $F(z)$ assuming that $\Omega(F)=\Omega(f)$.

Theorem 6.5. *For any d, $d=1,\ldots,n$, the polynomial $f^{d,n}(z)$ has the property $\mathcal{A}_d^{n,v}$ and*

$$\Omega(f^{d,n})=L^{n,v}(d).$$

Hence

$$A_v(n,d)\le A_v^*(n,d)\le L^{n,v}(d), \tag{6.29}$$

$$B_v(n,d)\ge B_v^*(n,d)=\frac{v^n}{A_v^*(n,d)}\ge\frac{v^n}{L^{n,v}(d)}. \tag{6.30}$$

Moreover,

$$L^{n,v}(d)=\min\Omega(f), \tag{6.31}$$

where the minimum is taken over all the polynomials $f(z)=\sum_{i=0}^{n}f_iK_i^{n,v}(z)$ of degree at most $h(d)$ such that $f_0>0$ and $f(z)\le 0$ for $d\le z\le n$.

The bound (6.29) was announced in [20] (1978) and was proved in [21] (and also in [34]) for all d when $v=2$ and for all d such that $\varepsilon(d)=0$ when $v\ge 3$. A detailed proof without this restriction can be found in [22],[24]. Since in the binary case the functions $L^{n,2}(d)$ and $2^n/L^{n,2}(d)$ do not satisfy functional equations (6.22) and (6.21), respectively, using (2.5)-(2.6) one can improve (6.29)-(6.30) for odd d as follows:

$$A(n,2h+1)=A(n+1,2h+2)\le A^*(n+1,2h+2)\le L^{n+1,2}(2h+2), \tag{6.32}$$

$$2B(n,2h+1) = B(n+1,2h+2) \geq B^*(n+1,2h+2) \geq \frac{2^{n+1}}{L^{n+1,2}(2h+2)}. \quad (6.33)$$

The bound (6.30) on the size of $(d-1)$-designs was recently published by the author in [24]. In particular, in the binary case it gives the following first three bounds:

$$B(n,d) \geq \frac{(2d-n)2^{n-1}}{d} \quad \text{if} \quad \frac{n+1}{2} \leq d \leq n; \quad (6.34)$$

$$B(n,d) \geq \frac{(2d-n+1)2^{n-2}}{d} \quad \text{if} \quad \frac{n}{2} \leq d \leq \frac{n+1}{2};$$

$$B(n,d) \geq \frac{(4d(n-d)-n(n-1))2^{n-1}}{d(n(n+3)-d(n+1))} \quad \text{if} \quad \frac{n+1-\sqrt{n-1}}{2} \leq d \leq \frac{n}{2}.$$

The bound (6.34) which is dual to the well-known Plotkin bound for codes was published earlier in an equivalent form by Friedman [14]. In [3] the authors found $B^*(n,d)$ when $n/2 \leq d \leq n$ and obtained a strengthening of the Friedman bound for odd d of this interval. Note that the same improvement of (6.34) in this range can be also obtained by means of (6.33). Assertion (6.31) was proved in [22], [24] with help of some ideas of [20] and [34]. Necessary and sufficient conditions of attainability of the bounds (6.18)-(6.19), (6.29)-(6.30) and examples of codes and designs meeting them can be found in [24].

7. Upper Bounds on the Size of Independent Resilient Systems

Now we shall use the necessary conditions for the existence of t-resilient and of T-wise independent t-resilient systems of functions in n variables over F_v obtained in Section 3, and results of Section 6 in order to obtain upper bounds on their maximum size $T_v(n,t)$ and $N_v(n,t,T)$. From (3.6) and Theorems 6.1 and 6.2 it follows

Theorem 7.1. *For any integers n and t $(1 \leq t \leq n)$,*

$$v^{T_v(n,t)} \leq A_v^*(n,t+1). \quad (7.1)$$

Thus any linear programming bound on the size of a code C of length n with $d(C) \geq t+1$ gives rise to an upper bound on the size of a t-resilient system (and even of range of a correlation-immune function of order t, see (1.1)) . Since the Singleton bound (6.15), the Hamming bound (6.19) and the author's bound (6.29) can be obtained by the linear programming method, for any t-resilient system of T functions in n variables we have

$$T \leq T_v(n,t) \leq n-t, \quad (7.2)$$

$$v^T \le v^{T_v(n,t)} \le \frac{v^n}{R^{n,v}(t+1)}, \tag{7.3}$$

$$v^T \le v^{T_v(n,t)} \le L^{n,v}(t+1), \tag{7.4}$$

respectively. Moreover, in the binary case by (4.14) and (7.4), one obtains

$$2^T \le 2^{T(n,t)} = 2^{T(n+1,t+1)} \le L^{n+1,2}(t+2) \text{ when } t \text{ is even.} \tag{7.5}$$

For $n/2 \le t+1 \le n$ the bounds (7.4) when $v=2$ and (7.5) were obtained in [3].

Theorem 7.2. *For the existence of a* $(t,n;T,N;v)-IRS$ *it is necessary that*

$$v^n \ge \max(B_v^{**}(n,t+1)B_v^{*}(N,T+1), B_v^{*}(n,t+1)B_v^{**}(N,T+1)).$$

Proof. Follows from Theorems 3.1 and 6.3. ■

In particular, (6.14), (6.18), and (6.30) imply that for the existence of a $(t,n;T,N;v)-IRS$ the following five inequalities (together with (7.2)-(7.4)) must be satisfied:

$$v^n \ge R^{n,v}(t+1)R^{N,v}(T+1), \tag{7.6}$$

$$\frac{v^n}{R^{n,v}(t+1)} \ge \frac{v^N}{L^{N,v}(T+1)}, \tag{7.7}$$

$$L^{n,v}(t+1) \ge R^{N,v}(T+1), \tag{7.8}$$

$$v^{n-t} \ge R^{N,v}(T+1), \tag{7.9}$$

$$L^{N,v}(T+1) \ge v^{N+t-n}. \tag{7.10}$$

Note that for $t=0$ the inequalities (7.9) and (7.10) together with the trivial condition $T \le n$ are necessary for the existence of a T-wise independent system of N functions of the form $F_v^n \to F_v$. Due to some monotony properties of $R^{N,v}(T+1)$ and $L^{N,v}(T+1)$, (7.6)-(7.10) give upper bounds on $N_v(n,t,T)$ and, in particular, on $N_v(n,T)$. We shall see in the next section that all inequalities of Section 7 are attained for some parameters.

8. Constructing Independent Resilient Systems. Consequences

By Theorem 3.1, a construction of a T-wise independent t-resilient system of N functions in n variables over F_v is equivalent to the existence of a systematic $\mathrm{SOA}_{v^{n-t-T}}(t,n;T,N;v)$.

Theorem 8.1. *If for some k, $T \le k \le n-t$, there exist an $OA_{v^{k-T}}(T,N;v)$ C_1 and a $(n-k)$-systematic $OA_{v^{n-k-t}}(t,n;v)$ C_2, then there exists a systematic $SOA_{v^{n-t-T}}(t,n;T,N;v)$ C. Moreover, if C_1 is systematic and linear with the matrix $G(C_1)=G_1$ of order $k\times(N-k)$ and C_2 is systematic and linear with the matrix $G(C_2)=G_2$ of order $(n-k)\times k$, then the design C can be chosen to be systematic and linear with the matrix*

$$G(C) = \left\| \begin{array}{cc} -G_2 & -G_2G_1 \\ E_k & G_1 \end{array} \right\| \tag{8.1}$$

of order $n\times N$ (see (2.9); here E_k is the identity matrix of order k).

Proof. Let $\mathbf{z}_j$, $j=1,\dots,v^k$, be the rows of C_1, and $|\mathbf{x}_i|\mathbf{y}_i|$, $i=1,\dots,v^{n-k}$, where $\mathbf{x}_i\in F_v^{n-k}$, $\mathbf{y}_i\in F_v^k$, be the rows of C_2. Since C_2 is $(n-k)$-systematic, $\mathbf{x}_i$, $i=1,\dots,v^{n-k}$, run over F_v^{n-k}. Let $\mathbf{u}_j$, $j=1,\dots,v^k$, be all the vectors of F_v^k enumerated in any order. In the case when C_1 is systematic, we shall fix the order and assume that $\mathbf{u}_j$ is the prefix of length k of $\mathbf{z}_j$. We consider a code C of length $n+N$ consisting of the rows

$$|\mathbf{x}_i|\mathbf{y}_i+\mathbf{u}_j|\mathbf{z}_j|, \quad i=1,\dots,v^{n-k}, \quad j=1,\dots,v^k \tag{8.2}$$

By the construction, C is systematic. Moreover, if both C_1 and C_2 are systematic and linear, then C is linear, and $G(C)$ is defined by (8.1), since in this case, $\mathbf{y}_i=\mathbf{x}_iG_2$ and $\mathbf{z}_j=|\mathbf{u}_j|\mathbf{u}_jG_1|$. Let us verify that C is a $\mathrm{SOA}_{v^{n-t-T}}(t,n;T,N;v)$. Since C_1 is an $OA_{v^{k-T}}(T,N;v)$, for any $j_1,\dots,j_T$ $(1\le j_1<\dots<j_T\le N)$ and any $b_i\in F_v$, $i=1,\dots,T$, there exists a set $J\subset\{1,\dots,v^k\}$ of size $|J|=v^{k-T}$ such that the rows $\mathbf{z}_l$ of C_1 where $l\in J$ have the entries b_i in the columns j_i respectively, $i=1,\dots,T$. The matrix formed by the rows

$$|\mathbf{x}_i|\mathbf{y}_i+\mathbf{u}_j|,\ i=1,\dots,v^{n-k},\ j\in J,$$

is a union of v^{k-T} $OA_{v^{n-k-t}}(t,n;v)$'s and hence forms an $OA_{v^{n-t-T}}(t,n;v)$. This completes the proof. ■

Example 8.2. *Apply Theorem 8.1 for $n=N=8$, $t=T=3$, $k=5$, $v=2$. Since there exists a [8,4,4] linear self-dual code which is an $OA_2(3,8;2)$, we can use this code as both C_1 and C_2 with the matrix*

$$G(C_1)=G(C_2)=\left\| \begin{array}{cccc} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{array} \right\|,$$

It gives a systematic $SOA_2(3,8;3,8;2)$ C with the matrix $G(C)$ constructed by (8.2) and presented in Example 2.1, and hence there exists a 3-wise independent 3-resilient system of 8 linear Boolean functions in 8 variables. This system is maximal by (7.6) (see also Corollary 8.8).

Construction (8.2) was used in coding theory ([27, p. 582]). Here we used it for constructing designs. Since an $OA_1(T, T; v)$ coincides with a systematic linear code F_v^T, Theorem 8.1 for $k = N = T$ and Corollary 3.3 lead to the following result by Massey and Stinson [38].

Corollary 8.3. *A $(t, n; T; v)$-resilient system exists if there exist a systematic $OA_{v^{n-T-t}}(t, n; v)$.*

This means that the inequality

$$T \leq n - \tilde{l}_v(n, t+1) \tag{8.3}$$

is sufficient for the existence of such a system and, due to (5.19),

$$T_v(n, t) \geq n - \tilde{l}_v(n, t+1) \geq k_v(n, t+1). \tag{8.4}$$

Let us find $T_v(n, t)$ in the case when the linear programming bound $A_v(n, t+1) \leq A_v^*(n, t+1)$ is attained in the class of systematic linear codes.

Theorem 8.4. *If*

$$A_v^*(n, t+1) = v^{k_v(n,t+1)}, \tag{8.5}$$

then $A_v(n, t+1) = A_v^*(n, t+1)$, $B_v(n, t+1) = B_v^*(n, t+1) = v^{l_v(n,t+1)}$, and

$$T_v(n, t) = k_v(n, t+1),$$

and there exists a maximal t-resilient system, which is linear. If, in addition,

$$B_v(n+1, t+1) > B_v^*(n, t+1),$$

then

$$N_v(m, t) = n \quad \text{for} \quad m = l_v(n, t+1).$$

Proof. This follows from (2.8), (2.10), Theorem 6.2, (5.19), (6.11), (7.1), (8.4), and Corollary 3.2. ∎

In particular, (8.5) holds in the following cases:

$$k_q(n, t+1) = n - t \text{ when } 0 \leq t \leq n-1 \leq q, \tag{8.6}$$

$$k_q\left(\frac{q^h - 1}{q - 1}, 3\right) = \frac{q^h - 1}{q - 1} - h, \; k_q\left(\frac{q^h - 1}{q - 1}, q^{h-1}\right) = h, h = 2, 3, \ldots, \tag{8.7}$$

$$k(2^h, 4) = 2^h - h - 1, \; k(2^h, 2^{h-1}) = h + 1, \; h = 2, 3, \ldots . \tag{8.8}$$

It follows from (6.15), (6.19), (6.29), (6.26), and from the existence of the Reed-Solomon codes, the perfect and extended binary Hamming codes and dual codes to them. Using also Corollary 3.2 and the fact that $R^{n+1,2}(d) > R^{n,2}(d)$ for $d \geq 3$ we have the following. (We continue to omit lower indices v when $v = 2$; in particular, $\log x$ means $\log_2 x$.)

Corollary 8.5. *For any $h = 2, 3, \dots,$*

$$N_q(h,2) = \frac{q^h - 1}{q-1} \text{ and } N(h,3) = 2^h;$$

$$T(n,3) = \log\frac{2^{n-1}}{n} \text{ and } T(n, \frac{n}{2} - 1) = \log 2n, \text{ when } n = 2^h;$$

$$T_q(n,2) = \log_q \frac{q^n}{n(q-1)+1} \text{ and } T_q(n, \frac{(q-1)(n-1)}{q}) = \log_q(n(q-1)+1),$$

when $n = \frac{q^h-1}{q-1}$. Moreover,

$$T_q(n,t) = n - t \text{ when } 0 \le t \le n-1 \le q.$$

In [38], Stinson and Massey disproved the conjecture [2], [7] that any maximal t-resilient system of Boolean functions is linear. They considered nonlinear binary codes of length $n = 2^{2h}$, $h = 2, \dots,$ which are $(n - 2\log n)$-systematic with minimal distance 6 (Preparata codes [30]) and $2\log n$-systematic with the minimal distance $\frac{n-\sqrt{n}}{2}$ (Kerdock codes [18]). Since these codes are formally dual,

$$\tilde{l}(n,6) \le 2\log n \text{ and } \tilde{l}(n, \frac{n-\sqrt{n}}{2}) \le n - 2\log n, \tag{8.9}$$

and hence by (8.4)

$$T(n,5) \ge n - 2\log n \text{ and } T(n, \frac{n-\sqrt{n}}{2} - 1) \ge 2\log n. \tag{8.10}$$

Thus, they presented an infinite number of parameters for which a maximal $(n,5)$-resilient system cannot be linear since $k(n,6) < n - 2\log n$ (see [15], [5]).

Note that

$$R^{n,2}(6) = n^2 - n + 2, \tag{8.11}$$

$$L^{n,2}(\frac{n-\sqrt{n}}{2}) = n^2 + \frac{\sqrt{n-1}(n-2)}{2} \tag{8.12}$$

and hence $B^*(n+1,6) > n^2$, $B^*(n,6) > \frac{n^2}{2}$, $A^*(n, \frac{n-\sqrt{n}}{2}) < 2n^2$ by (6.18) and (6.29). Therefore, using Corollaries 3.2 and 4.3, (8.9), (8.10), and (7.1) we have

Corollary 8.6. *For any $h = 2, 3, \dots,$*

$$N(4h,5) = N(4h-1,4) + 1 = 2^{2h},$$

$$T(n,5) = T(n-1,4) = \log\frac{2^n}{n^2} \text{ and } T(n, \frac{n-\sqrt{n}}{2} - 1) = 2\log n, \text{ when } n = 2^{2h}.$$

Theorem 8.7. *If*

$$\tilde{l}_v(N,T+1) \le n - \tilde{l}_v(n,t+1), \tag{8.13}$$

then there exists a T-wise independent t-resilient system of N functions in n variables over F_v. Moreover, if

$$N \le k_v(n,t+1) + k_v(N,T+1), \tag{8.14}$$

then there exists a T-wise independent t-resilient system of N linear functions in n variables over F_v.

Proof. Let $k = n - \tilde{l}_v(n,t+1)$. Then by (2.8), (6.14), and (8.13) $\tilde{l}_v(n,t+1) \ge t$, $\tilde{l}_v(N,T+1) \ge T$, and hence $T \le k \le n-t$. Since $\tilde{l}_v(n,t+1) = n-k$, there exists a $(n-k)$-systematic $OA_{v^{n-k-t}}(t,n;v)$. By condition (8.13), $\tilde{l}_v(N,T+1) = k-i$ for some integer i $(0 \le i \le k-T)$. It follows that there exists an $OA_{v^{k-i-T}}(T,N;v)$ and, hence, an $OA_{v^{k-T}}(T,N;v)$ (as a union of v^i such designs). Due to Theorem 8.1, this proves the first part of the theorem. In the case of (8.14) we use (5.19) and Theorem 8.1 for $k = k_v(n,t+1)$. This choice implies the existence of a $(n-k)$-systematic linear $OA_{v^{n-k-t}}(t,n;v)$ and implies inequalities $T \le k \le n-t$ since $k_v(n,t+1) \le n-t$, $k_v(N,T+1) \le N-T$ by (2.8), (2.10), and (6.15). Moreover $k \ge N - k_v(N,T+1) = l_v(N,T+1)$ and hence there exists a k-systematic linear $OA_{v^{k-T}}(T,N;v)$. This completes the proof. ■

Now we aim to use Theorem 8.7 in order to demonstrate that all necessary conditions (7.6)-(7.10) are attained in some cases.

Corollary 8.8.

$$N(n,3,3) = \frac{2^{n-2}}{n} \quad \textit{when } n = 2^h,\ h = 3,\ldots, \tag{8.15}$$

$$N(n,3,\frac{n}{2}-1) = n \textit{ when } n = 2^h,\ h = 3,\ldots, \tag{8.16}$$

$$N(n,\frac{n}{2}-1,3) = n \textit{ when } n = 2^h,\ h = 2,\ldots, \tag{8.17}$$

$$N_q(n,t,2) = \frac{q^{n-t}-1}{q-1} \quad \textit{when } 0 \le t < n-1 \le q, \tag{8.18}$$

$$N_q(q+2,3,q-1) \ge q+2 \quad \textit{when } q = 2^h,\ h = 1,\ldots. \tag{8.19}$$

Proof. To prove the lower bounds in (8.15)-(8.19) it is sufficient to verify that inequalities (8.14) are valid for the corresponding N. This follows from (8.6)-(8.8) and the fact that $k_q(q+2,q) = 3$ and $k_q(q+2,4) = q-1$ (the Bose code and its dual). Taking into account (6.26) and the equality $L^{q+2,q}(q) = q^3$, one can see that (7.6)-(7.10) are attained in these cases and that they imply the upper bounds in (8.15)-(8.18). ■

Analogously, we can use the general condition (8.13) and relations (8.9), (8.11), (8.12) in order to obtain other maximal or asymptotically maximal independent resilient systems.

Corollary 8.9.

$$N(n,5,5) \geq \frac{\sqrt{2^n}}{n} \quad \text{when } n = 2^{2h},\ h = 2, \dots,$$

$$N(n,5,3) \geq \frac{2^{n-1}}{n^2} \quad \text{when } n = 2^{2h},\ h = 2, \dots,$$

$$N(n,3,5) = \sqrt{\frac{2^{n-1}}{n}} \quad \text{when } n = 2^{4h-1},\ h = 2, \dots,$$

$$N(n, \frac{n}{2} - 1, 5) = \sqrt{2n} \quad \text{when } n = 2^{4h-1},\ h = 2, \dots,$$

$$N(n, \frac{n-\sqrt{n}}{2} - 1, 5) \geq n \quad \text{when } n = 2^{2h},\ h = 2, \dots,$$

$$N(n, 5, \frac{n-\sqrt{n}}{2} - 1) = n \quad \text{when } n = 2^{2h},\ h = 2, \dots.$$

Moreover, $N(n,5,5) \lesssim \frac{\sqrt{2^n}}{n}$, $N(n,5,3) \lesssim \frac{2^{n-1}}{n^2}$, *and* $N(n, \frac{n-\sqrt{n}}{2} - 1, 5) \lesssim n$ *as* n *tends to infinity.*

The inequality $k(2^h, 2s+2) \geq 2^h - 1 - sh$, which follows from the existence of the extended primitive BCH codes, can be used twice in (8.14) to yield the following fact.

Corollary 8.10. *For arbitrary integers* a, b *and* $n = 2^h$ *such that* $2^h \geq 2b + ah + 2$, *and* b *divides* $2^h - 2 - ah$,

$$N(n, 2a+1, 2b+1) \geq \sqrt[b]{\frac{2^{n-2}}{n^a}}. \tag{8.20}$$

In the case $a = b = 1$, (8.20) coincides with (8.15), but in the case $a = b = 2$, it is worst by the factor of two than Corollary 8.9. However, we can see now that for a certain asymptotic, (8.20) has the correct order.

Theorem 8.11. *For fixed integers* a *and* b *and* $n \to \infty$,

$$c_1(a,b) \sqrt[b]{\frac{2^n}{n^a}} \lesssim N(n, 2a+1, 2b+1) \lesssim c_2(a,b) \sqrt[b]{\frac{2^n}{n^a}}, \tag{8.21}$$

where

$$c_1(a,b) = 2^{-\frac{a+b+2}{b}},\ c_2(a,b) = (4^{-1} a! b!)^{\frac{1}{b}}.$$

Proof. Shortening a primitive BCH code shows that $k(n+1, 2s+2) = k(n, 2s+1) \geq n - s\log 2n$ for any n and s, $n \geq 2s$. By (8.14), we have $2N(n, 2a+1, 2b+1) \geq \sqrt[b]{\frac{2^{n-2}}{(2n)^a}}$ and hence, the lower bound in (8.21) is valid. On the other hand, $R^{n,2}(2a+2) \sim 2\frac{n^a}{a!}$ for fixed a and $n \to \infty$, and due to (7.6), we have the upper bound in (8.21). ■

Note that for all n and d, the bound $A_v^*(n, d) \leq L^{n,v}(d)$ is in general better than the McEliece-Rodemich-Rumsey-Welch bound [28], but in the asymptotic process when $n \to \infty$ and $\frac{d}{n} \to \alpha$ $(0 < \alpha < \frac{v-1}{v})$, they logarithmically coincide. Taking into account that the Varshamov-Gilbert bound is also valid for systematic linear codes over $\mathbf{Z}_v$ and using the Hamming bound, inequalities (8.4), (7.3) and (7.4), we have

Theorem 8.12. *For fixed v, $n \to \infty$ and $\frac{d}{n} \to \alpha$ $(0 \leq \alpha < \frac{v-1}{v})$,*

$$T_v(n, d) \gtrsim n(1 - H_v(\alpha)),$$

$$T_v(n, d) \lesssim n \min(1 - H_v(\frac{\alpha}{2}), H_v(\gamma(\alpha))),$$

where

$$H_v(x) = -x\log_v x - (1-x)\log_v(1-x) + x\log_v(v-1)$$

and

$$\gamma(x) = \frac{1}{v}(v - 1 - x(v-2) - 2\sqrt{(v-1)x(1-x)}).$$

Similarly, from (8.14) and (7.6)-(7.8), one can get lower and upper asymptotic bounds on $N_v(n, t, T)$ when v is fixed, $\frac{t}{n} \to \alpha$ $(0 \leq \alpha < \frac{v-1}{v})$ and $\frac{T}{n} \to \beta$ $(0 < \beta \leq 1)$ as $n \to \infty$. Provided these conditions $N_v(n, t, T)$ grows linearly with n. In particular, let $x(\alpha, \beta)$ be the unique root of the equation $xH_v(\frac{\beta}{x}) = 1 - H_v(\alpha)$.

Theorem 8.13. *If v is fixed, $\frac{t}{n} \to \alpha$ $(0 \leq \alpha < \frac{v-1}{v})$ and $\frac{T}{n} \to \beta$ $(0 < \beta \leq 1)$ when $n \to \infty$, then*

$$N_v(n, t, T) \gtrsim \begin{cases} nx(\alpha, \beta) & \text{if } 0 < \beta \leq \frac{v-1}{v}(1 - H_v(\alpha)), \\ n(1 - H_v(\alpha)) & \text{if } \frac{v-1}{v}(1 - H_v(\alpha)) \leq \beta \leq 1. \end{cases}$$

In conclusion we discuss some connections of split orthogonal arrays with error-correcting codes. Denote a code C in F_v^{n+N} such that any two distinct rows differ in at least d places of their prefixes of length n or in at least D places of their suffixes of length N by a $(n, d; N, D; v)$-code. We call a $(n, d; N, D; v)$-code *systematic* if it consists of v^N rows whose suffixes of length N run over

F_v^N. Note that by Theorems 3.1 and 5.10 a T-wise independent t-resilient system of N linear functions in n variables over F_v exists if and only if there exists a linear systematic $(n, t+1; N, T+1; v)$-code. Analogously to the definition of $B_v(n, t+1; N, T+1)$ (see Section 2) it is possible to define $A_v(n, d; N, D)$ as the maximum size of a $(n, d; N, D; v)$-code. Let us introduce the notations $B_v^*(n, d; N, D) = \max \Omega(f)\Omega(g)$ and $A_v^*(n, d; N, D) = \min \Omega(f)\Omega(g)$, where the extrema are taken over all pairs of polynomials $f(z) = \sum_{i=0}^{n} f_i K_i^{n,v}(z)$ and $g(z) = \sum_{i=0}^{N} g_i K_i^{N,v}(z)$ satisfying the property $\mathcal{B}_{n,d,N,D}$: $f_0 > 0$, $f(0) > 0$, $g_0 > 0$, $g(0) > 0$, $f(i)g(j) \geq 0$ for $i = 1, \ldots, n$, $j = 1, \ldots, N$; $f_i g_j \leq 0$ if $i \geq d$ or $j \geq D$, and, respectively, the property $\mathcal{A}_{n,d,N,D}$: $f_0 > 0$, $f(0) > 0$, $g_0 > 0$, $g(0) > 0$, $f_i g_j \geq 0$ for $i = 1, \ldots, n$, $j = 1, \ldots, N$; $f(i)g(j) \leq 0$ if $i \geq d$ or $j \geq D$. An argument similar to Theorems 6.1 and 6.2 shows that $B_v(n, d; N, D) \geq B_v^*(n, d; N, D)$, $A_v(n, d; N, D) \leq A_v^*(n, d; N, D)$ and

$$B_v^*(n, d; N, D) A_v^*(n, d; N, D) = v^{n+N}. \tag{8.22}$$

Since Theorem 6.3 gives in effect a lower bound on $B_v^*(n, d; N, D)$, this implies a linear programming upper bound on $A_v(n, d; N, D)$. Using bounds of Section 6 one can obtain eight upper bounds on $A_v(n, d; N, D)$ all of which are attained for some parameters. On the other hand, $\log_v A_v(n, d; N, D) \geq k_v(n, d) + k_v(N, D)$ implies $\log_v B_v^*(n, d; N, D) \leq l_v(n, d) + l_v(N, D)$ by (8.22) and (5.19).

It is also interesting that for $v = 2$, $t = 2s$, and $T = 2m$, the sufficient conditions (8.14) for the existence of a T-wise independent t-resilient system of N linear functions in n variables over F_v coincide with those for the existence of a (superimposed) code for multiple access modulo-2 sum channel when N is the total number of users, m is the number of active users and there are at most s errors in n successive bits (see [13], Corollary 1).

9. Acknowledgements.

The author is grateful to P. Camion, J. L. Massey, V. M. Sidelnikov and D. R. Stinson for useful discussions of the setting of the problem and the results obtained. The author wishes also to thank anonymous reviewers for their constructive comments, which helped to greatly improve this article.

References

[1] N.Alon, O.Goldreich, J.Hastad, R.Peralta, Simple constructions of almost k-wise independent random variables, Random Structures and Algorithms, **3**, no. 3 (1992), 289-304.

[2] C.H.Bennett, G.Brassard and J.-M.Robert, Privacy amplification by public discussion. SIAM J.Comput., **17** (1988), 210-229.

[3] J.Bierbrauer, K.Gopalakrishnan and D.R.Stinson, Orthogonal arrays, resilient functions, error correcting codes and linear programming bounds. SIAM J.Discrete Math., **9** (1996), 424-452.

[4] A.E.Brouwer, T.Verhoeff, An updated table of minimum-distance bounds for binary linear codes. IEEE Trans. on Inform. Theory, **39** (1993), 662-677.

[5] A.E.Brouwer and L.M.G.M.Tolhuizen, A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters, Designs, Codes and Cryptography **3** (1993), 95-98.

[6] P.Camion, C.Carlet, P.Charpin and N.Sendrier, On correlation-immune functions. Lecture Notes in Computer Science **576** (1992), 86-100.

[7] B.Chor, O.Goldreich, J.Hastad, J.Friedman, S.Rudich and R.Smolensky. The bit extraction problem or t-resilient functions. Proc. 26th IEEE Symp. on Foundations of Computer Science (1985), 396-407.

[8] O.V.Denisov, Asymptotic formula for the number of correlation-ummune boolean functions of order k. Discrete Mathematics **2**, 3 (1991), 25-46 (in Russian).

[9] Ph.Delsarte. Bounds for unrestricted codes, by linear programming, Philips Res. Reports **27** (1972), 272-289.

[10] Ph.Delsarte, Four fundamental parameters of a code and their combinatorial significance, Info. and Control, **23** (1973), 407-438.

[11] Ph.Delsarte. An algebraic approach to the association schemes of coding theory, Philips Res. Reports Suppl. **10** (1973).

[12] C.F.Dunkl. Discrete quadrature and bounds on t-design, Mich.Math.J. **26** (1979), 81-102.

[13] T.Ericson and V.I.Levenshtein, Superimposed codes in the Hamming space. IEEE Trans. Inform. Theory **40** (1994), 1882-1893.

[14] J.Friedman. On the bit extraction problem. Proc. 33 IEEE Symp. on Foundations of Computer Science (1992), 314-319.

[15] J.-M.Goethals and S.L.Snover. Nearly perfect binary codes, Discrete Math. **3** (1972), 65-88.

[16] X.Guo-zhen and J.L.Massey. A spectral characterization of correlation-immune functions. IEEE Trans. Inform.Theory **34** (1988), 569-571.

[17] R.W.Hamming, Error detecting and error correcting codes, Bell Syst. Techn. J., **29** (1950), 147-160.

[18] A.M.Kerdock, A class of low rate non-linear codes, Inform. and Control **20** (1972),182-187.

[19] M.Krawtchouk, Sur une generalisation des polynomes d'Hermite, Comptes Rendus, **189** (1929), 620-622.

[20] V.I.Levenshtein, On choosing polynomials to obtain bounds in packing problems (in Russian), in Proc. Seventh All-Union Conf. on Coding Theory and Inform Transmission, Part II, Moscow-Vilnius, 1978, p.103-108.

[21] V.I.Levenshtein, Bounds for packings of metric spaces and some their applications (in Russian), Problemy Kiberneticki, Issue 40, Moscow, "Nauka" Publishing House, 1983, p.43-110.

[22] V.I.Levenshtein, Designs as maximum codes in polynomial metric spaces, Acta Applicandae Mathematicae, **29** (1992), 1-82.

[23] V.I.Levenshtein, Bounds for self-complementary codes and their applications, in CISM Courses and Lectures - Eurocode 92, 159-171. Springer Verlag, 1993.

[24] V.I.Levenshtein, Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, IEEE Trans. Inform. Theory **41** (1995), 1303-1321.

[25] J.H.Van Lint, Introduction to Coding Theory, volume **86** of Graduate texts in Mathematics. Springer-Verlag, 1982.

[26] U.M.Maurer and J.L.Massey, Local randomness in pseudorandom sequences, Journal of Cryptology **4** (1991), 135-149.

[27] F.J.MacWilliams and N.J.Sloane. The Theory of Error-correcting Codes, North-Holland, 1977.

[28] R.J.McEliece, E.R.Rodemich, H.Rumsey Jr., and L.R.Welch, New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, IEEE Trans.Inform. Theory **23** (1977), 157-166.

[29] V.Pless, Introduction to the theory of error-correcting codes, 2nd ed. New York: Wiley, 1989.

[30] F.P.Preparata, A class of optimum non-linear double-error-correcting codes, Inform. and Control **13** (1968), 378-400.

[31] C.R.Rao, Factorial experiments derivable from combinatorial arrangements of arrays, J.Royal Stat.Soc. **9** (1947), 128-139.

[32] I.Schoenberg and G.Szego, An extremum problem for polynomials, Composito Math. **14** (1960), 260-268.

[33] E.Seiden, R.Zemach, On orthogonal arrays, Ann. Math. Stat. **37** (1966), 1355-1370.

[34] V.M.Sidelnikov, On extremal polynomials used to estimate the size of codes (in Russian), Problemy Peredachi Informacii **16**, no. 3 (1980), 17-30. English translation in Problems of Information Transmission **16**, no. 3 (1980), 174-186.

[35] T.Siegenthaler, Correlation immunity of nonlinear combining function for cryptographic applications, IEEE Trans. Inform. Theory **30** (1984), 776-780.

[36] R.C.Singleton, Maximum distance q-ary codes, IEEE Trans. on Inform. Theory, **10** (1964), 116-118.

[37] D.R.Stinson, Resilient functions and large sets of orthogonal arrays, Congressus Numer. **92** (1993), 105-110.

[38] D.R.Stinson and J.L.Massey, An infinite class of counterexamples to a conjecture concerning non-linear resilient functions, J. of Cryptology, **8**, no. 3 (1995), 167-173.

[39] L.Teirlinck. Large sets of disjoint designs and structures. In Contemporary Design Theory - A Collection of Surveys, John Wiley & Sons, New York, 1992, 561-592.