EXISTENCE OF SMALL ORDERED ORTHOGONAL ARRAYS

KAI-UWE SCHMIDT AND CHARLENE WEISS

Abstract. We show that there exist ordered orthogonal arrays, whose sizes deviate from the Rao bound by a factor that is polynomial in the parameters of the ordered orthogonal array. The proof is nonconstructive and based on a probabilistic method due to Kuperberg, Lovett and Peled.

1. Introduction

A t-(q,n,λ) *orthogonal array* is an $M \times n$ array on q symbols such that every $M \times t$ subarray contains each t-tuple on q symbols exactly λ times as a row. The parameter t is called the *strength* of the orthogonal array. These combinatorial objects were introduced in the 1940s and now have various applications, for example in statistics, coding theory, cryptography, and software testing. We refer to [HSS99] for background on orthogonal arrays and their applications. The complete set of n-tuples on q symbols is a t-(q,n,λ) orthogonal array for every strength t. Therefore one is interested in the existence of orthogonal arrays with a fixed strength t having as few rows as possible.

Ordered orthogonal arrays generalise orthogonal arrays and were independently introduced by Lawrence [Law96] and Mullen and Schmid [MS96] in 1996. A t-(q,n,r,λ) *ordered orthogonal array* is an $M \times nr$ array on q symbols, where the nr columns are divided into n blocks containing r ordered columns such that for every n-tuple $(t_1,t_2,\dots,t_n)$ of integers summing up to t with $0 \le t_i \le r$, the rows of the $M \times t$ subarray consisting of the first t_1 columns of the first block, the first t_2 columns of the second block and so on, contain every t-tuple exactly λ times as a row. Note that $M = \lambda q^t$. We often say that M is the *size* of the array. An example for a 2-$(2,2,2,1)$ ordered orthogonal array is

$$\left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right).$$

Date: 02 September 2021.

Observe that this is not an orthogonal array of strength 2 since in the subarray consisting of the second and fourth column, the tuples 01 and 10 do not occur as rows.

Again, ordered orthogonal arrays have numerous applications, in particular in coding theory and cryptography. Most notably, ordered orthogonal arrays are closely related to (t, m, s)-nets, which are of great significance in numerical integration, in the sense that a (t, m, s)-net in base q exists if and only if an $(m-t)$-$(q, s, m-t, q^t)$ ordered orthogonal array exists [Law96], [MS96].

Similarly to orthogonal arrays, one is interested in having as few rows as possible. Apart from using (t, m, s)-nets, only a few constructions for ordered orthogonal arrays are known, see [RT97], [Skr01], [CMPS17], [PSSW19], for example. Let $N(q, n, t)$ be the minimum number M such that a t-(q, n, λ) orthogonal array of size M exists for some λ. Define $N(q, n, r, t)$ accordingly for ordered orthogonal arrays. Every t-(q, n, r, λ) ordered orthogonal array gives a t-(q, n, λ) orthogonal array by only choosing the first column in every block of the ordered orthogonal array. On the other hand, every t-(q, nr, λ) orthogonal array gives a t-(q, n, r, λ) ordered orthogonal array by dividing the nr columns into r blocks each of size n. Hence we have

$$N(q, n, t) \le N(q, n, r, t) \le N(q, nr, t). \tag{1}$$

Our main result is that, roughly speaking, the lower bound is more accurate than the upper bound. A famous lower bound for $N(q, n, t)$ is given by the Rao bound [Rao73], which implies

$$\left(\frac{cqn}{t}\right)^{t/2} \le N(q, n, t) \quad \text{and} \quad \left(\frac{cqnr}{t}\right)^{t/2} \le N(q, nr, t),$$

where $c > 0$ is a universal constant independent of all other parameters. (The Rao bound has been strengthened for ordered orthogonal arrays by Martin and Stinson [MS99b], [MS99a], but this improvement is not relevant here.) We now state our main result.

Theorem 1. *For all integers q, n, r, t satisfying $q \ge 2$ and $1 \le t \le nr$, there exists a t-(q, n, r, λ) ordered orthogonal array Y such that $|Y| \le \left(\frac{cqn}{t}\right)^{ct}$ for some universal constant $c > 0$ independent of all other parameters.*

We shall deduce Theorem 1 from a landmark result by Kuperberg, Lovett, and Peled [KLP17], which can be used to establish the existence of regular combinatorial structures. Their proof is based on probabilistic arguments and is therefore nonconstructive. The theorem was applied in [KLP17] to

show that nontrivial t-designs, orthogonal arrays of strength t, and t-wise permutations exist for all t. The so-called KLP theorem has been proved to be powerful in various other contexts. For example, Fazeli, Lovett, and Vardy [FLV14] used this result to prove the existence of nontrivial q-analogs of t-designs for all t.

In fact it follows from (1) and [KLP17] that

$$N(q,n,r,t) \leq \left(\frac{cqnr}{t}\right)^{ct}$$

for some universal constant $c > 0$. We shall strengthen this result in order to prove Theorem 1. To do so, we first recall the KLP theorem in the next section and then give a proof of Theorem 1 in Section 3.

2. The KLP theorem

In this section we recall the main theorem of [KLP17]. Let X be a finite set and let V be a $\mathbb{Q}$-linear subspace of functions $f\colon X \to \mathbb{Q}$. We are interested in subsets Y of X satisfying

$$\frac{1}{|Y|}\sum_{x\in Y} f(x) = \frac{1}{|X|}\sum_{x\in X} f(x) \quad \text{for all } f \in V. \tag{2}$$

An *integer basis* of V is a basis of V in which all elements are integer-valued functions. Let $\{\phi_a : a \in \mathcal{F}\}$ be an integer basis of V, where $\mathcal{F}$ is an index set. Then a subset Y of X satisfies (2) if and only if

$$\frac{1}{|Y|}\sum_{x\in Y} \phi_a(x) = \frac{1}{|X|}\sum_{x\in X} \phi_a(x) \quad \text{for all } a \in \mathcal{F}. \tag{3}$$

The KLP theorem guarantees the existence of small subsets Y of X with this property, once the vector space satisfies five conditions. These conditions are recalled first.

Conditions.

- (**C1**) **Constant Function.** All constant functions belong to V, which means that every such function can be written as a rational linear combination of the basis functions ϕ_a with $a \in \mathcal{F}$.
- (**C2**) **Symmetry.** A permutation $\pi\colon X \to X$ is called a *symmetry* of V if $\phi_a \circ \pi$ lies in V for all $a \in \mathcal{F}$. The set of symmetries of V forms a group called the *symmetry group* of V. The symmetry condition requires that the symmetry group acts transitively on X, which means that for all $x_1, x_2 \in X$, there exists a symmetry π such that $x_1 = \pi(x_2)$.

(C3) Divisibility. There exists a positive integer c_1 such that, for all $a \in \mathcal{F}$, there exists $n \in \mathbb{Z}^X$ satisfying

$$\frac{c_1}{|X|} \sum_{x \in X} \phi_a(x) = \sum_{x \in X} n_x \phi_a(x) \quad \text{for every } a \in \mathcal{F}.$$

The smallest positive integer c_1 for which this identity holds is called the *divisibility constant* of V.

(C4) Boundedness of V. The ℓ_∞-norm of a function $g\colon X \to \mathbb{Q}$ is given by

$$\|g\|_\infty = \max_{x \in X} |g(x)|.$$

The vector space V has to be bounded in the sense that there exists a positive integer c_2 such that V has a c_2-bounded integer basis in ℓ_∞.

(C5) Boundedness of $V^\perp$. The ℓ_1-norm of a function $g\colon X \to \mathbb{Q}$ is given by

$$\|g\|_1 = \sum_{x \in X} |g(x)|.$$

The orthogonal complement

$$V^\perp = \left\{ g\colon X \to \mathbb{Q} : \sum_{x \in X} f(x) g(x) = 0 \text{ for all } f \in V \right\}$$

of V has to be bounded in the sense that $V^\perp$ has a c_3-bounded integer basis in ℓ_1.

We can now state the KLP theorem.

KLP theorem ([KLP17, Theorem 2.4])**.** Let X be a finite set and let V be a $\mathbb{Q}$-linear subspace of functions $f\colon X \to \mathbb{Q}$ satisfying the conditions (C1)–(C5) with the corresponding constants c_1, c_2, c_3. Let N be an integral multiple of c_1 with

$$\min(N, |X| - N) \geq C\, c_2 c_3^2 (\dim V)^6 \log(2 c_3 \dim V)^6,$$

where $C > 0$ is a constant. Then there exists a subset Y of X of size $|Y| = N$ such that

$$\frac{1}{|Y|} \sum_{x \in Y} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x) \quad \text{for all } f \in V.$$

We close this section with recalling a useful criterion for the verification of (C5) from [KLP17]. An integer basis $\{\phi_a : a \in \mathcal{F}\}$ of V is *locally decodable* if there exist functions $\gamma_a\colon X \to \mathbb{Z}$ such that

$$\sum_{x \in X} \gamma_a(x) \phi_{a'}(x) = m \delta_{a,a'} \quad \text{for all } a, a' \in \mathcal{F} \tag{4}$$

for some $m \in \mathbb{Z}$, where $\delta_{a,a'}$ denotes the Kronecker δ-function. Note that $\{\gamma_a : a \in \mathcal{F}\}$ is necessarily an integer basis of V. If this basis is c_4-bounded in ℓ_1, then we say that $\{\phi_a : a \in \mathcal{F}\}$ is locally decodable *with bound* c_4.

Lemma 2 ([KLP17, Claim 3.2])**.** *Suppose that $\{\phi_a : a \in \mathcal{F}\}$ is a c_2-bounded integer basis in ℓ_∞ of V that is locally decodable with bound c_4. Then $V^\perp$ has a c_3-bounded integer basis in ℓ_1 with $c_3 = 2c_2c_4|\mathcal{F}|$.*

3. Proof of Theorem 1

In this section we prove Theorem 1 using the KLP theorem. Not surprisingly, our proof proceeds along similar lines as the proof given in [KLP17] for orthogonal arrays. We start by defining an ordered orthogonal array in the framework of the KLP theorem and specifying the underlying vector space V. We then show that V satisfies the conditions (C1)–(C5) with suitable constants, which establishes the existence of sufficiently small ordered orthogonal arrays.

Henceforth we denote by $[m]$ the set $\{1, 2, \ldots, m\}$. Next we define the set X, the index set $\mathcal{F}$, and the vector space V. Let q, n, r, t be integers satisfying $n, r \geq 1$, $q \geq 2$, and $1 \leq t \leq nr$. Let X be the set of all functions $[nr] \to [q]$. We partition $[nr]$ into n blocks of size r containing subsequent numbers and let $\mathcal{S}$ be the family of t-subsets of $[nr]$ containing t_i subsequent numbers from the i-th block, where $t_1, t_2, \ldots, t_r \in \{0, 1, \ldots, r\}$ are integers summing up to t. Let $\mathcal{F}$ be the set of functions $S \to [q]$ with $S \in \mathcal{S}$ and, for $a \in \mathcal{F}$ with $a \colon S \to [q]$, define $\phi_a \colon X \to \mathbb{Q}$ by

$$\phi_a(x) = \begin{cases} 1 & \text{if } a(i) = x(i) \text{ for all } i \in S, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, let V be the $\mathbb{Q}$-span of $\{\phi_a : a \in \mathcal{F}\}$. Now a subset Y of X is a t-(q, n, r, λ) ordered orthogonal array if and only if (3) holds. Note that

$$\frac{|Y|}{|X|} \sum_{x \in X} \phi_a(x) = \frac{|Y|}{q^t} = \lambda.$$

In what follows we shall show that V satisfies the conditions (C1)–(C5) with suitable constants and then deduce Theorem 1 from the KLP theorem.

(C1) Constant Function. For each $x \in X$, the sum

$$\sum_{a \in \mathcal{F}} \phi_a(x) = |\{a \in \mathcal{F} : a(i) = x(i) \text{ for all } i \in S\}| \tag{5}$$

is the cardinality of $\mathcal{S}$ since the image of a is fixed by the image of x. This implies

$$\frac{1}{|\mathcal{S}|}\sum_{a\in\mathcal{F}}\phi_a(x)=1$$

for each $x\in X$ and hence V contains the constant function.

(C2) Symmetry. For each $x\in X$, define the permutation $\pi_x\colon X\to X$ by

$$\pi_x(b)=x+b,$$

where $x+b$ is the mapping in X that satisfies $(x+b)(i)\equiv x(i)+b(i) \pmod q$ for all $i\in[nr]$. Then $\{\pi_x : x\in X\}$ is a group that acts transitively on X. We now show that this group is a subgroup of the symmetry group of V, which shows that the symmetry condition is satisfied. For each $b\in X$ and each $a\in\mathcal{F}$ with $a\colon S\to[q]$, we have

$$(\phi_a\circ\pi_x)(b)=\phi_a(x+b)=\phi_{a'}(b),$$

where $a'\in\mathcal{F}$ is the mapping $S\to[q]$ that satisfies $a'(i)\equiv a(i)-x(i) \pmod q$ for all $i\in S$. Therefore the function $\phi_a\circ\pi_x$ lies in V, as required.

(C4) Boundedness of V. The set $\{\phi_a : a\in\mathcal{F}\}$ spans V and consists of integer-valued functions that are 1-bounded in ℓ_∞. Hence there exists a c_2-bounded integer basis of V with $c_2=1$.

(C5) Boundedness of $V^\perp$. We shall show that V has a locally decodable integer basis with bound 2^t. Lemma 2 then implies that $V^\perp$ has a c_3-bounded integer basis in ℓ_1 for $c_3=2^{t+1}|\mathcal{F}|$.

Recall that $a\in\mathcal{F}$ is a function $S\to[q]$ for some t-set $S\in\mathcal{S}$. Instead of taking the whole set S as the domain of a, we now allow subsets of S. Moreover these subsets are now only mapped to $[q-1]$ instead of $[q]$. More formally, define

$$\mathcal{S}'=\bigcup_{S\in\mathcal{S}}\bigcup_{T\subseteq S}T\quad\text{and}\quad\mathcal{F}'=\{T\to[q-1]\colon T\in\mathcal{S}'\}.$$

Note that, for each $b\in\mathcal{F}'$, there exists $a\in\mathcal{F}$ that coincides with b if the domain of a is restricted to that of b.

First we will show that V is spanned by $\{\phi_b : b\in\mathcal{F}'\}$.

Lemma 3. *The set $\{\phi_b : b\in\mathcal{F}'\}$ spans V.*

Proof. We first show that every function ϕ_b with $b \in \mathcal{F}'$ lies in V. To do so, let $b \in \mathcal{F}'$ with $b\colon T \to [q-1]$ for some $T \in \mathcal{S}'$ and choose some $S \in \mathcal{S}$ such that $T \subseteq S$. Consider the set M of all mappings $a\colon S \to [q]$ that coincide with b when their domains are restricted to T. Then, for every $x \in X$ with $\phi_b(x) = 1$, there is exactly one element $a \in M$ with $\phi_a(x) = 1$. Moreover, if $\phi_b(x) = 0$, then $\phi_a(x) = 0$ for all $a \in M$. Hence we have

$$\phi_b = \sum_{a \in M} \phi_a,$$

which belongs to V, as required.

Now choose $T \in \mathcal{S}'$ and $a\colon T \to [q]$ and note that $a \in \mathcal{F}$ if $|T| = t$. We show that ϕ_a is in the span of $\{\phi_b : b \in \mathcal{F}'\}$. We proceed with an induction on the number c of elements in $[nr]$ mapped to q under a, with the base case being $c = 0$. Suppose now that c is nonzero. Then there exists $i_0 \in T$ with $a(i_0) = q$. For each $k \in [q-1]$, define $a^k\colon T \to [q]$ by

$$a^k(i) = \begin{cases} a(i) & \text{for } i \neq i_0 \\ k & \text{for } i = i_0 \end{cases}$$

and let a' be the mapping a restricted to $T \setminus \{i_0\}$. Then we have

$$\phi_a = \phi_{a'} - \sum_{k=1}^{q-1} \phi_{a^k}.$$

By the induction hypothesis, the right-hand side is in the span of $\{\phi_b : b \in \mathcal{F}'\}$, which completes the proof. □

For the boundedness of $V^\perp$, it remains to prove that $\{\phi_b : b \in \mathcal{F}'\}$ is locally decodable, from which we can also deduce that this set is linearly independent. For $x \in X$, let $\phi(x)$ be the element of $\mathbb{Z}^{\mathcal{F}'}$ with entries $\phi_b(x)$. We will also show that the lattice spanned by the vectors $\{\phi(x) : x \in X\}$ equals $\mathbb{Z}^{\mathcal{F}'}$. This property will be helpful later to determine the divisibility constant of V.

Lemma 4. *The set $\{\phi_b : b \in \mathcal{F}'\}$ is a locally decodable basis for V with bound 2^t. Moreover we have*

$$\mathbb{Z}^{\mathcal{F}'} = \left\{ \sum_{x \in X} n_x \phi(x) : n_x \in \mathbb{Z} \right\}. \tag{6}$$

Proof. For $a\colon R \to [q-1]$ and $b\colon T \to [q-1]$ in $\mathcal{F}'$ write $a \preceq b$ if $R \subseteq T$ and $a(i) = b(i)$ for all $i \in R$. This defines a partial order on $\mathcal{F}'$.

We extend each mapping $b\colon T \to [q-1]$ in $\mathcal{F}'$ to a mapping $x^b\colon [nr] \to [q]$ in X via

$$x^b(i) = \begin{cases} b(i) & \text{for } i \in T, \\ q & \text{otherwise.} \end{cases}$$

For $a, b \in \mathcal{F}'$, we then have $\phi_a(x^b) = 1_{a \preceq b}$, where 1_A is the indicator of an event A. For each $b\colon T \to [q-1]$ in $\mathcal{F}'$, we define $\gamma_b\colon X \to \mathbb{Z}$ by

$$\gamma_b(x) = \begin{cases} (-1)^{|T|-|S|} & \text{if } x = x^c \text{ for some } c\colon S \to [q-1] \text{ in } \mathcal{F}' \text{ with } c \preceq b, \\ 0 & \text{otherwise.} \end{cases}$$

Next we show that the mappings γ_b satisfy (4) with $m = 1$. Note that each $x \in X$ with $\gamma_b(x) \neq 0$ corresponds to exactly one $c \in \mathcal{F}'$ with $c \preceq b$. Hence, for all $a, b \in \mathcal{F}$, we have

$$\begin{aligned} \sum_{x \in X} \gamma_b(x)\phi_a(x) &= \sum_{c \preceq b} \gamma_b(x^c)\phi_a(x^c) \\ &= \sum_{c \preceq b} \gamma_b(x^c) 1_{a \preceq c} \\ &= 1_{a \preceq b} \sum_{a \preceq c \preceq b} \gamma_b(x^c). \end{aligned}$$

Let a, c, b have domains R, S, T. Then the summand in the latter sum equals $(-1)^{|T|-|S|}$ and the condition $a \preceq c \preceq b$ means that $R \subseteq S \subseteq T$ and the image of S under c is fixed by the image of S under b. Hence the mappings $c \in \mathcal{F}'$ satisfying $a \preceq c \preceq b$ are in one-to-one correspondence with sets S satifying $R \subseteq S \subseteq T$. There are exactly $\binom{|T|-|R|}{k}$ ways to choose such a subset S with $|T| - k$ elements and therefore we have

$$\begin{aligned} \sum_{x \in X} \gamma_b(x)\phi_a(x) &= 1_{a \preceq b} \sum_{k=0}^{|T|-|R|} (-1)^k \binom{|T| - |R|}{k} \\ &= 1_{a \preceq b} \cdot 1_{|T|=|R|} \\ &= \delta_{a,b}. \end{aligned} \tag{7}$$

This establishes (4) for $m = 1$. Let ϕ and γ be the $X \times \mathcal{F}'$ matrices with $\phi_{x,b} = \phi_b(x)$ and $\gamma_{x,b} = \gamma_b(x)$, respectively. Then (7) implies that $\gamma^T\phi$ is the identity matrix and therefore ϕ has full rank. Together with Lemma 3 it follows that $\{\phi_b : b \in \mathcal{F}'\}$ is a basis for V. Since (4) holds, this basis is locally decodable.

To obtain a bound for the local decodability, note that for each $b \in \mathcal{F}'$, we have

$$\|\gamma_b\|_1 = \sum_{x \in X} |\gamma_b(x)| = |\{x \in X : \, x = x^c \text{ for some } c \preceq b\}|.$$

If T is the domain of b, then this number is just the number of subsets of T, namely $2^{|T|}$. Since $|T| \leq t$, this shows that $\{\phi_b : b \in \mathcal{F}'\}$ is a locally decodable basis for V with bound 2^t.

To prove the second statement of the lemma, note that $\mathbb{Z}^{\mathcal{F}'}$ is equipped with the standard basis $\{e^b : b \in \mathcal{F}'\}$, where $e^b_a = \delta_{a,b}$ for all $a, b \in \mathcal{F}'$. From (7) we have

$$\sum_{x \in X} \gamma_b(x)\phi(x) = e^b,$$

which establishes the second statement of the lemma. □

Now note that V has a c_2-bounded integer basis in ℓ_∞ with $c_2 = 1$ and $|\mathcal{F}'| \leq |\mathcal{F}|$, which follows since V has a basis of size $\mathcal{F}'$ and a spanning set of size $\mathcal{F}$. Hence Lemmas 2 and 4 imply that $V^\perp$ has a c_3-bounded integer basis in ℓ_1 with $c_3 = 2^{t+1}|\mathcal{F}|$.

(C3) Divisibility. For every $b \colon T \to [q-1]$ in $\mathcal{F}'$, we have

$$\begin{aligned}\frac{1}{|X|} \sum_{x \in X} \phi_b(x) &= \frac{1}{|X|} \, |\{x \in X : x(i) = b(i) \text{ for all } i \in T\}| \\ &= \frac{q^{nr-|T|}}{|X|} = \frac{1}{q^{|T|}}.\end{aligned}$$

Since $|T| \leq t$, the number $q^t/|X| \sum_{x \in X} \phi_b(x)$ is an integer. From (6) we conclude that V satisfies the divisibility condition and that the divisibility constant of V is $c_1 = q^t$.

Proof of Theorem 1. We have verified the conditions of the KLP theorem with the parameters

$$c_1 = q^t, \quad c_2 = 1, \quad c_3 = 2^{t+1}|\mathcal{F}|.$$

Moreover we have $\dim(V) \leq |\mathcal{F}|$ and $|\mathcal{F}| = q^t|\mathcal{S}|$, where

$$|\mathcal{S}| = |\{(t_1, \ldots, t_n) : t_i \in \{0, 1, \ldots, r\}, \sum_{i=1}^{n} t_i = t\}|.$$

This is the number of r-restricted partitions of t with at most n parts, which is upper bounded by the number non-restricted partitions of t with at most n

parts. It is well known and readily verified that this number equals $\binom{n-t+1}{t}$ and hence, by using the standard bound $\binom{m}{k} \le \left(\frac{em}{k}\right)^k$, we obtain

$$|\mathcal{S}| \le \binom{n-t+1}{t} \le \left(\frac{e(n-t+1)}{t}\right)^t \le \left(\frac{en}{t}\right)^t.$$

The KLP theorem now implies the existence of an ordered orthogonal array Y of strength t satisfying $|Y| \le \left(\frac{cqn}{t}\right)^t$ for some universal constant $c > 0$. This proves Theorem 1. □

References

[CMPS17] A. G. Castoldi, L. Moura, D. Panario, and B. Stevens, *Ordered orthogonal array construction using LFSR sequences*, IEEE Trans. Inform. Theory **63** (2017), no. 2, 1336–1347.

[FLV14] A. Fazeli, S. Lovett, and A. Vardy, *Nontrivial t-designs over finite fields exist for all t*, J. Combin. Theory Ser. A **127** (2014), 149–160.

[HSS99] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal arrays*, Springer Series in Statistics, Springer-Verlag, New York, 1999.

[KLP17] G. Kuperberg, S. Lovett, and R. Peled, *Probabilistic existence of regular combinatorial structures*, Geom. Funct. Anal. **27** (2017), no. 4, 919–972.

[Law96] K. M. Lawrence, *A combinatorial characterization of (t, m, s)-nets in base b*, J. Combin. Des. **4** (1996), no. 4, 275–293.

[MS96] G. L. Mullen and W. Ch. Schmid, *An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes*, J. Combin. Theory Ser. A **76** (1996), no. 1, 164–174.

[MS99a] W. J. Martin and D. R. Stinson, *Association schemes for ordered orthogonal arrays and (T, M, S)-nets*, Canad. J. Math. **51** (1999), no. 2, 326–346.

[MS99b] ———, *A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets*, Canad. Math. Bull. **42** (1999), no. 3, 359–370.

[PSSW19] D. Panario, M. Saaltink, B. Stevens, and D. Wevrick, *A general construction of ordered orthogonal arrays using LFSRs*, IEEE Trans. Inform. Theory **65** (2019), no. 7, 4316–4326.

[Rao73] C. R. Rao, *Some combinatorial problems of arrays and applications to design of experiments*, A Survey of Combinatorial Theory (J. N. Srivastava, ed.), North-Holland, 1973, pp. 349–359.

[RT97] M. Y. Rosenbloom and M. A. Tsfasman, *Codes for the m-metric*, Problems Inform. Transmission **33** (1997), no. 1, 45–52.

[Skr01] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz **13** (2001), no. 2, 191–239.

Department of Mathematics, Paderborn University, Warburger Str. 100, 33098 Paderborn, Germany.

Email address, K.-U. Schmidt: kus@math.upb.de

Email address, C. Weiß: chweiss@math.upb.de