Construction of orthogonal arrays

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
HOUGHTON (MI) 49931 (USA)

December 6, 1994

Abstract

For every prime-power q and $n \geq m$ we construct orthogonal arrays

$$OA_{q^{(t-1)(n-m)}}(t, q^n + \lfloor n/m \rfloor, q^m) \ (2 \leq t \leq q^n).$$

If $q^m < t \leq q^n$, we also get

$$OA_{q^{(t-1)(n-m)-n}}(t, q^n, q^m).$$

Finally we construct families of large sets of orthogonal arrays and of $t-$resilient functions.

1 Introduction

An *orthogonal array* with parameters $OA_\lambda(t, k, v)$ is defined as a multiset Σ of mappings from a k-set C into a v-set E such that for every choice of t distinct elements $x_1, x_2, \ldots x_t$ in C and t not necessarily distinct elements $y_1, y_2, \ldots y_t$ in E there are exactly λ elements $f \in \Sigma$ affording the operation $f(x_i) = y_i, i = 1, 2, \ldots t$. We may describe Σ as a uniformly t-transitive multiset of mappings from a k-set into a v-set. Σ may be visualized as an array with set C of columns and set E of entries, where each mapping $f \in \Sigma$

contributes a row. It is generally recognized that case $t = 2$ is much easier to handle than the general case. In section 2 we present a general direct construction of orthogonal arrays for arbitrary t when $v = q$ is a prime-power. This construction is a common generalization of the extended Reed-Solomon codes and of a well-known construction in case $t = 2$ ([1],p.363). The proof for this special case as given by Beth-Jungnickel-Lenz is rather involved. D.R.Stinson recently found a much simpler proof ([6],Theorem 5.2). This enabled us to generalize the construction to arbitrary t.
In section 3 we study the simplicity of the arrays with parameters

$$OA_{q^{(t-1)(n-m)}}(t, q^n, q^m)\ (n \geq m)$$

constructed in section 2. Observe that a family with these parameters was first constructed by Mukhopadhyay in 1981 (see [4]). An array is *simple* if each row occurs only once. We show that the arrays above are simple if and only if $t \leq q^m$. Each row occurs with the same multiplicity q^ρ. This permits the construction of simple arrays with a smaller value of λ :

$$OA_{q^{(t-1)(n-m)-\rho}}(t, q^n, q^m).$$

We prove lower bounds on ρ.
In the final section 4 we show that the simple orthogonal arrays constructed in the preceding section can be embedded into large sets of orthogonal arrays. This permits the construction of a family of resilient functions.

2 A direct construction

Theorem 1 *Let q be a prime-power, m, n, t natural numbers,$n \geq m, 2 \leq t \leq q^n$. Then there is an*

$$OA_{q^{(t-1)(n-m)}}(t, q^n, q^m).$$

Proof: Fix a surjective $\mathbb{F}_q-$linear mapping $\phi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$. For every t-tuple $(z, a_1, a_2, \ldots, a_{t-1})$, where $z \in \mathbb{F}_q^m, a_j \in \mathbb{F}_q^n, j = 1, 2, \ldots t-1$ we define a mapping $f = f(z, a_1, a_2, \ldots, a_{t-1}) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ by

$$f(x) = \phi(\sum_{j=1}^{t-1} a_j x^j) + z.$$

We claim that the set Σ of all these mappings is an orthogonal array with the given parameters. Let different elements $x_1, x_2, \dots x_t \in \mathbb{F}_q^n$ and (not necessarily different) elements $\alpha_1, \alpha_2, \dots \alpha_t \in \mathbb{F}_q^m$ be given. Put $p(X) = \sum_{i=1}^{t-1} a_i X^i$. We have to count the pairs $(p(X), z)$, where $p(X)$ is a polynomial over $\mathbb{F}_q^n$ without constant term, of degree $< t$, and $z \in \mathbb{F}_q^m$ satisfying

$$\phi(p(x_j)) + z = \alpha_j, j = 1, 2, \dots t.$$

By subtraction and making use of the linearity of ϕ we get the equivalent conditions

$$\phi(p(x_1) - p(x_j)) = \alpha_1 - \alpha_j, j = 2, 3, \dots t.$$

Here we count the polynomials p. If the conditions are met, then z is uniquely determined. Put $U_j = \phi^{-1}(\alpha_1 - \alpha_j), j = 2, 3, \dots, t$. Because of the surjectivity of ϕ we have $|U_j| = q^{n-m}$. Let now a $(t-1)$-tuple $(u_2, \dots, u_t)$ be given, where $u_j \in U_j$. The number of such tuples is exactly $q^{(t-1)(n-m)}$. We will therefore be done if we can show that there is exactly one polynomial $p(X) \in \mathbb{F}_q^n[X]$ of degree $< t$, without constant term, and satisfying

$$p(x_1) - p(x_j) = u_j (j = 2, 3, \dots t.)$$

This is fairly obvious. In fact, if we omit the condition $p(0) = 0$ and fix instead a value for $p(x_1)$, then p is uniquely determined by *Lagrange interpolation.* Changing the constant term affects only the value of $p(x_1)$, whereas the remaining conditions (on differences) are still met. We want the constant term to be 0. This shows the unicity of the polynomial $p(X)$ and finishes the proof. ■

A family of OA with these parameters was first constructed by Mukhopadhyay ([4]), using different methods. It is an interesting question how many columns can be added to the orthogonal arrays of the preceding theorem. We show that the number of columns can always be increased by $\lfloor n/m \rfloor$:

Corollary 1 *With the notation of the preceding Theorem, there is always an*

$$OA_{q^{(t-1)(n-m)}}(t, q^n + \lfloor n/m \rfloor, q^m).$$

Proof: We use the notation of the foregoing theorem. Let $\chi_1, \dots, \chi_{\lfloor n/m \rfloor}$ be a family of $\mathbb{F}_q$−linear functions $\chi_i : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^m}$ whose kernels intersect in a space of dimension $n-m\cdot\lfloor n/m\rfloor$. Let the additional columns be indexed by the χ_i and define the value of $f=f(z,a_1,a_2,\dots,a_{t-1})$ in column χ_i by

$$f(\chi_i)=\chi_i(a_{t-1}).$$

Consider columns corresponding to $x_1,x_2,\dots,x_k\in\mathbb{F}_{q^n},\chi_1,\dots\chi_l$, where $k+l=t$ and entries $\alpha_1,\dots,\alpha_k,\beta_1\dots\beta_l\in\mathbb{F}_{q^m}$. Let $\mathcal{P}$ be the set of polynomials $p(X)$ over $\mathbb{F}_q^n$ without constant term, of degree $<t$, satisfying

$$\phi(p(x_1)-p(x_j))=\alpha_1-\alpha_j, j=2,3,\dots k.$$

We have to count the polynomials $p(X)\in\mathcal{P}$ whose coefficient a_{t-1} satisfies in addition

$$\chi_j(a_{t-1})=\beta_j, j=1,\dots,l.$$

If $l=0$, then we are done by the preceding Theorem. So assume $l>0$, equivalently $k<t$. As before let $U_j=\phi^{-1}(\alpha_1-\alpha_j), j=2,3,\dots,k$, pick a tuple $(u_2,\dots,u_k)$, where $u_j\in U_j$. Denote by $\mathcal{Q}$ the set of polynomials in $\mathcal{P}$ satisfying $p(x_1)-p(x_j)=u_j, j=2,\dots,k$. By Lagrange interpolation polynomial $p(X)\in\mathcal{Q}$ is uniquely determined if it has degree $\leq t-1-l$. It follows that each polynomial $p(X)\in\mathcal{Q}$ is uniquely determined by its l highest coefficients. In particular, when $p(X)$ runs through $\mathcal{Q}$ its highest coefficient a_{t-1} will attain each value the same number of times. It follows that the tuple $(\chi_1(a_{t-1}),\dots\chi_l(a_{t-1}))$ will attain each value in $\mathbb{F}_{q^m}^l$ the same number of times. This completes the proof.$\blacksquare$

Case $n=m$ leads to the extended Reed-Solomon codes.

3 Improvements

3.1 Generalities

Let $\Sigma=\Sigma(q,n,m,t,\phi)$ be the orthogonal array with parameters

$$OA_{q^{(t-1)(n-m)}}(t,q^n,q^m)$$

as constructed in Theorem 1. We adopt the notation of the previous section. Recall that $n\geq m, 2\leq t\leq q^n$ and that ϕ is a surjective $\mathbb{F}_q-$linear mapping

$\phi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$.
We raise the question when Σ is simple. So let $(p_1(X), z_1)$ and $(p_2(X), z_2)$ be identical rows of Σ, where $z_i \in \mathbb{F}_q^m$ and

$$p_i(X) \in \mathcal{P} = \{p(X) | p(X) \in \mathbb{F}_q^n[X], p(0) = 0, deg(p(X)) < t\}.$$

The corresponding rows of Σ are the same if and only if the following holds:

$$\phi(p_1(u)) + z_1 = \phi(p_2(u)) + z_2 \text{ for all } u \in \mathbb{F}_q^n.$$

Putting $u = 0$ we see $z_1 = z_2$. The condition on the polynomials is

$$\phi((p_1 - p_2)(u)) = 0 \text{ for all } u \in \mathbb{F}_q^n.$$

Define $\mathcal{P}_0 = \mathcal{P}_0(q, n, m, t, \phi)$ as the set of polynomials $p(X) \in \mathcal{P}$ satisfying

$$\phi(p(u)) = 0 \text{ for all } u \in \mathbb{F}_q^n.$$

Clearly $\mathcal{P}_0$ is an $\mathbb{F}_q-$vector space. Denote its dimension by ρ. We have seen the following:

Proposition 1 *Let $\Sigma = \Sigma(q, n, m, t, \phi), \mathcal{P}, \mathcal{P}_0$ as above. Two rows $(p_1(X), z_1)$ and $(p_2(X), z_2)$ of Σ are the same if and only if*

$$z_1 = z_2$$

$$p_1(X) - p_2(X) \in \mathcal{P}_0.$$

In particular every row of Σ occurs with the same multiplicity q^ρ.

Corollary 2 *Let $\Sigma, \mathcal{P}, \mathcal{P}_0$ be as in the preceding Proposition. Define the* simplification *$\Sigma_0 = \Sigma_0(q, n, m, t, \phi)$, where each row of Σ is written only once (instead of q^ρ times). Then Σ_0 is a simple orthogonal array with parameters*

$$OA_{q^{(t-1)(n-m)-\rho}}(t, q^n, q^m).$$

Lemma 1 *If $t \leq q^m$, then $\rho = dim(\mathcal{P}_0) = 0$.*

Proof: Let $p(X)$ be a nonzero (hence nonconstant) polynomial in $\mathcal{P}_0$. As $p(u) \in \phi^{-1}(0)$ for every $u \in \mathbb{F}_q^n$ and as $p(X)$ takes on each fixed value at most $t - 1$ times, it follows $(t - 1)q^{n-m} \geq q^n$, hence $t > q^m$. ■

We show next that $\rho > 0$ really occurs, so that we obtain improvements upon the value of λ as given in section 2.

3.2 The case of linear codes.

Let $m = 1, tr : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ the *trace* and assume $t > q^i$ for some $i \geq 1$. Consider polynomials of the form

$$p(X) = (a_i X)^{q^i} + \ldots + (a_1 X)^q + a_0 X,$$

certainly contained in $\mathcal{P}$. Here $a_j \in \mathbb{F}_q^n$. When is $p(X) \in \mathcal{P}_0(q, n, 1, t, tr)$? The condition is

$$0 = tr((a_i u)^{q^i} + \ldots + (a_1 u)^q + a_0 u) = tr(a_i u + \ldots + a_1 u + a_0 u) =$$

$$= tr((a_i + \ldots + a_1 + a_0) \cdot u) \text{ for all } u \in \mathbb{F}_q^n.$$

Equivalently: $a_i + \ldots + a_1 + a_0 = 0$. We conclude:

Theorem 2 *If $m = 1, \phi = tr : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q, t > q^i$, then $\mathcal{P}_0$ contains the $\mathbb{F}_q^n$-polynomials*

$$(a_i X)^{q^i} + \ldots + (a_1 X)^q + a_0 X, \text{ where } \sum_j a_j = 0.$$

Hence $\rho = dim(\mathcal{P}_0) \geq i \cdot n$.

Corollary 3 *If $t > q^i$, there is an*

$$OA_{q^{(t-1)(n-1)-in}}(t, q^n, q).$$

Consider the case $t = q + 1$. It is clear that we have equality in the Theorem above:

Corollary 4 *If $m = 1, \phi = tr : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q, t = q + 1$, then*

$$\mathcal{P}_0 = \{(aX)^q - aX | a \in \mathbb{F}_q^n\},$$

hence $\rho = dim(\mathcal{P}_0) = n$. The simplification Σ_0 of $\Sigma(q, n, 1, q + 1, tr)$ is a simple orthogonal array with parameters

$$OA_{q^{(q-1)(n-1)-1}}(q + 1, q^n, q).$$

We cannot hope to find essentially new orthogonal arrays in this subsection. In fact our orthogonal arrays are linear codes and the connection between linear codes and orthogonal arrays is well known. By construction our codes are essentially trace-codes of Reed-Solomon codes. Consider the binary case of the above Corollary. The parameters are

$$OA_{2^{n-2}}(3, 2^n, 2).$$

This is interesting as the Rao bound for orthogonal arrays is met with equality (see [5]). It is in fact easy to see that we have rediscovered the binary first-order Reed-Muller codes.

3.3 Bounds on ρ in the general case

Let $\Sigma = \Sigma(q, n, m, t, \phi), \mathcal{P}, \mathcal{P}_0$ and $\rho = \rho(q, n, m, t, \phi)$ as defined in the beginning of the present chapter. We want to obtain lower bounds on ρ. In the sequel all dimensions are dimensions of $\mathbb{F}_q-$vector spaces.

Definition 1 *Let $U \subseteq \mathbb{F}_{q^n}$. Define the polynomial*

$$p_U(X) = \prod_{u \in U} (x - u).$$

Lemma 2 *Let $U \subset \mathbb{F}_{q^n}$ be an r-dimensional $\mathbb{F}_q-$subspace. Then the following hold:*

- *The polynomial $p_U(X)$ has the form*

$$p_U(X) = \sum_{j=0}^{r} a_j X^{q^j}, \quad \textit{where } a_j \in \mathbb{F}_{q^n}.$$

- *The mapping $z \mapsto p_U(z), z \in \mathbb{F}_{q^n}$ is $\mathbb{F}_q-$linear with image of dimension $n - r$.*

Proof: Clearly the second statement is a consequence of the first one. We prove the first statement by induction over r. For $r = 0$ there are no problems. We shall make repeated use of the obvious identity

$$X^{q-1} - Y^{q-1} = \prod_{\lambda \in F_q^*} (X - \lambda Y)$$

between polynomials in two indeterminates over $I\!F_q$.
If $U =< \beta >$ is 1-dimensional, then

$$p_U(X) = X \cdot \prod_{\lambda \in F_q^*} (X - \lambda\beta) = X(X^{q-1} - \beta^{q-1}) = X^q - \beta^{q-1} \cdot X.$$

The claim is proved in this case. Assume the claim is proved for some $p_U(X)$, where $dim(U) = r < n$. Let $\beta \in I\!F_{q^n} - U$. Because of the second statement of our Lemma, when applied to U, we have

$$p_{U+\beta}(X) = p_U(X - \beta) = p_U(X) - p_U(\beta).$$

It follows

$$p_{<U,\beta>}(X) = p_U(X) \cdot \prod_{\lambda \in F_q^*} (p_U(X) - \lambda p_U(\beta)) = p_U(X) \cdot (p_U(X)^{q-1} - p_U(\beta)^{q-1}) =$$

$$= p_U(X)^q - p_U(\beta)^{q-1} p_U(X).$$

The claim follows. ∎

Lemma 3 *Let* $0 \leq r \leq n, 0 \neq p(X) = \sum_{j=0}^{r} a_j X^{q^j}$, *where* $a_j \in I\!F_{q^n}$. *Then* $p(I\!F_{q^n})$ *is an* $I\!F_q-$*subspace of dimension* $\geq n - r$.

Proof: It is obvious that the mapping $z \mapsto p(z)$ is $I\!F_q-$linear. We have to prove that the kernel of this mapping has dimension $\leq r$. This is clear as $p(X)$ has degree $\leq q^r$. ∎

Proposition 2 *The mapping*

$$U \longrightarrow p_U(I\!F_{q^n})$$

induces a bijection between the $r-$*dimensional and the* $(n-r)-$*dimensional* $I\!F_q-$*subspaces of* $I\!F_{q^n}$, *for every* $r = 0, 1, \ldots, n$.

Proof: Let U_1, U_2 be different $r-$dimensional subspaces such that

$$p_{U_1}(I\!F_{q^n}) = p_{U_2}(I\!F_{q^n}) = V.$$

We know that V is an $(n-r)-$ dimensional subspace. Then

$$f(X) = p_{U_1}(X) - p_{U_2}(X) = \sum_{j=0}^{r-1} z_j X^{q^j}.$$

By the preceding Lemma $dim(f(\mathbb{F}_{q^n})) \geq n-r+1$. However $f(\mathbb{F}_{q^n}) \subseteq V$ by the assumption, contradiction. ∎

It should be noted that the mapping $U \longrightarrow p_U(\mathbb{F}_{q^n})$ does not induce a polarity of the $(n-1)-$dimensional projective space over $\mathbb{F}_q$. This means that for subspaces $U_1 \subset U_2$ the inclusion $p_{U_1}(\mathbb{F}_{q^n}) \supset p_{U_1}(\mathbb{F}_{q^n})$ does not in general hold.

The preceding Proposition suffices to derive interesting lower bounds on $\rho(q,n,m,t,\phi)$.

In particular we see that $\rho > 0$ whenever the conditions of Lemma 1 are not met:

Theorem 3 *The orthogonal array $\Sigma(q,n,m,t,\phi)$ is simple (equivalently $\rho(q,n,m,t,\phi) = 0$) if and only if $t \leq q^m$.*

We shall see shortly that $\rho \geq n$ whenever $\rho > 0$.

Consider the smallest nontrivial case $t = q^m+1$, let $V = \phi^{-1}(0)$. We have seen that there is exactly one $m-$dimensional space U such that $p_U(\mathbb{F}_{q^n}) = V$. Let $0 \neq \alpha \in \mathbb{F}_{q^n}$, choose U_α such that $p_{U_\alpha}(\mathbb{F}_{q^n}) = \alpha^{-1} \cdot V$. Then $\alpha \cdot p_{U_\alpha}(\mathbb{F}_{q^n}) = V$, hence $\alpha \cdot p_{U_\alpha}(X) \in \mathcal{P}_0$. It follows $\rho \geq n$. We claim that equality holds. In fact, let $0 \neq p(X) \in \mathcal{P}_0(q,n,m,q^m+1,\phi)$. As $\rho(q,n,m,q^m,\phi) = 0$, the polynomial $p(X)$ has degree q^m. Let $p(X) = \alpha \cdot X^{q^m} + \ldots$. Then $p(X) - \alpha \cdot p_{U_\alpha}(X) \in \mathcal{P}_0$ and has smaller degree, hence $p(X) = \alpha \cdot p_{U_\alpha}(X)$. We have seen the following:

Theorem 4 *Let $m < n$. Then*

$$\rho(q,n,m,q^m+1,\phi) = n.$$

Thus the simplification of $\Sigma(q,n,m,q^m+1,\phi)$ is a (simple)

$$OA_{q^{q^{m(n-m)-n}}}(q^m+1, q^n, q^m).$$

Small nontrivial cases are $q = 2, n = 3, m = 2$ and $q = 3, n = 3, m = 2$. This yields simple

$$OA_2(5, 8, 4)$$

$$OA_{3^6}(10, 27, 9).$$

For larger t our results are less tight. Let $t = q^{m+1} + 1$, where $n \geq m + 2$, put $V = \phi^{-1}(0)$. Apply the same method as in the proof of Theorem 4. We get $q^n - 1$ polynomials $p(X) \in \mathcal{P}_0$ of degree q^m satisfying $p(\mathbb{F}_{q^n}) = V$. Moreover, for each of the $(q^{n-m} - 1)/(q - 1)$ subspaces W of codimension 1 in V, we get $q^n - 1$ polynomials $p(X) \in \mathcal{P}_0$ of degree q^{m+1} with $p(\mathbb{F}_{q^n}) = W$. We have $1 + (q^n - 1)(q^{n-m-1} + \ldots + q + 2)$ different polynomials $p(X) \in \mathcal{P}_0$. This number is easily seen to be $> q^{2n-m-1}$. It follows $\rho \geq 2n - m$.

Theorem 5 *Let $n \geq m + 2, t > q^{m+1}$. Then*

$$\rho(q, n, m, t, \phi) \geq 2n - m.$$

In order to get better bounds one should study the linear dependence between the polynomials $\alpha \cdot p_U(X) \in \mathcal{P}_0$.
As an example, consider the case $q = 2, n = 5, m = 3, t = 17$. We have $\rho \geq 7$. This yields an

$$OA_{2^{25}}(17, 32, 8).$$

4 Resilient functions

Definition 2 *Let $\mathcal{A}$ be an alphabet of v letters, $k > t$. A function f from $\mathcal{A}^k$ into an r-set W is t-*resilient *(and q-*ary*) if for every t-subset $\{i_1, i_2, \ldots, i_t\} \subset \{1, \ldots, k\}$, for every choice $z_j \in \mathcal{A}, j = 1, 2, \ldots, t$ and for each $w \in W$, the probability of the occurence of the output value $w \in W$ satisfies*

$$Pr(f(x_1, x_2, \ldots, x_k) = w \mid x_{i_j} = z_j, j = 1, \ldots t) = 1/r.$$

This is a slight generalization of the usual concept of a t-resilient function in that we remove the somewhat artificial assumptions that $v = q$ be a prime-power and that r be a power of q. More on resilient functions and their applications in cryptography can be found in [7]. D.R.Stinson proved the fundamental fact that t-resilient functions are equivalent to large sets of orthogonal arrays of strength t :

Definition 3 *A* large set *of $OA_\lambda(t,k,v)$ is a partition of the set $\mathcal{A}^k$ of all k-tuples with entries in a $v-$element alphabet $\mathcal{A}$ into orthogonal arrays $OA_\lambda(t,k,v)$.*

Clearly each element of a large set of $OA_\lambda(t,k,v)$ must be a *simple* $OA_\lambda(t,k,v)$.

Theorem 6 (Stinson) *Let $\mathcal{A}$ be a $v-$element alphabet, $t<k$. Then the following are equivalent:*

- *A t-resilient function from $\mathcal{A}^k$ into a $v^{k-t}/\lambda-$element set.*
- *A large set of $OA_\lambda(t,k,v)$.*

The proof is identical with the proof of [7],Theorem 2.1. For the following observation the author is indebted to D.R.Stinson.

Lemma 4 (Stinson) *Let q be a prime-power and Σ a simple $OA_\lambda(t,k,q^m)$, which is an $\mathbb{F}_q-$vector space. This means that we endow the image set with the structure of an $\mathbb{F}_q-$vector space and we assume that sums and scalar multiples of rows of Σ are rows of Σ again.*
Then Σ can be embedded into a large set of $OA_\lambda(t,k,q^m)$.

Proof: The set of all functions from a k-set into a q^m-set forms an $\mathbb{F}_q-$vector space V. We assume that Σ is a subspace. Hence V is the disjoint union of cosets of Σ. Each coset is an $OA_\lambda(t,k,q^m)$. ■

By construction the arrays $\Sigma_0(q,n,m,t,\phi)$ as constructed in Corollary 2 satisfy the conditions of the preceding Lemma.

Corollary 5 *Let q be a prime-power,$n\geq m, t<q^n, \phi$ an $\mathbb{F}_q-$linear surjective mapping : $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m, \rho=\rho(q,n,m,t,\phi)$.*
Then there is a large set of $OA_{q^{(t-1)(n-m)-\rho}}(t,q^n,q^m)$, equivalently a $t-$resilient q^m-ary function f from a $q^{mq^n}-$set to a $q^{mq^n-(t-1)n-m+\rho}-$set.

References

[1] T.Beth,D.Jungnickel,H.Lenz: *Design Theory,* Bibliographisches Institut, Zürich 1985.

[2] J.Bierbrauer: *Universal hashing and geometric codes,* to appear in *Designs, Codes and Cryptography.*

[3] J.Bierbrauer,Y.Edel: *Theory of perpendicular arrays,* to appear in *Journal of Combinatorial Designs.*

[4] A.C.Mukhopadhyay: *Construction of some series of orthogonal arrays,* Sankhya B 43(1981),81-92.

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

[6] D.R.Stinson: *Universal Hashing and Authentication Codes,* to appear in *IEEE Transactions on Information Theory.*

[7] D.R.Stinson: *Resilient functions and large sets of orthogonal arrays,* University of Nebraska, Computer Science and Engineering Department, Report Series:UNL-CSE-93-005 (1993).