A Gröbner Bases Method for Complementary Sequences

Christos Koukouvinos
National Technical University of Athens, Greece
Dimitris E. Simos*
SBA Research, 1040 Vienna, Austria
Zafeirakis Zafeirakopoulos†
RISC - Research Institute for Symbolic Computation, Linz, Austria
zafeirakopoulos@risc.jku.at

Abstract

We employ tools from the field of symbolic computation for the construction of new classes of combinatorial designs, in particular complementary sequences and orthogonal designs. Combinatorial designs are used in a variety of applications ranging from statistics to coding theory and from telecommunications to software testing.

Keywords
Complementary Sequences, Orthogonal Designs, Gröbner Bases, Algebraic Modeling

1 Introduction

Orthogonal designs (ODs) are square matrices with entries in the field of quotients of the integral domain $\mathbb{Z}[a_1, a_2, \ldots, a_\ell]$ with certain orthogonality properties while complementary sequences are tuples of sequences with zero autocorrelation function and elements from the same domain as the orthogonal designs. Orthogonal designs have numerous applications in Statistics, Telecommunications, Coding Theory and Cryptography, see [2, 6, 7]. An OD of order n and type $(t_1, t_2, \ldots, t_\ell)$ denoted $OD(n; t_1, t_2, \ldots, t_\ell)$ in the commuting variables $a_1, a_2, \ldots, a_\ell$, is a square matrix D of order n with entries from the set $\{0, \pm a_1, \pm a_2, \ldots, \pm a_\ell\}$ satisfying $DD^T = \sum_{i=1}^{\ell}(t_i a_i^2) I_n$, where I_n is the identity matrix of order n.

Our approach is twofold; firstly we develop an algebraic framework that models properties of complementary sequences. In this manner, we can apply tools from symbolic computation, i.e., Gröbner bases, to algorithmically treat complementary sequences. Our goal is to obtain an effective (algorithmic) version of the reverse of the celebrated Equating/Killing Lemma in the theory of orthogonal designs.

Lemma 1 (Equating and Killing Lemma [2])**.** *If D is an orthogonal design $OD(n; t_1, t_2, \ldots, t_\ell)$ in the commuting variables $\{0, \pm a_1, \pm a_2, \ldots, \pm a_\ell\}$, then there exist orthogonal designs:*

(i) $OD(n; t_1, t_2, \ldots, t_i + t_j, \ldots, t_\ell)$ $(a_i = a_j)$ *(Equating)*

(ii) $OD(n; t_1, t_2, \ldots, t_{j-1}, t_{j+1}, \ldots, t_\ell)$ $(a_j = 0)$ *(Killing)*

on the $u - 1$ commuting variables $\{0, \pm a_1, \pm a_2, \ldots, \pm a_{j-1}, \pm a_{j+1}, \ldots, \pm a_\ell\}$.

Sequences of zero autocorrelation give rise to ODs, for more details see [2, 6, 7]. In this work, we focus on the level of complementary sequences instead of ODs. In particular, given a set of complementary sequences of type $(t_1, t_2, \ldots, t_\ell)$, we investigate how to compute a new set of complementary sequences of type $(t_1, t_2, \ldots, t_{i-1}, a, b, t_{i+1}, \ldots, t_\ell)$ and another set of complementary sequences of type $(t_1, t_2, \ldots, t_\ell, t_{\ell+1})$ (if possible, otherwise decide it is impossible). In the aftermath, these sets of sequences can be used in suitable arrays to generate the desired ODs.

[*] This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme. This Programme is supported by the Marie Curie Co-funding of Regional, National and International Programmes (COFUND) of the European Commission. In addition, this work was funded by COMET K1, FFG - Austrian Research Promotion Agency.

[†] This research was partially supported by Austrian Science Fund (FWF) grants P20347-N18 and P22748-N18.

2 Complementary Sequences

2.1 Notation

Let $A = \{a_1, a_2, \ldots, a_\ell\}$ be a set of ℓ variables. We denote by $\mathcal{S}^{A,n}$ the set of sequences of length n containing elements from $\{\pm a_1, \pm a_2, \ldots, \pm a_\ell\} \cup \{0\}$. Given k sequences $S_i \in \mathcal{S}^{A,n}$ for $i \in [k]$, we define the k-tuple T to be the sequence $T = (S_i)_{i\in[k]}$, where $[k] = \{1, \ldots, k\}$. The set of all k-tuples containing sequences from $\mathcal{S}^{A,n}$ is denoted by $\mathbb{T}_k^{n,\ell}$. We note that the names of the variables are not essential, thus for denoting $\mathbb{T}_k^{n,\ell}$, ℓ is sufficient and A is not needed.

Given a sequence S we denote by $[S]_a$ the number of occurrences of $\pm a$ in S. We extend the definition for tuples in a natural way, as follows. For $T \in \mathbb{T}_k^{n,\ell}$, we have

$$[T]_i = \sum_{j=1}^{k} [S_j]_i.$$

Definition 2 (Type)**.** *Given a tuple $T \in \mathbb{T}_k^{n,\ell}$ with elements from $\{a_1, a_2, \ldots, a_\ell\}$, we define its type, denoted $\mathcal{T}(T)$, to be $(t_1, t_2, \ldots, t_\ell)$ if $t_i = [T]_{a_i}$ for $i \in [\ell]$.*

2.2 Autocorrelation Function

Let $T \in \mathbb{T}_k^{n,\ell}$, then we define the *non-periodic autocorrelation function* $\mathrm{NPAF}_T(s)$ (abbreviated as NPAF) of T as

$$\mathrm{NPAF}_T(s) = \sum_{j=1}^{k} \sum_{i=1}^{n-s} {S_j}_i {S_j}_{i+s} \tag{1}$$

for $s = 0, 1, \ldots, n-1$ and the *periodic autocorrelation function* $\mathrm{PAF}_T(s)$ (abbreviated as PAF) of T, is defined, reducing $i + s$ modulo n, as

$$\mathrm{PAF}_T(s) = \sum_{j=1}^{k} \sum_{i=1}^{n} {S_j}_i {S_j}_{i+s} \tag{2}$$

for $s = 0, 1, \ldots, n-1$.

It is clear that $\mathrm{PAF}_T(s) = \mathrm{NPAF}_T(s) + \mathrm{NPAF}_T(n-s)$, for $s = 1, \ldots, n-1$. Therefore, if $\mathrm{NPAF}_T(s) = 0$ for all $s = 1, \ldots, n-1$, then $\mathrm{PAF}_T(s) = 0$ for all $s = 1, \ldots, n-1$. But, $\mathrm{PAF}_T(s)$ may equal zero for all $s = 1, \ldots, n-1$, even if the $\mathrm{NPAF}_T(s)$ are not.

Definition 3. *Let $T \in \mathbb{T}_k^{n,\ell}$ with $\mathcal{T}(T) = (t_1, t_2, \ldots, t_\ell)$. We say that T is $k-\mathrm{PAF}(n; t_1, t_2, \ldots, t_\ell)$ (resp. $k - \mathrm{NPAF}(n; t_1, t_2, \ldots, t_\ell)$) if T has zero* PAF *(resp.* NPAF*), i.e,* $\mathrm{PAF}_T(s) = 0$ *(resp.* $\mathrm{NPAF}_T(s) = 0$*) for $s = 1, \ldots, n-1$.*

Remark 4. Recall that the k-tuple $T \in \mathbb{T}_k^{n,\ell}$ was defined as a tuple of sequences $S_i \in \mathcal{S}^{A,n}$ for $i \in [k]$. When the assumptions of definition 3 hold, we say that the k-tuple T is a tuple of complementary sequences.

For more details on complementary sequences and their application in the construction of ODs we refer the interested reader to [2, 3, 4, 7].

In order to unify notation and since the distinction is not essential for the rest of the model, we will use AF_T to denote the autocorrelation function (AF) of a tuple T, irrelevant of whether it is the non-periodic or the periodic one. When needed, the distinction will be made clear by context.

Let $T \in \mathbb{T}_k^{n,\ell}$, then

$$\mathrm{AF}_T(s) = \sum_{j=1}^{k} \sum_{i=1}^{p} {S_j}_i {S_j}_{i+s} \tag{3}$$

for $s = 0, 1, \ldots, n-1$. As already mentioned we are interested only in the two possible types of AF defined previously, namely the non-periodic AF where $p = n - s$ (c.f. Eq. 1) and the periodic AF where $p = n$ and $i + s$ is computed modulo n (c.f. Eq. 2).

Finally, we would like to mention that this work is an extension of our previous approach to provide an algebraic framework for complementary sequences [5].

3 An Algebraic Model for Complementary Sequences

The goal of this section is to develop an algebraic framework for the manipulation of complementary sequences. The three problems we consider are SPLIT, FILL and EXPAND, where SPLIT is the reverse of Equating while FILL and EXPAND are the reverse of Killing. Given a tuple $T \in \mathbb{T}_k^{n,\ell}$ with $\mathcal{T} = (t_1, t_2, \dots, t_\ell)$, we will construct three algebraic systems S_s, S_f and S_e whose solutions give rise to tuples in $\mathbb{T}_k^{n,\ell}$ with types:

SPLIT	FILL	EXPAND
$(t_1, \dots, t_{i-1}, \mathsf{t}, t_i - \mathsf{t}, t_{i+1} \dots, t_\ell)$ for some $\mathsf{t} \in [t_i - 1]$	$(t_1, t_2, \dots, t_i, \mathsf{t}, t_{i+1}, \dots, t_\ell)$ for some $\mathsf{t} \in \left[kn - \sum_{i=1}^{\ell} t_i\right]$	$(t_1, t_2, \dots, t_i + \mathsf{t}, \dots, t_\ell)$ for some $\mathsf{t} \in \left[kn - \sum_{i=1}^{\ell} t_i\right]$

The first step is to introduce new variables x_i and substitute accordingly in the tuple:

SPLIT	FILL	EXPAND
x_i for $i \in [t_i]$ and substitute the j-th occurence of a_i by x_j	x_i for $i \in \left[kn - \sum_{i=1}^{\ell} t_i\right]$ and substitute the j-th 0 by x_j	x_i for $i \in \left[kn - \sum_{i=1}^{\ell} t_i\right]$ and substitute the j-th 0 by x_j

Now we have a tuple of sequences where each position that is candidate to change is assigned to a new variable. We denote by m the number of new variables (this varies depending on the problem). We denote this tuple by T' and note that this tuple no longer belongs to $\mathbb{T}_k^{n,\ell}$, but in $\mathbb{T}_k^{n,\ell+m}$. In order to construct an algebraic model we need to express autocorrelation relations and the type of a tuple algebraically. Moreover, the variables should be bounded and discrete. Although structurally the algebraic systems are the same for all three problems, at each step, the polynomials added in the system are slightly different. Let $\mathcal{R} = \mathbb{Q}[a_1, a_2, \dots, a_\ell, x_1, x_2, \dots, x_m]$ be the polynomial ring in $\ell + m$ variables over the field of rational numbers.

Zero autocorrelation In order to encode autocorrelation algebraically, we observe that the expression for the autocorrelation function is already a polynomial one. It is clear that $\mathrm{AF}_{T'}(s) \in \mathcal{R}$ for $s = 0, 1, \dots, n-1$, i.e., $\mathrm{AF}_{T'}(s)$ is a polynomial in the variables $a_1, a_2, \dots, a_\ell, x_1, x_2, \dots, x_m$. The algebraic conditions for the new tuple, where in the position of x_i we put the value indicated by the root of the system, being a k-AF tuple is that these polynomials are zero.

Bounded Discrete Variables By bounded discrete variable, we mean a variable that takes values from a finite subset of the integers. We need to restrict the solutions of the algebraic systems to take particular values in order to use the solutions to construct new tuples with the desired types. It is easy to see that for $f_i \in \mathbb{K}[x_1, x_2, \dots, x_m]$ we have $V(\langle f_1, f_2, \dots, f_k \rangle) \cap M^m = V(\langle f_1, f_2, \dots, f_k, b_1, b_2, \dots, b_m \rangle)$, where $b_i = \prod_{\alpha \in M}(x_i - \alpha)$ and M is a finite subset of the algebraic closure of $\mathbb{K}$.

It is exactly these polynomials b_i that we need to add to the respective algebraic systems for each of the problems, depending on what set we want the solutions to be restricted in.

SPLIT	FILL	EXPAND
$b_i = x_i^4 - 1$	$b_i = x_i\left(x_i^2 - 1\right)$	$b_i = x_i\left(x_i^2 - a^2\right)$
$x_i \in \{\pm 1, \pm i\}$	$x_i \in \{0, \pm 1\}$	$x_i \in \{0, \pm a\}$

The choice for these values is justified since for SPLIT we want to introduce two new (signed) symbols in the tuple, for FILL we want to introduce one new (signed) symbol but we should allow for zeros to remain zeros and for EXPAND we want to introduce no new symbol, but use the existing one that is being expanded and allow for possible zeros.

Type Conditions We need conditions that force a certain type for the new tuple. For this we use two polynomials, one relating the x_i variables to the variable x_t and one that forces x_t to take discrete values in a feasible range $\{1, 2, \dots, B\}$.

For SPLIT we have that a variable a can be split into two variables of type x_t and $[T]_a - x_t$ for $1 \leq x_t \leq \left\lfloor \frac{[T]_a}{2} \right\rfloor$. For FILL and EXPAND we have that a variable (new or existing respectively) can replace up to $kn - \sum_{i=1}^{\ell} t_i$ zeros. Thus the type conditions consist of two polynomials as follows:

SPLIT	FILL	EXPAND
$B = \left\lfloor \frac{[T]_a}{2} \right\rfloor$	$B = kn - \sum_{i=1}^{\ell} t_i$	$B = kn - \sum_{i=1}^{\ell} t_i$
$T_1 = \prod_{i=1}^{B}(x_t - i)$	$T_1 = \prod_{i=1}^{B}(x_t - i)$	$T_1 = \prod_{i=1}^{B}(x_t - i)$
$T_2 = \left(\sum_{i=1}^{m} x_i^2\right) - m + 2x_t$	$T_2 = \left(\sum_{i=1}^{m} x_i^2\right) - x_t$	$T_2 =$ $\left(\sum_{i=1}^{m} x_i^2\right) - a^2\left([T']_a + x_t\right)$

The algebraic system According to the discussion above, we have that the three algebraic systems S_s, S_f and S_e are as follows:

SPLIT

$$\begin{array}{c} S_s = \\ \left\{ \begin{array}{c} \mathrm{AF}_{T'}(s) \text{ for } s \in [n] \\ B_i = x_i^4 - 1, i \in [m] \\ T_1 = \prod_{i=1}^{B} (x_t - i) \\ T_2 = \left(\sum_{i=1}^{m} x_i^2\right) - m + 2x_t \end{array} \right\} \end{array}$$

FILL

$$\begin{array}{c} S_f = \\ \left\{ \begin{array}{c} \mathrm{AF}_{T'}(s) \text{ for } s \in [n] \\ B_i = x_i \left(x_i^2 - 1\right), i \in [m] \\ T_1 = \prod_{i=1}^{B} (x_t - i) \\ T_2 = \left(\sum_{i=1}^{m} x_i^2\right) - x_t \end{array} \right\} \end{array}$$

EXPAND

$$\left\{ \begin{array}{c} S_e = \\ \mathrm{AF}_{T'}(s), s \in [n] \\ B_i = x_i \left(x_i^2 - a^2\right), i \in [m] \\ T_1 = \prod_{i=1}^{B} (x_t - i) \\ T_2 = \quad \left(\sum_{i=1}^{m} x_i^2\right) - \\ a^2 \left([T']_a + x_t\right) \end{array} \right\}$$

Retrieving the solutions The algebraic systems S_s, S_f and S_e provide us with solutions to the three problems at hand. The last step we need to take is to interpret a root of the system and connect it to a new tuple of complementary sequences. Assume that $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ is such a root of the respective algebraic system. Then we create a new tuple making substitutions in T' as follows:

SPLIT

$$\left\{ \begin{array}{c} \text{if } \alpha_i = 1 \text{ then } x_i = a \\ \text{if } \alpha_i = -1 \text{ then } x_i = -a \\ \text{if } \alpha_i = i \text{ then } x_i = b \\ \text{if } \alpha_i = -i \text{ then } x_i = b \end{array} \right\}$$

FILL

$$\left\{ \begin{array}{c} \text{if } \alpha_i = 0 \text{ then } x_i = 0 \\ \text{if } \alpha_i = 1 \text{ then } x_i = a \\ \text{if } \alpha_i = -1 \text{ then } x_i = -a \end{array} \right\}$$

EXPAND

$$\left\{ \begin{array}{c} \text{if } \alpha_i = 0 \text{ then } x_i = 0 \\ \text{if } \alpha_i = a \text{ then } x_i = a \\ \text{if } \alpha_i = -a \text{ then } x_i = -a \end{array} \right\}$$

We note that since the solution set is zero dimensional (finite number of possible values for a finite number of variables). This means that the reduced Gröbner Basis for a lexicographic (elimination) order will have a triangular form [1].

It is important to mention that the variables a_i appear in the algebraic system we constructed. Nevertheless, due to the independence of the solutions with respect to the variables x_i from the variables a_i, we can project by choosing random values for the variables a_i. There is a finite set of evaluations of the variables a_i that affects the projected variety of the algebraic system. Since we treat the variables a_i as parameters, we are not interested in these evaluations. In other words, by substituting the variables a_i by random values from an infinite set, the part of the solutions of the system that corresponds to the variables x_i remains unchanged with probability 1.

Examples Given a tuple T we apply the algorithm described above to construct an algebraic system, find a solution to the system and interpret accordingly to construct a new tuple of the desired type:

SPLIT

$$T = (a, b, a)|(a, b, -a)|(b, -a, b)|(b, d, -b)$$

$$\mathcal{T}\left((a, b, a)|(a, b, -a)|(b, -a, b)|(b, d, -b)\right) = (1, 5, 6)$$

$$T' = (x_1, b, x_2)|(x_3, b, x_4)|(b, x_5, b)|(b, d, -b)$$

$$\left\{ \begin{array}{c} b * x_1 + b * x_2 + b * x_3 + b * x_4 + 2 * b * x_5, \\ x_1 * x_2 + x_3 * x_4, \\ x_1^4 - 1,\ x_2^4 - 1, \\ x_3^4 - 1,\ x_4^4 - 1, \\ x_5^4 - 1, \\ x_t^2 - 3 * x_t + 2, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + 2 * x_t - 5 \end{array} \right\}$$

Solution: $\alpha = (i, -1, -1, -i, 1)$ and $x_t = 2$

Substitution: $(x_1, x_2, x_3, x_4, x_5) = (a, -c, -c, -a, c)$

New tuple: $(a, b, -c)|(-c, b, -a)|(b, c, b)|(b, d, -b)$

$$\mathcal{T}\left((a, b, -c)|(-c, b, -a)|(b, c, b)|(b, d, -b)\right) = (1, 2, 3, 6)$$

FILL

$$T = (0, b, 0)|(0, b, 0)|(b, 0, b)|(b, d, -b)$$

$$\mathcal{T}\left((0, b, 0)|(0, b, 0)|(b, 0, b)|(b, d, -b)\right) = (1, 6)$$

$$T' = (x_1, b, x_2)|(x_3, b, x_4)|(b, x_5, b)|(b, d, -b)$$

$$\left\{ \begin{array}{c} b * x_1 + b * x_2 + b * x_3 + b * x_4 + 2 * b * x_5, \\ x_1 * x_2 + x_3 * x_4, \\ (x_1^2 - 1) * x_1,\ (x_2^2 - 1) * x_2, \\ (x_3^2 - 1) * x_3,\ (x_4^2 - 1) * x_4, \\ (x_5^2 - 1) * x_5, \\ x_t^5 - 15 * x_t^4 + 85 * x_t^3 - 225 * x_t^2 + 274 * x_t - 120, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - x_t \end{array} \right\}$$

Solution: $\alpha = (1, 1, 1, -1, -1)$ and $x_t = 5$

Substitution: $(x_1, x_2, x_3, x_4, x_5) = (a, a, a, -a, -a)$

New tuple: $(a, b, a)|(a, b, -a)|(b, -a, b)|(b, d, -b)$

$$\mathcal{T}\left((a, b, a)|(a, b, -a)|(b, -a, b)|(b, d, -b)\right) = (1, 5, 6)$$

EXPAND

$$T = (0, b, 0)|(0, b, 0)|(b, 0, b)|(b, d, -b)$$

$$\mathcal{T}\left((0, b, 0)|(0, b, 0)|(b, 0, b)|(b, d, -b)\right) = (1, 6)$$

$$T' = (x_1, b, x_2)|(x_3, b, x_4)|(b, x_5, b)|(b, d, -b)$$

$$\left\{ \begin{array}{c} b * x_1 + b * x_2 + b * x_3 + b * x_4 + 2 * b * x_5, \\ x_1 * x_2 + x_3 * x_4, \\ (x_1 - d)(x_1 + d)x_1,\ (x_2 - d)(x_2 + d)x_2, \\ (x_3 - d)(x_3 + d)x_3,\ (x_4 - d)(x_4 + d)x_4, \\ (x_5 - d)(x_5 + d)x_5,\ d^2 - 1, \\ x_t^5 - 15 * x_t^4 + 85 * x_t^3 - 225 * x_t^2 + 274 * x_t - 120, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - x_t \end{array} \right\}$$

Solution: $\alpha = (1, 1, 1, -1, -1)$ and $x_t = 5$

Substitution: $(x_1, x_2, x_3, x_4, x_5) = (d, d, d, -d, -d)$

New tuple: $(d, b, d)|(d, b, -d)|(b, -d, b)|(b, d, -b)$

$$\mathcal{T}\left((d, b, d)|(d, b, -d)|(b, -d, b)|(b, d, -b)\right) = (6, 6)$$

4 Conclusion

In this paper, we dealt with the problem of constructing new tuples of complementary sequences from a given tuple of complementary sequences on ℓ variables, providing an algorithmic version of the reverse of the Equating-Killing Lemma.

We describe the construction of three algebraic systems, solving the three problems that reverse the Equating-Killing Lemma, namely SPLIT, FILL, EXPAND. This construction is algorithmic and thus, if combined with the use of Gröbner bases, it provides a fully algorithmic framework for the computation of new tuples of complementary sequences.

We employ Gröbner bases, in order to get a convenient description of the ideal of the (zero dimensional) variety we are interested in. The variety provides full information concerning the possible ways to SPLIT a variable, FILL the zeros or EXPAND a variable in a given k-tuple T of complementary sequences.

Our goal is to provide an algebraic model for complementary sequences which can be used to generate orthogonal designs. Conditioned that the algorithmic implementations of the proposed framework retrieve the desired properties for complementary sequences, our next step is to model the statistical properties of orthogonal designs (orthogonality, interactions) again in terms of complementary sequences. This statistical modelling of complementary sequences together with the algorithmic implementations of SPLIT, FILL, EXPAND, will be further explored in future work.

References

[1] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[2] A. V. Geramita and J. Seberry. *Orthogonal designs. Quadratic forms and Hadamard matrices*, volume 45 of *Lecture Notes in Pure and Applied Mathematics.* Marcel Dekker, Inc., New York, NY, 1979.

[3] C. Koukouvinos. Sequences with zero autocorrelation. In C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 452–456. CRC Press, Boca Raton, Fla., 1996.

[4] C. Koukouvinos and J. Seberry. New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function - a review. *J. Statist. Plann. Inference*, 81:153–182, 1999.

[5] C. Koukouvinos, D. E. Simos, and Z. Zafeirakopoulos. An algebraic framework for extending orthogonal designs. In *ISSAC '11: Abstracts of Poster Presentations of the 36th International Symposium on Symbolic and Algebraic Computation, ACM Commun. Comput. Algebra*, volume 45, pages 123–124, 2011.

[6] J. Seberry and R. Craigen. Orthogonal designs. In C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 400–406. CRC Press, Boca Raton, Fla., 1996.

[7] J. Seberry and M. Yamada. Hadamard matrices, sequences and block designs. In J. H. Dinitz and D. R. Stinson, editors, *Contemporary Design Theory: A Collection of Surveys*, pages 431–560. J. Wiley and Sons, New York, 1992.