1997

The Hadamard Matroid and an Anomaly in Its Single Element Extensions

C. H. Cooke
Old Dominion University

Original Publication Citation

Cooke, C. H. (1997). The Hadamard matroid and an anomaly in its single element extensions. *Computers & Mathematics with Applications, 33*(7), 115-120. doi:10.1016/s0898-1221(97)00046-1

Pergamon

Computers Math. Applic. Vol. 33, No. 7, pp. 115–120, 1997

0898-1221/97 $17.00 + 0.00

PII: S0898-1221(97)00046-1

The Hadamard Matroid and an Anomaly in Its Single Element Extensions

C. H. COOKE
Department of Mathematics and Statistics, Old Dominion University, Norfolk, VA 23529, U.S.A.

(Received August 1996; accepted September 1996)

Abstract—A nonstandard vector space is formulated, whose bases afford a representation of what is called a Hadamard matroid, M_p. For prime p, existence of M_p is equivalent to the existence of both a classical Hadamard matrix $H(p,p)$ and a certain affine resolvable, balanced incomplete block design $AR(p)$. An anomaly in the representable single element extension of a Hadamard matroid is discussed.

Keywords—Generalized Hadamard matrix, Hadamard matroid, Independence space, Combinatorial equivalence, Hadamard exponential.

1. INTRODUCTION

The purpose of this note is to present a nonstandard vector space $V_p = V(p,p)$ whose bases afford, for prime p, representations of what is called a Hadamard matroid M_p. Existence of M_p is equivalent to the existence of a generalized Hadamard matrix $H(p,p)$.

There is established a combinatorial equivalence between the class of Hadamard matroids M_p and a certain class of affine resolvable BIB designs $AR(p)$.

The concept of matroid construction by means of an independence rule is considered. It is shown that although some sets in the domain of an independence rule may represent matroids which under the rule allow representable extensions, incompatible sets may exist which are not so favored. Whereas, by set partitioning separate but possibly unrelated matroids may be represented, these incompatible sets *en toto* violate the axioms of an independence space.

In the sequel, unqualified occurrence of the letter p in a mathematical context will be understood as signifying a prime number larger than two. Where special emphasis is desired, the occurrence of prime p will be explicitly indicated.

2. λ-INDEPENDENCE

For $p > 2$ a prime number and λ a positive integer, consider the vector space ${V^\lambda}_p = V(\lambda p, F)$ of vectors whose elements are from the Galois field $F = Gf(p)$. A subset Q is to be called λ-independent iff the vector difference, mod p, of any two arbitrary vectors in Q contains among its elements each member of F exactly λ times. The thrust of this paper will be directed to the case for which $\lambda = 1$, in which circumstance these spaces will be referred to as $V_p = V(p,p)$. Other cases exhibit somewhat similar behaviour and will receive perhaps cursory attention in the final section.

A maximal λ-independent set of vectors from ${V^\lambda}_p$ shall be called a λ-base. The λ-rank of a set B will be defined as the cardinality of a maximal λ-independent subset. The following two theorems characterize the λ-bases of V_p.

THEOREM 1. *Let A be a $q \times q$ matrix over F, where $q = \lambda p$. Then, the column vectors of A are λ-independent iff the column vectors of $A^{\top}$ are λ-independent.*

THEOREM 2. *A λ-base of V_p contains exactly p vectors.*

PROOF OF THEOREM 1. For primes $p > 2$, let x be a primitive p^{th} root of unity. Consider the matrix $H = x^A$, where the notation suggests that $H_{ij} = x^{A_{ij}}$; $i, j = 0, 1, \ldots, \lambda p - 1$. The condition that the column vectors of A are λ-independent and of dimension λp guarantees that the column vectors of H are orthogonal and have square norm of value λp. Therefore, for $p > 2$, H is a generalized Hadamard matrix (see [1,2] for a discussion of generalized Hadamard matrices). As the conjugate-transpose of H is also Hadamard, the row vectors of H are orthogonal and have square norm of value λp. Consequently, the row vectors of A are λ-independent. Conversely, if the rows of A are λ-independent, the previous proof applied to $A^{\top}$ shows that the columns of A are λ-independent. ∎

PROOF OF THEOREM 2. For $\lambda = 1$, let $\omega^{\top} = (0, 1, 2, \ldots, p-1)$. The set of vectors $\{j\omega : j = 0, 1, \ldots, p-1\}$ exhibit a λ-independent set which has cardinality p. To see that p is maximal requires an excursion into the theory of combinatorial design (see [3]). If the zero vector is excluded, the remaining set of $p-1$ vectors can be cyclicly developed, $\bmod p$, to obtain a set of mutually orthogonal Latin squares (mols) of side p. If the base were to possess an additional nonzero vector, a set of $p+1$ mols could likewise be found. However, a maximal set of mols of side p cannot exceed $p-1$ in cardinality. ∎

Equivalence Operations

The major differences encountered when representing vector matroids over subsets of V_p under λ-independence as opposed to ordinary linear independence is now considered. The equivalence operations $E_{(1\text{-}3)}$ given below preserve λ-independence of subsets from V_p whose vectors appear as the columns of some matrix A:

(1) interchange of two rows (or columns);
(2) add any element from F to all elements of any row (or column);
(3) add any element from F to every element of the matrix.

Pivoting as it usually is practiced in solving linear systems does not necessarily preserve λ-independence; nor does permutation of the elements via automorphisms of F. The deletion of an all-zero row can change the character of a set. Possible incompatibility of subsets of vectors of the nonstandard vector space also complicates matters; this subsequently will be discussed.

Canonical Bases

By applying equivalence operations to a matrix B whose column vectors form a base of V_p, one can obtain an equivalent base, or canonical form B, whose first row and column are zero, and whose second row and column each consist of the elements of F in natural order. When matrix A represents a canonical base of V_p, the Hadamard matrix $H = x^A$ referred to in the proof of Theorem 1 is in standard form, and it is also a Vandermonde matrix ($H_{ij} = x^{ij}$, $i, j = 0, 1, 2, \ldots, p-1$).

EXAMPLE 1. For $p = 5$ the symmetric canonical base, C, of V_p which appears to the right

$$\left[\begin{array}{ccccc|ccccc} * & * & B & * & * & * & * & C & * & * \\ 4 & 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 2 & 4 & 0 & 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 & 0 & 0 & 2 & 4 & 1 & 3 \\ 2 & 1 & 0 & 4 & 3 & 0 & 3 & 1 & 4 & 2 \\ 4 & 4 & 4 & 4 & 4 & 0 & 4 & 3 & 2 & 1 \end{array}\right]$$

is obtained from the unsymmetric and apparently unlikely base, B, on the the left by the following sequence: add respectively, one to row 1, four to row 2, two to row 3, three to row 4, one to row 5; then move row 5 into the first position.

3. MATROIDS REPRESENTABLE OVER V_p

Oxley [4] gives the following definition: a matroid $M = M(E)$ is an ordered pair (E, I) consisting of a finite set E and a maximal collection, I, of subsets from E which satisfy the axioms $(\kappa)_{1,2}$ of *heredity* and *independence augmentation*:

(1) $I_1 \in I$ and $I_2 \subset I_1 \Rightarrow I_2 \in I$,

(2) $I_1, I_2 \in I$ with $|I_1| < |I_2| \Rightarrow \exists e \in (I_2 - I_1)$ such that $I_1 \cup e \in I$.

REMARK. $(\kappa)1 \Rightarrow \phi \in I$.

EXAMPLE 2: THE HADMARD MATROID. Let $E = \{0, 1, 2, 3, 4\}$ represent the collection of column indices of either of the 5×5 matrices B or C of Example 1. If a subset of E is defined as independent when the corresponding set of column vectors of B (or C) are λ-independent, there results two vector matroids $M_B(E), M_C(E)$, each of which is isomorphic to the uniform free matroid $U_{5,5}$ (see [4, p. 19]). B and C are called representation matrices over V_p of the matroid $U_{5,5}$.

In general, under the rule of λ-independence $U_{p,p}$ is representable by a vector matroid over V_p (see the bases B_p which appear in the proof of Theorem 2). This representation is not unique, as any sequence of equivalence operations $E1$–$E3$ produces the representation matrix of a vector matroid isomorphic to $U_{p,p}$. In the sequel any vector matroid M_p over V_p which is a representation of $U_{p,p}$ will be referred to as a *Hadamard matroid*.

4. COMBINATORIALLY EQUIVALENT STRUCTURES

Butson [1,2] investigates the properties of generalized Hadamard matrices and relations to relative difference sets. Shrikhande [5] establishes that the existence of certain orthogonal arrays of strength two implies existence of generalized Hadamard matrices. In the present section it is demonstrated that for primes $p > 2$, the problems of constructing a generalized Hadamard matrix $H(p, p)$, or a Hadamard matroid M_p, are combinatorially equivalent to constructing an *affine resolvable* balanced incomplete block design characterized by parameters

$$AR(p) : v = p^2,\ b = p^2 + p,\ r = p + 1,\ k = p,\ \lambda = 1. \tag{1}$$

This result is a counterpart of Todd's report [6] that, for integers $t > 1$, construction of a classical Hadamard matrix $H(2, 4t)$ is combinatorially equivalent to the problem of constructing an *unresolvable*, symmetric, balanced incomplete block design whose parameters are $(v = b = 4t - 1,\ r = k = 2t - 1,\ \lambda = t - 1)$.

For primes $p > 2$ and x a primitive p^{th} root of unity, consider the Hadamard matrix $H(p, p)$ whose elements satisfy $h_{ij} = x^{ij};\ i, j = 0, 1, 2, \ldots, p - 1$, and whose conjugate-transpose has the property $H * H^{CT} = pI$. It is remarked that any generalized Hadamard matrix $H^*(p, p)$ can be transformed into the standard form $H(p, p)$.

As in the proof of Theorem 1, there is associated by means of the equation

$$H = x^E, \tag{2}$$

a matrix of exponents $E = (e_{ij}) = (ij)$, $\bmod p : i, j = 0, 1, \ldots, p - 1$, where E as a base for V_p uniquely represents (the standard form of) what has been defined as an isomorphic class of Hadamard matroids M_p.

The fact that for $\lambda = 1$, E is λ-independent and in the standard form required of a generating matrix for the α method (see [7]) assures that the $\alpha(0, 1)$ design generated by E will be a group

divisible (GDD2), resolvable, incomplete block design characterized by m groups of n treatments whose parameters are

$$\text{GDD}(p) : v = mn;\ m = n = p;\ k = r = p;\ b = p^2;\ \lambda_1 = 0;\ \lambda_2 = 1. \tag{3}$$

Moreover, the groups of first associates of the design appear together in the rows of the matrices which represent each resolution class.

The previous process can be reversed: as John [7] observes, given design GDD(p) generated by the alpha method, its generating matrix B is readily inferred. If the generator matrix B were not a λ-base, the design could not be $\alpha(0,1)$. By transforming the base to canonical form E through the equivalence operations ($E1$–$E3$), a generalized Hadamard matrix $H(p,p) = x^E$ in standard form is obtained.

Finally, to complete the demonstration it is shown that $AR(p)$ and GDD(p) can each be obtained from the other. To obtain $AR(p)$ from GDD(p), as resolution class $p+1$ simply take the transpose of the first resolution class, whose columns are the p groups of first associates which have never concurred in the blocks of the design. The extended design is the affine resolvable BIB design having parameters

$$AR(p) : v = p^2;\ k = p;\ r = p+1;\ b = p^2 + p;\ \lambda = 1. \tag{4}$$

Clearly, to obtain GDD(p) from arbitrary $AR(p)$, that unique resolution class is omitted whose columns qualify as the groups of first associates. (If no resolution class has columns which qualify as groups of first associates, there is an isomorphic design for which this will be true.)

Thus, to within isomorphism on the design end, and to within standard form of the λ-base and the generalized Hadamard matrix $H(p,p)$, there exists a combinatorial equivalence between the three said structures.

5. ANOMALIES CONCERNING MATROID SINGLE ELEMENT EXTENSIONS

The concept of matroid extension by means of an independence rule is now considered. It is shown that although some sets in the domain of the independence rule for V_p may represent matroids which under the rule have representable extensions, incompatible sets may exist which are not so favored. Whereas by set partitioning separate but unrelated matroids thus may be represented, these incompatible sets *en toto* violate the axioms of an independence space.

Matroids can be defined by many equivalent sets of axioms (see [4]), of which $(\kappa)_{1,2}$ represent perhaps the most basic. The study of matroids is an analysis of an abstract theory of independence, and matroidal structures are sometimes referred to as independence spaces [8].

Implicit in Oxley's definition of a matroid is the existence of an *independence rule*, R, for determining which subsets of ground set E are independent. This rule can be an explicit listing of independent subsets, or an analytical prescription describing means to partition the members of the power set 2^E into independence class I and dependence class not(I). In any case, the rule implies existence of a binary mapping $f : 2^E \to Gf(2)$. An independence space is defined *a posteriori* by the rule iff the set members of $I = f^{-1}(1)$ satisfy the axioms of independence $(\kappa)_{1,2}$.

An independence rule, R, whose domain covers the entire power set of a space S is defined as a *global* or else a *local* independence rule on S depending upon whether or not the power set 2^E of each finite set $E \subset S$ possesses a maximal subcollection I of sets satisfying $\kappa_{(1,2)}$. Ordinary and affine linear independence each provide a global independence rule on V_p. It is intended to show that the rule associated with λ-independence is strictly local.

Where no confusion should be so caused, subsets of V_p could simply be referred to as independent whenever they are λ-independent; otherwise, they are called dependent. However, this terminology is strictly correct only for specially selected subsets E of V_p which also satisfy the axioms $(\kappa)_{1,2}$ of an independence space.

For example, consider the bases B and C exhibited in Example 1: suppose it is attempted to represent a six element matroid $M1 = M(B \cup e)$ by inclusion of any column vector, $e \in C$. Of necessity, $M(B)$ is a restriction of $M1$ (a deletion of e). However, under the rule of λ-independence, the independent sets B and e do not satisfy the independence augmentation axiom $(\kappa)_2$. This is because in its actions e is a zero vector: although there are no vectors in V_p which under λ-independence represent single-element minimal dependent sets, yet e makes dependent any subset of B with which it is included. Therefore, $B \cup e$ cannot represent a vector matroid. (However, changing the independence rule such that e is a dependent vector (a loop) would allow $B \cup e$ to represent a vector matroid.)

As Example 2 indicates, whereas $Q = B \cup C$ does not collectively represent a matroid on V_p, the existence of $M(B)$ and $M(C)$ demonstrates existence of restricted subsets of Q which do represent vector matroids. Generally, the matroids which are representable by vector matroids over V_p consist of the direct sum of a uniform free matroid $U_{n,n}$, $n < p+1$ and a nontrivial parallel class. Loops as well as circuits of more than two elements cannot be represented. Of course, this means that the dual of a representable matroid may not be representable.

Oxley [4] proves that if matroid $M = M(E)$ possesses a modular cut C, there is a unique single element extension $N = M(E \cup e)$ such that C consists of flats F of M for which $F \cup e$ is a flat of N having the same rank as F. This theorem has been used by Crapo [9] in finding all matroids on a given set of eight elements. The process concerns starting with a matroid M having n elements and progressing to matroids N having $n+1$ elements by examining all modular cuts of M and its dual M^*. It is perhaps interesting to point out that in forming representable single element extensions of representable matroids, for the case of a global independence rule it appears necessary only to arbitrarily include another vector.

6. SPACES $V^{\lambda}{}_{p}$ WITH $\lambda > 1$

There is now given an example of λ-independence where $\lambda > 1$. Consider $V_p = V^3{}_p = V(3p, F)$: for $p = 3$ the column vectors of the matrix D defined by

$$\begin{bmatrix} * & * & * & * & D & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

constitute a λ-base of $V^{\lambda}{}_3$. The justification is as follows: these nine vectors are a maximal independent set, as existence of a set of ten independent vectors contradicts the fact that no first associates of an $\alpha(0,3)$ GDD2 design can concur in the design. Nine resolution classes employ each pair of second associates exactly three times each.

Further, as one suspects, if x is a primitive cube root of unity, the generalized Hadamard matrix $H = H(3,9)$ is obtained from the relation $H = x^D$. Also, the vector matroid $M(D)$ is the Hadamard matroid which represents the free matroid $U_{9,9}$.

Shrikhande [5] establishes that the existence of a certain orthogonal array of strength two implies the existence of a generalized Hadamard matrix $H(p, p^2)$.

The array Q given below provides the Hadamard exponent for a Hadamard matrix $H(3,6) = x^Q$:

$$\begin{bmatrix} * & * & Q & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 \end{bmatrix}.$$

Whereas matrix Q is tedious to obtain by trial and error, the matrix D easily follows by use of a direct sum, employing

$$\begin{bmatrix} * & E & * \\ 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}$$

the result below on E, plus row and column interchanges.

LEMMA 1. *If $H = H(p,p)$ is a Hadamard exponent, then the direct sum $H(p,p^2) = (h_{ij} + H;\ i,j = 0,1,\ldots,p-1)$ is a block Hadamard exponent which is also a Hadamard exponent.*

REFERENCES

1. J.A. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13**, 894–898 (1962).
2. J.A. Butson, Relations among generalized Hadamard matrices, *Can. J. Math.* **15**, 42–48 (1963).
3. C.H. Cooke, An enlarged class of resolvable, incomplete block designs, *Ars Combinatoria* (in press).
4. J.G. Oxley, *Matroids*, Oxford University Press, Oxford, (1992).
5. S.S. Shrikhande, Generalized Hadamard matrices and orthogonal arrays of strength two, *Can. J. Math.* **16**, 736–740 (1964).
6. J.A. Todd, A combinatorial problem, *J. Math. Phys.* **12**, 321–333 (1933).
7. J.A. John, *Cyclic Designs*, Chapman and Hall, New York, (1987).
8. V. Bryant and H. Perfect, *Independence Theory in Combinatorics*, Chapman and Hall, New York, (1980).
9. H.H. Crapo, Single element extensions of matroids, *J. Res. Nat. Bur. Standards Sec. B* **69B**, 55–65 (1965).
10. E.R. Williams, A new class of resolvable block designs, Ph.D. Thesis, University of Edinburgh, (1975).