Abstract hyperovals and Hadamard designs

Burkard Polster
Department of Pure Mathematics
University of Adelaide
Adelaide, SA 5005
E-mail: bpolster@maths.adelaide.edu.au

Dedicated to the memory of Derrick Breach, 1933–1996

1 Introduction

Given a hyperoval in a finite projective plane of even order, define an incidence structure whose point and block sets both coincide with the set of points of the plane not contained in the hyperoval and let a point and a block of the incidence structure be incident if and only if their connecting line in the projective plane intersects the hyperoval. It is a well-known fact that this incidence structure is a Hadamard design (cf. [6, Section 1] and the references given there).

By mimicking Buekenhout's definition of abstract ovals, we introduce abstract hyperovals. Associated with any hyperoval in a projective plane is an abstract hyperoval. We describe a construction of Hadamard designs from abstract hyperovals which can be regarded as a generalization of the above construction since the Hadamard designs constructed from a hyperoval and its associated abstract hyperoval are isomorphic. Nevertheless, our construction is a proper generalization since there exist abstract hyperovals that do not arise from hyperovals in projective planes.

2 Abstract ovals and abstract hyperovals

An *abstract oval* (also *Buekenhout oval* or *B-oval*) (M, F) of order n consists of a set M of $n+1 > 2$ points and a set F of *involutions* of M such that the set F is *quasi sharply 2-transitive*, that is, for any $a_1, a_2, b_1, b_2 \in M$, with $a_i \neq b_j$, $i, j = 1, 2$, there is a unique $f \in F$ such that $f(a_1) = a_2$ and $f(b_1) = b_2$. Similarly, an *abstract hyperoval* (M, F) of order n consists of a set M of $n+2 > 3$ points and a set F of fixed-point-free involutions of M such that for any four distinct elements $a_1, a_2, b_1, b_2 \in M$ there is a unique $f \in F$ such that $f(a_1) = a_2$ and $f(b_1) = b_2$.

The standard reference for abstract ovals is [2]. To our knowledge abstract hyperovals have not appeared in the literature yet, but, as we shall see below, they are to a large extent equivalent to abstract ovals and their properties can easily be derived from the respective properties of abstract ovals.

Australasian Journal of Combinatorics 16(1997), pp.29–33

Let P be the point set of a projective plane of order n and let M be a set of $n+1$ or $n+2$ points in P such that no three of the points in M are collinear. Then M is called an *oval* or a *hyperoval*, respectively. A line in the plane is called *tangent* or *secant* of M if it intersects M in 1 or 2 points, respectively. For an introduction to ovals and hyperovals the reader is referred to [1]. For every point $p \in P \setminus M$ define an involution $i_p : M \to M$ as follows: Let $x \in M$ and let l be the connecting line of p and x. If l is a tangent of M, then $i_p(x) = x$. If l is secant of M, then $i_p(x)$ is the second point of intersection, other than x, of l with M. If F is the set of all involutions defined in this manner, it is easy to verify that (M, F) is an abstract oval or an abstract hyperoval, depending on whether M is an oval or a hyperoval. An abstract oval or hyperoval is called *projective* if it arises in this manner from an oval or a hyperoval, respectively, in a projective plane.

Remember that hyperovals occur only in projective planes of even order and that, similarly, because the set F consists of fix-point-free involutions, abstract hyperovals are necessarily of even order. It is also well-known that all tangents of an oval in a projective plane of even order meet in a point and that by adding this point to the oval we arrive at a hyperoval. On the other hand, removing a point from a hyperoval gives an oval. By imitating the first construction, it is possible to construct abstract hyperovals from abstract ovals: Let (M, F) be an abstract oval of even order n. Then it is known that the set F contains the identity id_M and that all other involutions contained in F are involutions fixing one point each (cf. [2, p. 338, 1.9]). Let $\bar{M} := M \cup \{\infty\}$, where ∞ is not contained in M. If i is an involution contained in $F \setminus \{id_M\}$, we extend i to an involution $\bar{i}$ of $\bar{M}$ by replacing the uniquely determined fixed point (p) of i in the cycle decomposition of i by the transposition (p, ∞). Clearly, if $\bar{F}$ is the set of all such extended involutions, the pair $(\bar{M}, \bar{F})$ is an abstract hyperoval. It is also clear how one derives an abstract oval from an abstract hyperoval (M, F): Delete one point ∞ from M to arrive at a set M', replace the transposition (∞, p) in the cycle decomposition of every involution $i \in F$ by the fixed point (p) to arrive at a set of involutions of M' and add $id_{M'}$ to this set to arrive at a set F'. Then (M', F') is clearly an abstract oval.

Given any abstract (hyper)oval $A = (M, F)$, we may construct the so-called *ambient* of A. This ambient is an incidence structure the point set of which is $M \cup F$. For any $a, b \in M$, where $a \neq b$, if A is an abstract hyperoval, we define a line $(a, b) = (b, a)$ that contains the points a and b and precisely those involutions in F that map a to b. The line (a, b) is called a tangent or secant if $a = b$ or $a \neq b$, respectively. We note that any two distinct lines intersect in a unique point and that the ambient of an abstract hyperoval contains no tangents. Clearly, in the case of a projective abstract (hyper)oval the lines in the ambient, as we defined them above, correspond to those lines in the projective plane that intersect the corresponding (hyper)oval.

We summarize some basic properties of abstract hyperovals in the following proposition.

2.1 Proposition. *Let $A = (M, F)$ be an abstract oval or an abstract hyperoval. Then $(\bar{M}, \bar{F})$ or (M', F'), respectively, is an abstract hyperoval or an abstract oval.*

Let A be an abstract hyperoval of order $n = 2t$. Then

(1) *F contains $n^2 - 1 = 4t^2 - 1$ involutions;*

(2) *every line in the ambient of A contains precisely $2t - 1$ involutions. This means that, given $a, b \in M$, $a \neq b$, the set F contains $2t - 1$ involutions exchanging a with b.*

Proof. The two properties correspond to the respective properties of the abstract oval (M', F'). See [2, 1.6 and 1.11]. □

Clearly, we do get the same abstract hyperoval no matter whether we first complete an oval to a hyperoval and then associate an abstract hyperoval with this hyperoval or whether we first associate an abstract oval to the oval and then make this abstract oval into an abstract hyperoval as above. With these considerations it is clear that an abstract hyperoval associated with an abstract oval is projective if and only if the abstract oval is projective. Since non-projective abstract ovals of even order have been shown to exist we arrive at the following corollary.

2.2 Corollary. *There exist non-projective abstract hyperovals.*

3 Hadamard designs

A *Hadamard design* is a symmetric 2-design with parameters $v = 4t-1$, $k = 2t-1$ and $\lambda = t - 1$. See [1, Chapter 7] for information about Hadamard designs.

We want to generalize the construction of Hadamard designs from hyperovals in finite projective planes as described in Section 1. Our generalized construction can be described in very simple terms as follows.

Let $A = (M, F)$ be an abstract hyperoval. Define an incidence structure whose point and block sets both coincide with F and let a point and a block of the incidence structure be incident if and only if they are connected by a line in the ambient of A. We will show that this incidence structure is a Hadamard design.

Using the remarks in the previous section, this translates to the well-known construction in the projective setting described in the Section 1 and it is clear that the Hadamard designs constructed from a hyperoval and its associated abstract hyperoval are isomorphic.

In the following let A be of order $n = 2t$, identify M with the set $\{1, 2, \ldots, 2t+2\}$ and let i_r ($r = (2t-1)(x-2)+1, (2t-1)(x-2)+2, \ldots, (2t-1)(x-2)+(2t-1) = (2t-1)(x-1)$) denote the $n - 1 = 2t - 1$ involutions in F that are contained in the line $(1, x)$, $1 \neq x \in M$ (see Proposition 2.1).

We define a map $(|) : F \times F \to \{0, 1\}$ as follows: Let $(i_r|i_s) = 1$, with $r, s \in \{1, 2, \ldots, 4t^2 - 1\}$, if there are two elements $a, b \in M$ such that both i_r and i_s exchange a with b. This is of course equivalent to saying that there is a line in the ambient of A that contains both i_r and i_s. Let $(i_r|i_s) = 0$ otherwise. Since each involution $i \in F$ is contained in precisely one of the lines through the point $1 \in M$, this map is well-defined.

3.1 Theorem. *The matrix* $H = (h_{r,s})$ *with entries* $h_{r,s} := (i_r|i_s)$ *for* $r, s \in \{1, 2, \ldots, 4t^2 - 1\}$ *is the incidence matrix of a Hadamard design with parameters* $v = 4t^2 - 1$, $k = 2t^2 - 1$, $\lambda = t^2 - 1$. *Furthermore,* H *is symmetric and can be partitioned into* $(2t+1)^2$ *blocks* $H_{a,b}$, $a, b \in M \setminus \{1\}$, *of* $(2t-1) \times (2t-1)$ *matrices such that* $H_{a,a}$ *is a matrix all of whose entries are 1's and* $H_{a,b}$, $a \neq b$, *has the property that precisely* $t-1$ *of the entries in each of its rows and columns are 1's.*

Proof. Let $N(i_r)$ be the number of $i \in F$ such that there is a line in the ambient of A containing both i_r and i. Let $N(i_r, i_s)$, $r \neq s$, be the number of $i \in F$ that are connected by lines in the ambient of A to both i_r and i_s.

Since $(i_r|i_s) = (i_s|i_r)$, the matrix H is symmetric. We have to show that $N(i_r) = 2t^2 - 1$ and $N(i_r, i_s) = t^2 - 1$ for all possible $r, s \in \{1, 2, \ldots, 4t^2 - 1\}$. The cycle decomposition of i_r contains $|M|/2 = t + 1$ transpositions. This just means that there are $t + 1$ lines in the ambient of A passing through this point. By Proposition 2.1, each such line contains $2t - 1$ involutions. Furthermore, these lines are pairwise disjoint except for the point i_r itself. Thus $N(i_r) = (2t-2)(t+1)+1 = 2t^2 - 1$.

Let i_r, i_s be two distinct involutions, that is, $r \neq s$. We distinguish two cases:

(1) $(i_r|i_s) = 1$, that is, there is a line (a_1, a_2) in the ambient of A that contains both i_r and i_s. This line contains $2t - 1$ involutions. Apart from (a_1, a_2) there are t further lines in the ambient of A that pass through i_r, and the same is of course true for i_s. If we pick one, say (a_3, a_4), and look at the points of intersection of (a_3, a_4) with the lines through i_s excepting the line (a_1, a_2), we count t different points, two of which, namely a_3 and a_4, are no involutions but elements of M. Thus $N(i_r, i_s) = 2t-1+t(t-2) = t^2-1$.

(2) $(i_r, i_s) = 0$. In the ambient of A each of the $t+1$ lines through i_r intersects the $t + 1$ lines through i_s in $t + 1$ points two of which are no involutions. Thus $N(i_r, i_s) = (t + 1)(t - 1) = t^2 - 1$. This proves that H is indeed the incidence matrix of a Hadamard design.

By arranging the i_r's in a very special manner we achieved that $H_{a,a}$ is a matrix of 1's just means that in the ambient of A any two of the involutions on the line $(1, a)$ are connected by lines. Of course, this is true. Furthermore, $H_{a,b}$, $a \neq b$, is a matrix such that precisely $t - 1$ of the entries in each of its rows and columns are 1's means that each involution i on $(1, a)$ is connected to precisely $t - 1$ involutions on $(1, b)$ and vice versa: Apart from $(1, a)$ there are t lines passing through i intersecting $(1, b)$ in t distinct points. The point $b \in M$ is always among these and is the only one that is not an involution. □

Further properties of the Hadamard designs constructed in this manner from hyperovals in finite projective planes (via the associated abstract hyperovals) have been investigated in [5] and [6] (see also the information on *oval designs* in [1]). In particular, it is shown in [6] that under suitable circumstances some of the submatrices $H_{a,b}$, $a \neq b$, can themselves be incidence matrices of Hadamard designs.

Of course, the Hadamard design associated with an abstract oval can be considered as an invariant of the abstract oval. In this context it would be interesting

to investigate whether this invariant is complete or not, that is, whether there are non-isomorphic abstract ovals whose associated Hadamard designs are isomorphic.

We also want to point out that there is a construction by Bush [3] which associates with any projective plane of even order n a Hadamard design with the same parameters as the Hadamard design associated with any hyperoval in a finite projective plane of order n.

References

[1] E. F. Assmus and J. D. Key, *Designs and their codes, Cambridge Tracts in Mathematics, 103. Cambridge University Press, Cambridge, 1992.*

[2] F. Buekenhout, *Étude intrensèque des ovales*, Rend. Mat. **25** (1966), 333-393.

[3] K. A. Bush, *Unbalanced Hadamard matrices and finite projective planes of even order*, J. Comb. Theory, Series A **11** (1971), 38–44.

[4] G. Faina, *The B-ovals of order $q \leq 8$*, J. Comb. Theory, Series A **36** (1984), 307–314.

[5] A. Maschietti, *Hyperovals and Hadamard designs*, J. Geometry **44** (1992), 107–116.

[6] A. Maschietti, *On Hadamard designs associated with hyperovals*, J. Geometry **53** (1995), 122–130.

(Received 3/9/96)