A Model of the Witt Design W_{12} based on Quadrics of PG$(2,3)$*

Hans Havlicek

In memory of H. Brauner (1928–1990) on the occasion of his 70th birthday

Abstract

An elementary geometric proof for the existence of Witt's 5–$(12,6,1)$ design is given.

Keywords: small Witt design, quadrics.

1 Introduction

In the present paper we present a proof for the existence of *Witt's* 5–$(12,6,1)$ *design* W_{12}. The points of the design will be all points but one of the projective plane of order three, the blocks are defined via quadratic equations. Some blocks are subsets of quadrics, others are sets of points related with quadrics, e.g., the set of external points of a conic.

Although we shall never make use of it, in the background of our considerations there will always be the *Veronese surface* $\mathcal{V}$ in PG$(5,3)$ and a cap $\mathcal{K}$ in PG$(5,3)$, which is a point model for Witt's 5–$(12,6,1)$ design W_{12} [2], [6]. There are various connections between the Veronese surface $\mathcal{V}$ and the cap $\mathcal{K}$ [3], [4]. By implementing results from the above–mentioned papers, our proof could even be shortened. We aim, however, at an elementary proof. In fact, the prerequisites for reading this article are basic linear algebra and some properties of quadrics in PG$(2,3)$.

2 A planar model of W_{12}

Throughout this paper $F := \mathrm{GF}(3) = \{0,1,2\}$ denotes the field with three elements. The point set $\mathcal{P}(F^3)$ of the projective plane PG$(2,3)$ is the set of one–dimensional subspaces of F^3. Lines of PG$(2,3)$ are considered as sets of points.

*Research supported by the Austrian FWF, project P12353–MAT.

Definition 1 *An incidence structure* $(\mathcal{W},\mathcal{B},\in)$ *with point set* $\mathcal{W}$ *and block set* $\mathcal{B}$ *is given as follows: Fix one point* $U = F(u_0,u_1,u_2)\in\mathcal{P}(F^3)$ *and define*

$$\mathcal{W} := \mathcal{P}(F^3)\setminus\{U\}. \tag{1}$$

A subset b *of* $\mathcal{W}$ *is a block, if the subsequent conditions hold true:*

1. *b has more than three elements.*
2. *There is a non–zero quadratic form* $q : F^3 \to F$ *such that* b *consists of all points* $X = F(x_0,x_1,x_2)\in\mathcal{W}$ *satisfying*

$$(x_0,x_1,x_2)^q = 2\cdot(u_0,u_1,u_2)^q. \tag{2}$$

Observe that

$$(2\cdot(x_0,x_1,x_2))^q = 2^2\cdot(x_0,x_1,x_2)^q = (x_0,x_1,x_2)^q \tag{3}$$

for all $(x_0,x_1,x_2)\in F^3$ and all quadratic forms $q : F^3\to F$. Thus (2) does not depend on the choice of vectors representing the points X and U, respectively.

It is an easy task to describe all blocks explicitly: Each quadratic form $q : F^3 \to F$ and each $t\in F$ give rise to a point–set of $\mathrm{PG}(2,3)$ by putting

$$\mathcal{Q}_t(q) := \{F(x_0,x_1,x_2) \mid (x_0,x_1,x_2)^q = t,\ (x_0,x_1,x_2)\neq(0,0,0)\}. \tag{4}$$

By (3), this definition is unambiguous. Note that $\mathcal{Q}_1(q)=\mathcal{Q}_2(2q)$ and $\mathcal{Q}_2(q)=\mathcal{Q}_1(2q)$.

Up to a change of coordinates and multiplication of q by $2\in F$ there are the following cases for $q\neq 0$ [5, p. 156]:

$(x_0,x_1,x_2)^q$	$\#\mathcal{Q}_0(q)$	$\#\mathcal{Q}_1(q)$	$\#\mathcal{Q}_2(q)$
$x_0^2+x_1^2+x_2^2$	4	3	6
$x_0^2+x_1^2$	1	6	6
$x_0^2-x_1^2$	7	3	3
x_0^2	4	9	0

(5)

(Here $\#M$ denotes the cardinality of a set M.) Therefore a subset b of $\mathcal{W}$ is a block if, and only if, one of the following holds:

Case A: $b=\mathcal{Q}_t(q)$ with $t\in F\setminus\{0\}$ and $U\in\mathcal{Q}_{2t}(q)$. By $\#\mathcal{Q}_t(q)>3$ and $\#\mathcal{Q}_{2t}(q)>0$ the last two lines of (5) can be ruled out. So either $\mathcal{Q}_0(q)$ is a conic ($x_0^2+x_1^2+x_2^2=0$) and b is the set of its six external points, whereas U is internal, i.e., it does not lie on a tangent; or $\mathcal{Q}_0(q)$ is a singleton ($x_0^2+x_1^2=0$) and b is the symmetric difference $(r\cup s)\setminus(r\cap s)$ of two distinct lines with $U\notin r\cup s$ and $\mathcal{Q}_0(q)=r\cap s$.

Case B: $b=\mathcal{Q}_0(q)\setminus\{U\}$ with $q\neq0$ and $U\in\mathcal{Q}_0(q)$. We infer from $\#\mathcal{Q}_0(q)>4$ and (5) that $\mathcal{Q}_0(q)$ is a pair of lines ($x_0^2-x_1^2=0$), say $\mathcal{Q}_0(q)=g\cup h$. Therefore $b=(g\cup h)\setminus\{U\}$, where $U\in g\cup h$.

Very loosely speaking, a block is either one "side" of a quadric with U being on the "other side", or it is the set of all points in $\mathcal{W}$ of a quadric containing U.

Theorem 1 *The incidence structure* $(\mathcal{W}, \mathcal{B}, \in)$ *described in Definition 1 is a* 5–$(12, 6, 1)$ *design.*

Proof. By (1), there are 12 points in $\mathcal{W}$ and, from our previous discussion, all blocks have exactly 6 elements.

In the sequel let $(u_0, u_1, u_2) := (1, 0, 0)$. So, in terms of coordinates, an equation of a block takes the form

$$\sum_{0 \le i \le j \le 2} a_{ij} x_i x_j = 2a_{00}, \text{ with at least one } a_{ij} \neq 0. \tag{6}$$

Suppose that we are given a 5–set $\mathcal{D} = \{F(d_{0k}, d_{1k}, d_{2k}) \mid k \in \{0, 1, \dots, 4\}\}$ contained in $\mathcal{W}$. In order to obtain all blocks through $\mathcal{D}$ we have to find the non–zero solutions of the linear homogeneous system

$$\sum_{0 \le i \le j \le 2} a_{ij} d_{ik} d_{jk} = 2a_{00}, \quad k \in \{0, 1, \dots, 4\}. \tag{7}$$

This is a system of 5 equations in 6 unknowns a_{ij}, whence a non–zero solution exists, i.e., there is at least one block containing $\mathcal{D}$. In order to show its uniqueness, we have to distinguish two cases:

Case A: Each solution with $a_{00} = 0$ is trivial. Consequently,

$$\det \begin{pmatrix} d_{00}d_{10} & d_{00}d_{20} & d_{10}^2 & d_{10}d_{20} & d_{20}^2 \\ d_{01}d_{11} & d_{01}d_{21} & d_{11}^2 & d_{11}d_{21} & d_{21}^2 \\ \dots & \dots & \dots & \dots & \dots \\ d_{04}d_{14} & d_{04}d_{24} & d_{14}^2 & d_{14}d_{24} & d_{24}^2 \end{pmatrix} \neq 0, \tag{8}$$

so that all solutions of (7) form a one–dimensional subspace of F^6, as required.

Case B: There is a non–trivial solution $(\overline{a}_{00}, \dots, \overline{a}_{22}) \in F^6$ with $\overline{a}_{00} = 0$. The numbers $\overline{a}_{ij} \in F$ determine a non–zero quadratic form $\overline{q} : F^3 \to F$ and a quadric $\mathcal{Q}_0(\overline{q})$ containing $\mathcal{D} \cup \{U\}$. By (5), $\mathcal{Q}_0(\overline{q})$ is a pair of lines, say $\overline{g} \cup \overline{h}$. So

$$\overline{b} := (\overline{g} \cup \overline{h}) \setminus \{U\} \tag{9}$$

is one block through $\mathcal{D}$.

Conversely, let b be a block passing through $\mathcal{D}$. There is no 5–arc in $\mathrm{PG}(2, 3)$, so that at least three points of $\mathcal{D}$ are on a line, say $\overline{g}$. There are three possibilities:

1. b stems from a pair of lines $g \cup h$, i.e., $b = (g \cup h) \setminus \{U\}$. Then the quadrics $g \cup h$ and $\overline{g} \cup \overline{h}$ have six common points, whence they are identical.

2. b is the set of external points of a conic c. No line contains four external points of a conic (cf. [5, p. 178]). So $\overline{g}$ is a tangent of c and $\#(\overline{g} \cap \mathcal{D}) = 3$. We infer $U \notin \overline{g}$, since there are no internal points on a tangent. By $\#\mathcal{D} = 5$, $\overline{h} \setminus \overline{g}$ contains two distinct external points and the internal point U. Hence $\overline{h}$ is an exterior line carrying two distinct internal points. This implies that $\overline{g}$ and $\overline{h}$ meet at an internal point which contradicts $\overline{g}$ being a tangent.

3. There are two distinct lines r, s, with $b = (r \cup s) \setminus (r \cap s)$ and $U \notin r \cup s$. W.l.o.g. let $\#(r \cap \mathcal{D}) = 3$, so that $\#(s \cap \mathcal{D}) = 2$. The quadric $\overline{g} \cup \overline{h}$ contains three distinct points of r, whence $r \subset \overline{g} \cup \overline{h}$. Similarly, it follows now that $s \subset \overline{g} \cup \overline{h}$. Hence $U \in \overline{g} \cup \overline{h} = r \cup s$, an absurdity.

Thus obviously $b = \overline{b}$. $\square$

Remark 1 Up to isomorphism, the Witt design W_{12} is the only 5–$(12, 6, 1)$ design [1, Chapter IV, §2]. The stabilizer of U in the collineation group of $\mathrm{PG}(2, 3)$ yields a subgroup of the automorphism group of W_{12}, i.e., the Mathieu group M_{12}.

Remark 2 If $\{A, B, C, U\} =: g$ is a line of $\mathrm{PG}(2, 3)$, then the three–fold derived design $(W_{12})_{A,B,C}$ is an affine plane of order 3. It is immediate from the definition of blocks that this is just the affine plane $\mathcal{A}$ which arises from $\mathrm{PG}(2, 3)$ by removing the line g.

Each affinity α of $\mathcal{A}$ extends, on one hand, to a unique collineation κ of $\mathrm{PG}(2, 3)$ and, on the other hand, to a unique automorphism β of W_{12}.

For each $X \in g \setminus \{U\}$ there is a unique elliptic (i.e., fixed–point free) involution γ_X of g which interchanges X with U. We mention without proof that

$$X^{\beta} = U^{\kappa^{-1}\gamma_X\kappa}. \tag{10}$$

Thus X^{κ} and X^{β} need not coincide. Cf. also [3, Remark 6].

The discussion of other derivations of W_{12} in terms of the present planar model is left to the reader.

References

[1] Beth, Th., Jungnickel, D., and Lenz, H.: *Design Theory*. Mannheim Wien Zürich, BI Wissenschaftsverlag 1985.

[2] Coxeter, H.S.M.: *Twelve points in PG*$(5, 3)$ *with* 95040 *self–transformations*. Proc. Royal Soc. London A **427**, 279–293 (1958).

[3] Havlicek, H.: *The Veronese surface in* $\mathrm{PG}(5, 3)$ *and Witt's* 5–$(12, 6, 1)$ *design*. J. Comb. Theo. Ser. A. **84**, 87–94 (1998).

[4] Havlicek, H.: *Giuseppe Veronese and Ernst Witt – Neighbours in* $\mathrm{PG}(5, 3)$. Aequationes Math. **58**, 85–92 (1999).

[5] Hirschfeld, J.W.P.: *Projective Geometries over Finite Fields*. 2nd ed., Oxford, Clarendon Press 1998.

[6] Pellegrino, G.: *Su una interpretazione geometrica dei gruppi* M_{11} *ed* M_{12} *di Mathieu e su alcuni* t–(v, k, λ)–*disegni deducibili da una* $(12)^4_{5,3}$ *calotta completa*. Atti Sem. Mat. Fis. Univ. Modena **23**, 103–117 (1974).

Hans Havlicek, Abteilung für Lineare Algebra und Geometrie, Technische Universität, Wiedner Hauptstraße 8–10, A–1040 Wien, Austria.
EMAIL: `havlicek@geometrie.tuwien.ac.at`