Another Simple Proof for the Existence of the Small Witt Design

Hans Havlicek* Hanfried Lenz

Abstract

We give a short proof for the existence of the small Witt design which is based on the projective plane of order three with one point deleted.

1 Introduction

The Swiss geometer J. Steiner posed the following question ("Combinatorische Aufgabe") in 1853:

"Welche Zahl, N, von Elementen hat die Eigenschaft, dass sich die Elemente so zu dreien ordnen lassen, dass je zwei in einer, aber nur in einer Verbindung vorkommen?"

If we write v, k, and t instead of N, 3, and 2, respectively, then we arrive at the following contemporary definition: A *Steiner system* $S(t, k, v)$ is a finite set $\mathcal{V}$ of elements (called *points*) with a distinguished family of subsets (called *blocks*) such that the following holds true:

1. There are exactly v points in $\mathcal{V}$.
2. Each block has exactly k elements.
3. Any t distinct points belong to a unique block.

In order to avoid trivialities it is usually assumed that $2 \leq t < k < v$.

So Steiner asked for $S(2, 3, v)$ systems. As a matter of fact, T.P. Kirkman proved already in 1847 that an $S(2, 3, v)$ exists if, and only if, $v \equiv 1,\ 3 \pmod 6$.

In this short communication we present another proof for the existence of a Steiner system $S(5, 6, 12)$ which is also called *small Witt design* W_{12}. See [1] or [2], in particular Chapter IV. There the reader will also find the definition of a *t-design* (which is more general than that of a Steiner system) and references on other results mentioned in this section.

In an $S(5, 6, 12)$ there are twelve points, each block has exactly six elements, and any five distinct points are contained in a unique block. There is a unique $S(5, 6, 12)$ up to isomorphism. The same uniqueness property holds true for an $S(5, 8, 24)$ which carries the name

*Partially supported by the City of Vienna (*Hochschuljubiläumsstiftung der Stadt Wien, Projekt H-39/98.*)

large Witt design W_{24}. The Steiner systems W_{12} and W_{24} are due to E. Witt (1938) and R.D. Carmichel (1937). For many decades W_{12} and W_{24} were the only known Steiner systems with parameter $t = 5$. Even today only finitely many Steiner systems $S(t, k, v)$ with $t > 3$ and none with $t > 5$ seem to be known [3, 67], [7].

Another remarkable property of the two Witt designs concerns their automorphism group. Recall that a group G of permutations acts (sharply) t-transitively, if for two ordered t-tuples of elements there is a (unique) permutation in G taking the first to the second t-tuple. The automorphism groups of the Witt designs W_{12} and W_{24} act 5-transitively on their sets of points; for the small Witt design the action is even sharply 5-transitive. These automorphism groups are the *Mathieu groups* M_{12} and M_{24}, respectively. They were discovered by E. Mathieu in 1861 and 1873, and they are early examples of *sporadic finite simple groups*. The only finite t-transitive permutation groups with $t > 3$ other than symmetric and alternating groups that seem to be known are the two Mathieu groups mentioned above and two of their subgroups (the Mathieu groups M_{11} and M_{23}). So the Witt designs are indeed remarkable combinatorial structures.

The starting point of our construction of W_{12} is the projective plane of order three with point set $\mathcal{P}$. It is a Steiner system $S(2, 4, 13)$, but its blocks are called *lines*.

The first step is to discuss the 6-sets of points in $\mathcal{P}$. They fall into four classes which can be described in various ways, but the crucial observation is that two 6-sets are in the same class if and only if they have the same number of trisecants (i.e. lines meeting the set in exactly three points).

Next we choose one point of $\mathcal{P}$, say U. The twelve points of $\mathcal{W} := \mathcal{P} \setminus \{U\}$ will be the points of the Witt design W_{12}. We introduce three kinds of 6-subsets of $\mathcal{W}$ and call them blocks. Each block together with the distinguished point U has a complement in $\mathcal{P}$ with exactly six elements. So properties of 6-sets in $\mathcal{P}$ carry over to properties of blocks.

Finally, we show that $\mathcal{W}$, together with the set of all blocks, is a Steiner system $S(5, 6, 12)$. Again, the results on 6-sets of points turn out useful when showing that any 5-set $\mathcal{M} \subset \mathcal{W}$ is contained in a block, since $\mathcal{M} \cup \{U\}$ is a 6-set of points in the projective plane.

The proof presented in this paper is closely related to a projective representation, in the five-dimensional projective space of order three, of the small Witt design due to H.S.M. Coxeter [4]; see [5] and the references given there. Furthermore, we refer to [6] for an alternative description of the present construction of W_{12} using completely different methods.

2 Construction

Let $\mathcal{P}$ be the set of points of the projective plane of order three or, in other words, the Steiner system $S(2, 4, 13)$ [1, 19]. There are exactly 4 lines (blocks) through each point of $\mathcal{P}$. The unique line joining distinct points A and B will be written as AB.

First we introduce four types of sets $\mathcal{S} \subset \mathcal{P}$, each consisting of exactly six points.

1. $\mathcal{S}$ is the union of a line and two further points (fig. 1).

2. $\mathcal{S}$ is the symmetric difference of two different lines (fig. 2).

3. $\mathcal{S}$ consists of a triangle and an inscribed triangle, i.e. each point of the second triangle lies on exactly one line of the first triangle (fig. 3).

4. $\mathcal{S}$ is the set of vertices of a quadrilateral, i.e. the set of points where two distinct lines of the quadrilateral meet (fig. 4).

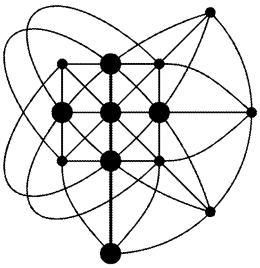

Fig. 1.

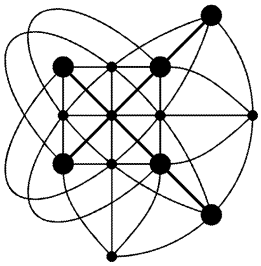

Fig. 2.

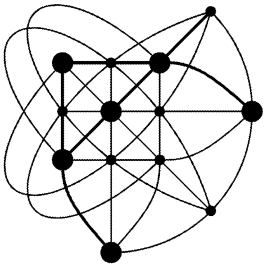

Fig. 3.

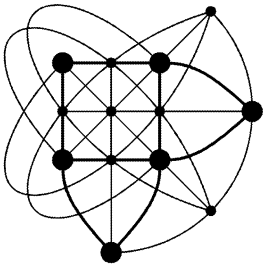

Fig. 4.

A set of type 1 contains a unique line. So there are exactly $13 \cdot \binom{9}{2} = 13 \cdot 36$ sets of type 1.
A set $\mathcal{S}$ of type 2 can be written as symmetric difference of two lines in one way only. Hence there are exactly $\frac{13 \cdot 12}{2!} = 13 \cdot 6$ sets of type 2.
If $\mathcal{S}$ is of type 3 then each vertex of the "basic" triangle is on exactly two trisecants of $\mathcal{S}$, whereas each point of the "inscribed" triangle is on one trisecant only. So the role of the two triangles is not the same. Since two distinct vertices of the inscribed triangle determine the remaining one uniquely, the number of 6-sets of type 3 is $\frac{13 \cdot 12 \cdot 9}{3!} \cdot 2 \cdot 2 = 13 \cdot 72$.
If $\mathcal{S}$ is of type 4 then the defining quadrilateral can be recovered from $\mathcal{S}$ as the set its four trisecants. So the number of sets of type 4 equals $\frac{13 \cdot 12 \cdot 9 \cdot 4}{4!} = 13 \cdot 18$.
We observe that a 6-set of type $i \in \{1, 2, 3, 4\}$ has exactly i trisecants. So the four types of 6-sets do not overlap. Finally, from

$$13 \cdot (36 + 6 + 72 + 18) = 13 \cdot 132 = \binom{13}{6},$$

our list from above comprises all 6-sets of points.
Let $U \in \mathcal{P}$ be a fixed point and put $\mathcal{W} := \mathcal{P} \setminus \{U\}$. A *block*, say $\mathcal{B}$, is defined to be a subset of $\mathcal{W}$ satisfying one of the following conditions:

A. $\mathcal{B}$ is the symmetric difference of two distinct lines, each not incident with U.

B. $\mathcal{B} \cup \{U\}$ is the union of two distinct lines.

C. $\mathcal{B}$ consists of a quadrangle together with two of its diagonal points; moreover, U is the remaining diagonal point.

If a block $\mathcal{B}$ is of type A, B, or C, then $\mathcal{P} \setminus (\mathcal{B} \cup \{U\})$ is easily seen to be a 6-set of type 1, 2 or 4, respectively. Thus the blocks fall into classes A, B, and C. Also, let us remark that the complement in $\mathcal{W}$ of a block of type A, B, or C is a block of type B, A, or C, respectively.

The number of blocks of type A is equal to the number of 2-sets of lines, both not running through U. So it is $\frac{9\cdot 8}{2} = 36$.

Blocks of type B are of the form $(a \cup b) \setminus \{U\}$ with lines $a \neq b$ and $U \in a \cup b$. Counting the possibilities for a and b, and taking into account whether U is on both lines or not, shows that there are precisely $4 \cdot 9 + \binom{4}{2} = 42$ blocks of type B.

We obtain all quadrangles with diagonal point U by drawing two distinct lines, say a and b, through U and choosing two distinct points on $a \setminus \{U\}$ and $b \setminus \{U\}$, respectively. So the number of blocks of type C equals $\binom{4}{2} \cdot \binom{3}{2} \cdot \binom{3}{2} = 54$.

Summing up shows that there are exactly 132 blocks.

Here is our main result:

Theorem 1 *The set $\mathcal{W}$, together with the set of all blocks, is a Steiner system $S(5, 6, 12)$.*

Proof: (a) By definition, all blocks have exactly 6 elements and $\#\mathcal{W} = 12$.

(b) We show that each 5-set $\mathcal{M}$ in $\mathcal{W}$ belongs to at least one block. There are four cases, depending on the type of the 6-set $\mathcal{S} := \mathcal{M} \cup \{U\}$:

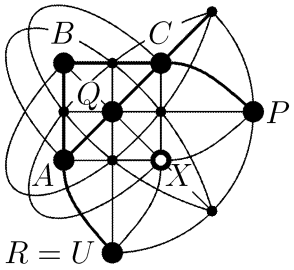

Fig. 5.

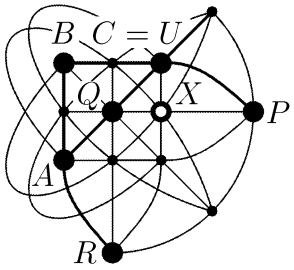

Fig. 6.

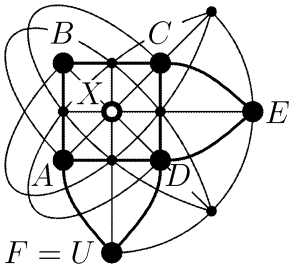

Fig. 7.

1. Suppose that $\mathcal{S}$ consists of a line a and two further points; let b be the line joining those points. Then $(a \cup b) \setminus \{U\}$ is a block of type B containing $\mathcal{M}$.

2. Let $\mathcal{S}$ be the symmetric difference of distinct lines a and b. Then $(a \cup b) \setminus \{U\}$ is a block of type B with the required property.

3. Let $\mathcal{S}$ be the union of a triangle $\{A, B, C\}$ and an inscribed triangle $\{P, Q, R\}$ such that $P \in BC$, $Q \in CA$, and $R \in AB$. There are two subcases:

   If $U \in \{P, Q, R\}$, say $R = U$, then put $\{X\} := AP \cap BQ$. Then $\{X\} \in CR$ and $\{A, B, C, X\}$ is a quadrangle with diagonal points P, Q, and $R = U$ which gives rise to a block of type C containing $\mathcal{M}$ (fig. 5).

   If $U \in \{A, B, C\}$, say $C = U$, then put $\{X\} := PQ \cap RU$. Then $U \notin AB \cup PQ$. So the symmetric difference of AB and PQ is a block of type A through $\mathcal{M}$ (fig. 6).

4. Let $\mathcal{S} = \{A, B, C, D, E, F\}$ be the set of vertices of a quadrangle. W.l.o.g. let $\{U\} = \{F\} = AB \cap CD$. So $\{A, B, C, D\}$ is a quadrangle with diagonal points E, $F = U$, and X, say. Therefore $\{A, B, C, D, E, X\} \supset \mathcal{M}$ is a block of type C (fig. 7).

(c) Given a 5-set $\mathcal{M} \subset \mathcal{W}$ then denote by $r(\mathcal{M})$ the number of blocks passing through it. Since each of the 132 blocks contains exactly 6 subsets of $\mathcal{W}$ with 5 elements, we obtain from the principle of counting in two ways that

$$\sum_{\substack{\mathcal{M}\subset\mathcal{W},\\ \#\mathcal{M}=5}} r(\mathcal{M}) = 132 \cdot 6 = 792.$$

From (b), $r(\mathcal{M}) \geq 1$ for each of the $\binom{12}{5} = 792$ sets $\mathcal{M}$ appearing in the sum above. So $r(\mathcal{M}) = 1$ is constant. This completes the proof. $\square$

References

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

[2] Th. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, 2nd ed., Cambridge, Cambridge University Press 1999.

[3] C.J. Colbourn and R. Mathon, Steiner Systems, in C.J. Colbourn and J.H. Dinitz (eds.), *The CRC Handbook of Combinatorial Designs*, Boca Raton, CRC Press 1996.

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

[5] H. Havlicek, Giuseppe Veronese and Ernst Witt — Neighbours in PG(5,3), *Aequationes Math.* 58 (1999), 85–92.

[6] H. Havlicek, A Model of the Witt Design W_{12} Based on Quadrics of PG(2,3), *Discrete Math.*, submitted.

[7] R. Mathon, Searching for Spreads and Packings, in J.W.P. Hirschfeld, S.S. Magliveras, and M.J. de Resimini (eds.), *Geometry, Combinatorial Designs and Related Structures*, London Math. Soc. Lect. Notes Ser. 245, Cambridge, Cambridge University Press, 1997.

Hans Havlicek, Institut für Geometrie, Technische Universität, Wiedner Hauptstraße 8–10, A–1040 Wien, Austria.

Hanfried Lenz, Mathematisches Institut II (WE2), Freie Universität Berlin, Arnimallee 3, D-14195 Berlin, Germany.