Extensions of PG(3, 2) with bases

Joseph L. Yucas

Department of Mathematics
Southern Illinois University-Carbondale
Carbondale, Il. 62901-4408
U.S.A.

Abstract

If one hopes to extend AG(4, 2) to an $S(4, 5, 17)$, an extension of PG(3, 2) with bases is necessary. A geometric construction of such an extension of PG(3, 2) is given along with some remarks on further extending AG(4, 2) to an $S(4, 5, 17)$.

1 Introduction

A t-(v, k, λ)-*design* is a pair (**P**,**B**) where **P** is a v-element set of *points* and **B** is a collection of k-subsets of **P** called *blocks* such that every t-element subset of **P** is contained in exactly λ blocks. If the t is omitted we assume $t = 2$. If $\lambda = 1$ then the design is called a *Steiner system* and denoted by $S(t, k, v)$.

If $\mathbf{D} = (\mathbf{P},\mathbf{B})$ is an $S(t, k, v)$ and p is a point of **D** then the pair $\mathbf{D}_p$ consisting of the point set $\mathbf{P} - \{p\}$ with blocks $\{B - \{p\} | p \in B \in \mathbf{B}\}$ is an $S(t - 1, k - 1, v - 1)$ called the Steiner system derived from **D** with respect to p. In this case we say that **D** is an extension of $\mathbf{D}_p$. Basic results and terminology on Design Theory can be found in [2], [3] and [4].

Let **V** be a 4-dimensional vector space over GF(2). The 15 non-zero vectors of **V** together with the 35 blocks of the form $\{\alpha, \beta, \alpha + \beta\}$ form an $S(2, 3, 15)$, denoted PG(3, 2). This is the design coming from the 3-dimensional projective geometry over GF(2). The blocks of PG(3, 2) will be called *lines*. The non-zero vectors of 3-dimensional subspaces of **V** will be called *planes*.

It is well-know that PG(3, 2) can be extended to an $S(3, 4, 16)$. One simply adds a new point, say 0, to the fifteen points of PG(3, 2) and takes as blocks all sets of the form $\{\ell \cup \{0\} \mid \ell$ is a line of PG(3, 2)$\}$ and all sets of the form $\{\pi - \ell \mid \pi$ is a plane of PG(3, 2), ℓ is a line of PG(3, 2) and $\ell \subset \pi\}$. This extension comes from the 4-dimensional affine geometry over GF(2) and will be denoted by AG(4, 2). Equivalently, AG(4, 2) is the collection of all cosets of all 2-dimensional subspaces of **V**. The sets $\pi - \ell$ have the form $\{\alpha, \beta, \gamma, \alpha + \beta + \gamma\}$ where α, β, γ are linearly independent. These are called *ovals*. The main concern of this paper will be with the construction of a different type of $S(3,4,16)$ extending $\mathrm{PG}(3,2)$.

It is not yet known whether a Steiner system $S(4,5,17)$ exists. A Steiner system $S(4,5,17)$ would have 476 blocks, each point occurring 140 times, each pair of points occurring 35 times and each triple occurring 7 times. One possible way of constructing such a Steiner system of course would be to extend $\mathrm{AG}(4,2)$. In order to extend $\mathrm{AG}(4,2)$ we must add a point, say ∞, to $\mathbf{V}$ and then add ∞ to each of the 140 blocks of $\mathrm{AG}(4,2)$. The 35 blocks of the form $\{0, \alpha, \beta, \alpha+\beta, \infty\}$ will be called *projective sets*. The 105 blocks of the form $\{\alpha, \beta, \gamma, \alpha+\beta+\gamma, \infty\}$ will be called *oval sets*.

There are then 336 new blocks of size 5 that need to be constructed. The point ∞ already occurs 140 times so it cannot occur again. The point 0 occurs 35 times in the projective sets and does not appear at all in the oval sets. Consequently, 0 must occur 105 more times. Since the 105 ovals and the 35 4-tuples of the form $\ell \cup \{0\}$ already occur, these remaining 105 blocks containing 0 must have the form $\{0, \alpha, \beta, \gamma, \delta\}$ where $\{\alpha, \beta, \gamma, \delta\}$ is a basis for $\mathbf{V}$. We will call these *basis sets*.

Notice that if this extension of $\mathrm{AG}(4,2)$ does exist then the derived design with respect to 0 is an $S(3,4,16)$ on $(\mathbf{V}\backslash\{0\}) \cup \{\infty\}$. Now, the projective sets contain both 0 and ∞. Consequently, the 105 bases in the basis sets must extend $\mathrm{PG}(3,2)$ to an $S(3,4,16)$ on $(\mathbf{V}\backslash\{0\}) \cup \{\infty\}$. It is this extension with which we are concerned here. In [1] we showed, under a certain uniformity condition, that this extension could not exist. Surprisingly, V. Tonchev [5], with a computer search, found 105 basis sets not satisfying this uniformity condition. In the next section we give a geometric construction of a family of such basis sets. Tonchev's example is one of these. It would be interesting to know if there are other non-isomorphic extensions of $\mathrm{PG}(3,2)$ containing 105 basis sets. Finally, in the third section, we give some remarks on then extending $\mathrm{AG}(4,2)$ to an $S(4,5,17)$.

2 The Basis Sets

In this section we extend $\mathrm{PG}(3,2)$ to an $S(3,4,16)$ whose new blocks are bases for $\mathbf{V}$. Fix a plane $\mathbf{\Pi}$ of $\mathrm{PG}(3,2)$ and let $\mathbf{L}$ be the collection consisting of the 7 lines of $\mathbf{\Pi}$. Let $\phi : \mathbf{\Pi} \longrightarrow \mathbf{L}$ be any bijection acting on the points of $\mathbf{\Pi}$ satisfying:

$$\alpha \in \phi(\beta) \Longrightarrow \beta \notin \phi(\alpha).$$

Example 2.1 Such bijections do exist. For example, fix a basis $\{\alpha_1, \alpha_2, \alpha_3\}$ for $\mathbf{\Pi}$. Define ϕ by:

α_1	$\longrightarrow$	α_2	α_3	$\alpha_2+\alpha_3$
α_2	$\longrightarrow$	α_3	$\alpha_1+\alpha_2$	$\alpha_1+\alpha_2+\alpha_3$
α_3	$\longrightarrow$	$\alpha_1+\alpha_2$	$\alpha_1+\alpha_3$	$\alpha_2+\alpha_3$
$\alpha_1+\alpha_2$	$\longrightarrow$	α_1	$\alpha_2+\alpha_3$	$\alpha_1+\alpha_2+\alpha_3$
$\alpha_1+\alpha_3$	$\longrightarrow$	α_1	α_2	$\alpha_1+\alpha_2$
$\alpha_2+\alpha_3$	$\longrightarrow$	α_2	$\alpha_1+\alpha_3$	$\alpha_1+\alpha_2+\alpha_3$
$\alpha_1+\alpha_2+\alpha_3$	$\longrightarrow$	α_1	α_3	$\alpha_1+\alpha_3$

Proposition 2.2 (i) $\alpha \notin \phi(\alpha)$. (ii) If $\alpha \neq \beta$ and $\alpha \notin \phi(\beta)$ then $\beta \in \phi(\alpha)$.

Proof: (i) is clear; for (ii) suppose $\alpha \notin \phi(\beta)$. By (i), $\beta \notin \phi(\beta)$. There are only two lines in $\mathbf{L}$ not containing α or β. Call these lines l_1 and l_2 and suppose $\phi(\beta) = l_1$. Assume $\beta \notin \phi(\alpha)$. By (i) and the fact that ϕ is a bijection we have $\phi(\alpha) = l_2$. Both l_1 and l_2 contain $\alpha + \beta$ hence $\alpha, \beta \notin \phi(\alpha + \beta)$. Consequently, $\phi(\alpha + \beta) = \phi(\alpha)$ or $\phi(\beta)$ contradicting ϕ being a bijection.

Proposition 2.3 If a point p is on a line $\phi(q)$ and if $\phi(p) \cap \phi(q)$ is known then ϕ can be completely determined.

Proof: Suppose $\phi(p) \cap \phi(q) = \{i\}$. We show that ϕ is given by:

$$\begin{array}{lllll}
q & \longrightarrow & i & p & p+i \\
p & \longrightarrow & i & q+p+i & q+p \\
p+q & \longrightarrow & q & p+i & q+p+i \\
i & \longrightarrow & p+q & p+i & q+i \\
p+i & \longrightarrow & p & p+q+i & q+i \\
q+i & \longrightarrow & p & q & p+q \\
p+q+i & \longrightarrow & q & q+i & i
\end{array}$$

To begin we have $i, p \in \phi(q)$, hence $\phi(q) = \{i, p, p+i\}$. Now, $p, q \notin \phi(p)$ so this leaves only two possible lines of $\mathbf{\Pi}$ for $\phi(p)$. Both of these lines contain $p+q$. Consequently, $\phi(p) = \{i, p+q, p+q+i\}$. The other five lines are determined by using Proposition 2.2(ii). For example, $p+q, q+i, p+q+i \notin \phi(q)$ implies $q \in \phi(p+q), q \in \phi(q+i)$ and $q \in \phi(p+q+i)$.

Fix a point outside of $\mathbf{\Pi}$. Throughout, this point will be denoted by x. From each point $p \in \mathbf{\Pi}$, we construct six bases of $\mathbf{V}$. Suppose $\phi(p) = \{\alpha, \beta, \alpha+\beta\}$. The bases are the rows of the following array:

$$\begin{array}{llll}
\alpha & \beta & x+\alpha+\beta & p+\alpha+\beta \\
\alpha & \alpha+\beta & x+\beta & p+\beta \\
\beta & \alpha+\beta & x+\alpha & p+\alpha \\
x & p+\alpha & p+\beta & p+\alpha+\beta \\
p & x+p+\alpha & x+p+\beta & x+p+\alpha+\beta \\
x+p & x+\alpha & x+\beta & x+\alpha+\beta
\end{array}$$

Since $\{p, \alpha, \beta, x\}$ is a basis for $\mathbf{V}$, it is easy to see that these six rows are also. This gives us 42 of the 105 bases we desire.

From a pair p, q, of distinct points of $\mathbf{\Pi}$ we derive three more bases of $\mathbf{V}$. By Proposition 2.2(ii), either $p \in \phi(q)$ or $q \in \phi(p)$. Say $p \in \phi(q)$. Let $\phi(p) \cap \phi(q) = \{i\}$ and consider the rows of the following array:

p	$p+x$	$q+x$	$q+i$
q	$p+q+i$	$i+x$	$p+q+i+x$
x	$p+x$	$p+q$	$p+i+x$

Again, since $\{p,q,i,x\}$ is a basis for $\mathbf{V}$ so are these rows. This gives us the $3 \cdot C(7,2) = 63$ other bases we need.

Theorem 2.4 The 105 bases for $\mathbf{V}$ constructed above extends PG$(3,2)$ to an $S(3,4,16)$ on $(\mathbf{V}\backslash\{0\}) \cup \{\infty\}$.

Proof: Since each line occurs exactly once in PG$(3,2)$ it suffices to show that each triple of linearly independent points occurs exactly once within the 105 bases. We have $105 \cdot C(4,3) = 420$ of these triples occurring and there is a total of $C(15,3) - 35 = 420$ of these triples. Hence we show that the triples occurring are distinct. Listed below are the various types of triples that we have occurring. The first group lists the triples containing x. The second group lists the triples containing three points from $\mathbf{\Pi}$. The third group lists all triples containing three points outside $\mathbf{\Pi}$ none of which is x. The fourth group lists all triples containing exactly one point of $\mathbf{\Pi}$ and not x and the fifth group lists the triples containing exactly two points from $\mathbf{\Pi}$ but not containing x. In all cases α and β are points in $\phi(p)$.

1

x	$p+x$	$p+q$
x	$p+x$	$p+i+x$
x	$p+q$	$p+i+x$
x	$p+\alpha$	$p+\beta$

2

α	β	$p+\alpha+\beta$
$p+\alpha$	$p+\beta$	$p+\alpha+\beta$

3

$x+p+\alpha$	$x+p+\beta$	$x+p+\alpha+\beta$
$x+p$	$x+\alpha$	$x+\beta$
$x+\alpha$	$x+\beta$	$x+\alpha+\beta$

4

$p+x$	$q+x$	p
$p+x$	$q+x$	$q+i$
$i+x$	$p+q+i+x$	q
$i+x$	$p+q+i+x$	$p+q+i$
$p+x$	$p+i+x$	$p+q$
$x+p+\alpha$	$x+p+\beta$	p

5

p	$q+i$	$p+x$
p	$q+i$	$q+x$
q	$p+q+i$	$i+x$
q	$p+q+i$	$p+q+i+x$
α	β	$\alpha+\beta+x$
α	$p+\alpha+\beta$	$\alpha+\beta+x$
α	$\alpha+\beta$	$x+\beta$
α	$p+\beta$	$x+\beta$

Notice that triples from different groups cannot be equal. But, there are still several cases involving triples from within a group. Each case is simple, however, just depending on Propositions 2.2 and 2.3. We provide proofs of some representative cases and leave the remaining cases for the reader.

Case(i) Suppose $\{x, p_1 + x, p_1 + q_1\} = \{x, p_2 + q_2, p_2 + i_2 + x\}$. Here $p_1 = p_2 + i_2$ and $p_1 + q_1 = p_2 + q_2$. By Proposition 2.3, with $p = p_2$ and $q = q_2$, we have $p_2 + i_2 \in \phi(p_2 + q_2) = \phi(p_1 + q_1)$. With $p = p_1$ and $q = q_1$, we have $p_2 + i_2 = p_1 \notin \phi(p_1 + q_1)$. This is a contradiction.

Case(ii) Suppose $\{\alpha_1, \beta_1, p_1 + \alpha_1 + \beta_1\} = \{p_2 + \alpha_2, p_2 + \beta_2, p_2 + \alpha_2 + \beta_2\}$. Assume first that $\alpha_1 = p_2 + \alpha_2, \beta_1 = p_2 + \beta_2$ and $p_1 + \alpha_1 + \beta_1 = p_2 + \alpha_2 + \beta_2$. Then $p_2 + \alpha_2 + \beta_2 = p_1 + \alpha_1 + \beta_1 = p_1 + p_2 + \alpha_2 + p_2 + \beta_2 = p_1 + \alpha_2 + \beta_2$. Hence $p_1 = p_2$. Now $\alpha_1 \in \phi(p_1) = \phi(p_2)$ implies $\alpha_1 \in \{\alpha_2, \beta_2, \alpha_2 + \beta_2\}$. If $\alpha_1 = \alpha_2$ then $p_2 = 0$, a contradiction. If $\alpha_1 = \beta_2$ then $p_1 = p_2 = \beta_1 + \alpha_1 \in \phi(p_1)$, a contradiction. If $\alpha_1 = \alpha_2 + \beta_2$ then $\beta_1 = 0$, a contradiction. The other subcases are similar.

Case(iii) Suppose $\{x+p_1+\alpha_1, x+p_1+\beta_1, x+p_1+\alpha_1+\beta_1\} = \{x+p_2, x+\alpha_2, x+\beta_2\}$. Assume first that $p_1+\alpha_1 = p_2, p_1+\beta_1 = \alpha_2$ and $p_1+\alpha_1+\beta_1 = \beta_2$. Then $\alpha_1 = p_2+p_1 \neq p_2, \beta_1 = p_1 + \alpha_2 = \alpha_1 + p_2 + \alpha_2 \neq p_2$ and $\alpha_1 + \beta_1 = p_2 + p_1 + p_1 + \alpha_2 = p_2 + \alpha_2 \neq p_2$. Hence, $p_2 \notin \phi(p_1)$, and thus $p_1 \in \phi(p_2)$. If $p_1 = \alpha_2$ then $\beta_1 = 0$, a contradiction. If $p_1 = \beta_2$ then $\alpha_1 = \beta_1$, a contradiction. If $p_1 = \alpha_2 + \beta_2$ then $p_1 = \alpha_1 \in \phi(p_1)$, a contradiction. The other subcases are similar.

Case(iv) Suppose $\{p_1 + x, q_1 + x, p_1\} = \{p_2 + x, p_2 + i_2 + x, p_2 + q_2\}$. Then $p_1 = p_2 + q_2$ and $\{p_1, q_1\} = \{p_2, p_2 + i_2\}$. If $p_1 = p_2$ then $q_2 = 0$, a contradiction. If $p_1 = p_2 + i_2$ then $p_2 + q_2 = p_2 + i_2$ and hence $q_2 = i_2 \in \phi(q_2)$, a contradiction.

Case(v) Suppose $\{p_1, q_1 + i_1, p_1 + x\} = \{q_2, p_2 + q_2 + i_2, p_2 + q_2 + i_2 + x\}$. Here $p_1 = p_2 + q_2 + i_2$ and $\{p_1, q_1 + i_1\} = \{q_2, p_2 + q_2 + i_2\}$. If $q_2 = p_1$ then $p_2 = i_2 \in \phi(p_2)$, a contradiction. If $q_2 = q_1 + i_1$ then by Proposition 2.3, $\phi(q_2) = \phi(q_1 + i_1) = \{p_1, q_1, p_1 + q_1\}$. On the other hand, $\phi(q_2) = \{p_2, i_2, p_2 + i_2\}$. If $p_1 = p_2$ then $q_2 = i_2 \in \phi(q_2)$, a contradiction. If $p_1 = i_2$ then $p_2 = q_2$, a contradiction. Finally, if $p_1 = p_2 + i_2$ then $q_2 = 0$, a contradiction.

3 Line sets and ovoid sets

We begin this section with some results observed by A. Baartmans and the author when working on [1] which were not needed and hence not published there. Continue with our hypothetical extension of AG(4, 2) to an $S(4, 5, 17)$. So far we have seen that it must contain 35 projective sets, 105 oval sets, and 105 basis sets. There are still 231 blocks to consider.

In our extension, a line $\ell = \{\alpha, \beta, \alpha + \beta\}$ occurs once so far, so it must occur 6 more times. We have then blocks of the form $\{\alpha, \beta, \alpha+\beta, \gamma, \delta\}$. Notice that δ cannot be linearly dependent on α, β and γ for otherwise this block would contain an oval which already appears in the oval sets. Consequently, we must have $35 \cdot 6 = 210$ blocks of this form with $\{\alpha, \beta, \gamma, \delta\}$ being a basis for $\mathbf{V}$. We will call these *line sets*.

There are still 21 blocks unaccounted for. Now, there are 840 bases for $\mathbf{V}$ with 105 of them appearing in the basis sets and $210 \cdot 3 = 630$ of them appearing in the line sets. Consequently, we must cover 105 bases with 21 blocks. The only way to do this is to have the 21 blocks covering 5 bases each. This can be done only with ovoids; that is, with blocks of the form $\{\alpha, \beta, \gamma, \delta, \alpha+\beta+\gamma+\delta\}$ where $\{\alpha, \beta, \gamma, \delta\}$ is a basis for $\mathbf{V}$. These 21 blocks will be called *ovoid sets*.

In summary,

Theorem 3.1 If an extension of AG(4, 2) exists it must consist of the following five types of blocks:

(*i*) 35 *projective sets*;
(*ii*) 105 *oval sets*;
(*iii*) 105 *basis sets*;
(*iv*) 210 *line sets*;
(*v*) 21 *ovoid sets*.

Now, a nonzero vector α of $\mathbf{V}$ occurs in 7 lines of PG(3, 2). Since each line must occur 6 times in the line sets, α occurs 42 times in the line sets as a point on the line. Consider the 6 line sets containing a given line ℓ with $\alpha \notin \ell$. Each of these line sets contains 2 points not on ℓ, 12 points total in the 6 line sets. Now, there are 12 points not on ℓ. A point not on ℓ cannot appear twice in these 6 line sets for otherwise a 4-tuple would be repeated. Consequently, α must occur exactly once in these line sets. Since α is not on 28 lines, we see that α occurs 28 times in the line sets as a point not on the line. We have:

Proposition 3.2 The 210 line sets must form a 1-(15, 5, 70)-design.

We now know that a nonzero vector of $\mathbf{V}$ occurs 7 times in the projective sets, 28 in the oval sets, 28 in the basis sets, and 70 times in the line sets. It must occur 140 times total, hence we have:

Proposition 3.3 The 21 ovoid sets must form a 1-(15, 5, 7)-design.

Notice that the ovoid sets cannot form a 2-design. It would be a 2-(15, 5, 2)-design. This is a residual of a symmetric (22, 7, 2)-design which does not exist (see[3]). A pair of non-zero vectors of $\mathbf{V}$ must occur 35 times in an $S(4, 5, 17)$. Since each pair occurs once in the projective sets, 6 times in the oval sets, and 6 times in the basis sets, pairs cannot occur the same number of times in the line sets since then they are forced to occur the same number of times in the ovoid sets. Consequently, the line sets cannot form a 2-design either. It may be that the existence of an $S(4, 5, 17)$ implies the existence of a (15, 5, 2)-design thus explaining the non-existence of an $S(4, 5, 17)$.

However, we end on a brighter note and give a possible strategy for the construction of the line sets and ovoid sets. There are 168 ovoids. 21 of these must be chosen for the ovoid sets. The basis sets eliminate 105 of these ovoids from consideration for else a 4-tuple would occur twice. Consequently, 21 ovoids must be chosen from the remaining 63. Which ones to choose is the first problem. Once these are chosen, the remaining 42 ovoids contain 5 bases each, none of which appeared so far. Hence, they must appear in the line sets. This observation leads to a possible construction of the line sets.

Consider one of these 42 remaining ovoids, say $\{\alpha, \beta, \gamma, \delta, \alpha+\beta+\gamma+\delta\}$. Since each 4-tuple contained in this ovoid must appear in the line sets we must have 5 line sets with the following form:

α	β	γ	δ	$------$
α	β	γ	$\alpha+\beta+\gamma+\delta$	$------$
α	β	δ	$\alpha+\beta+\gamma+\delta$	$------$
α	γ	δ	$\alpha+\beta+\gamma+\delta$	$------$
β	γ	δ	$\alpha+\beta+\gamma+\delta$	$------$

The second problem is then how to fill in the $-----$s. To be line sets each blank must be filled in with the sum of two of the previous four. There are six possibilities for each, and we must keep in mind that we want each line occurring exactly 6 times in the line sets. If this can be accomplished then we have the $42 \cdot 5 = 210$ line sets that we desire.

References

[1] A. Baartmans and J. Yucas, On the existence of a double extension of PG(3, 2), *Ars Combinatoria* 33 (1992), 145–156.

[2] T. Beth, D. Jungnickel and H. Lenz, “Design Theory”, Cambridge University Press, Zurich, 1986.

[3] M. Hall Jr., “Combinatorial Theory”, Wiley-Interscience, New York, 1986.

[4] D. Hughes and F. Piper, “Design Theory”, Cambridge University Press, New York, 1985.

[5] V. Tonchev, Private communication.

(Received 1 Dec 2000)