On perpendicular arrays with $t \geq 3$

Earl S. Kramer, Donald L. Kreher, Rolf Rees and Douglas R. Stinson[1]

Abstract. We begin an investigation of perpendicular arrays with $t \geq 3$, and determine some necessary and sufficient conditions for existence. In particular, a perpendicular array $PA_3(3,4,v)$ exists for all $v \geq 4$.

1. Introduction

A perpendicular array $PA_\lambda(t,k,v)$ is a $\lambda\binom{v}{t}$ by k array, A, of the symbols $\{1,\cdots,v\}$, which satisfies the following properties:

i) every row of A contains k distinct symbols
ii) for any t columns of A, and for any t distinct symbols $x_i(1 \leq i \leq t)$, there are exactly λ rows of A that contain every $x_i(1 \leq i \leq t)$.

Notice that property ii) implies property i) if $t \geq 2$. We also note that property i) implies that $k \leq v$ in a perpendicular array. Finally, observe that if we delete any $k-j$ columns from a $PA_\lambda(t,k,v)$, we obtain a $PA_\lambda(t,j,v)$.

The arrays $PA_1(2,k,v)$ have been investigated by several researchers in combinatorial design theory (see for example [3], [10], [11], [13]). In this paper, we begin an investigation of the arrays $PA_\lambda(t,k,v), t \geq 3$. In particular, the spectrum of $PA_3(3,4,v)$ is completely determined.

Let's first determine some necessary conditions for the existence of a $PA_\lambda(t,k,v)$.

Theorem 1.1. *Suppose* $0 \leq t' \leq t$ *and* $\binom{k}{t} \geq \binom{k}{t'}$. *Then, a* $PA_\lambda(t,k,v)$ *is also a* $PA_\mu(t',k,v)$, *where*

$$\mu = \lambda\binom{v-t'}{t-t'}/\binom{t}{t'}$$

Hence,

$$\lambda\binom{v-t'}{t-t'} \equiv 0 \text{ modulo } \binom{t}{t'}.$$

Proof: Let A be a $PA_\lambda(t,k,v)$, and name the columns by $1,\cdots,k$. Let Y be any set of t' distinct symbols. For any set J' of t' columns, define $I(J')$ to be the number of rows of A in which the symbols in Y are all contained in the columns in J'. We obtain some linear equations in the $I(J')$ as follows. For any set J of t columns, we get an equation

$$\sum_{J' \subseteq J, |J'|=t'} I(J') = \lambda\binom{v-t'}{t-t'}.$$

[1]This research was supported in part by the Institute for Mathematics and its Application with funds provided by the National Science Foundation
Research of D.L. Kreher supported by National Science Foundation grant CCR-8711229
Research of R. Rees supported by NSERC operating grant P36507
Research of D.R. Stinson supported by NSERC operating grant A9287

In this way we get $\binom{k}{t}$ equations in $\binom{k}{t'}$ unknowns. If $\binom{k}{t} \geq \binom{k}{t'}$, then the system has the unique solution

$$I(J') = \lambda \binom{v-t'}{t-t'} / \binom{t}{t'}$$

for every J'. Consequently, A is a $PA_\mu(t', k, v)$, where μ is as above. ∎

Corollary 1.2. *If a $PA_1(2,3,v)$ exists, then v is odd.*

Corollary 1.3. *If a $PA_1(3,4,v)$ exists, then $v \equiv 1$ or 2 modulo 3. If a $PA_1(3,5,v)$ exists, then $v \equiv 2$ modulo 3.*

The following observations are immediate.

Theorem 1.4. *A $PA_\lambda(t,v,v)$ is also a $PA_\lambda(v-t,v,v)$.*

Theorem 1.5. *For all v, there exists a $PA_1(1,v,v)$ and a $PA_1(v-1,v,v)$.*

Proof: A $PA_1(1,v,v)$ is a Latin square of order v. By Theorem 1.4, it is also a $PA_1(v-1,v,v)$. ∎

2. Recursive constructions for $PA_\lambda(t,k,v)$

Let v and t be positive integers, and let $K \subseteq \{t, \cdots, v-1\}$. A (v, K, λ)-tBD (*t-wise balanced design*) is a pair $(X, \mathcal{B})$, where X is a set of v elements (called *points*) and $\mathcal{B}$ is a collection of subsets of X (called *blocks*), such that every (unordered) t-subset of points occurs in exactly λ blocks $B \in \mathcal{B}$, and $|B| \in K$ for every $B \in \mathcal{B}$. In the case $K = \{k\}$, a $(v,\{k\},\lambda)$-tBD is also denoted $S_\lambda(t,k,v)$.

Our main recursive construction for PAs uses tBDs, as follows.

Construction 2.1. *(tBD Construction) Suppose $(X, \mathcal{B})$ is a (v, K, λ)-tBD, and for every $n \in K$, suppose there exists a $PA_\mu(t,k,n)$. Then we can construct a $PA_{\lambda\mu}(t,k,v)$, by taking a $PA_\mu(t,k,|B|)$ on symbol set B, for every $B \in \mathcal{B}$.*

Using the PAs constructed in Theorem 1.5, we have the following.

Theorem 2.2. *Suppose there is an $S_\lambda(k-1,k,v)$. Then there is a $PA_\lambda(k-1,k,v)$.*

As a corollary, we can obtain the following infinite class of $PA_{15}(5,6,v)$.

Theorem 2.3. *For all $a \geq 2$, there is a $PA_{15}(5,6,2^\alpha+2)$.*

Proof: Jungnickel and Vanstone have shown in [9] that there is an $S_{15}(5,6,2^\alpha+2)$ for all $\alpha \geq 2$. ∎

Examples of $PA_1(k-1,k,v)$ can be obtained whenever a Steiner system $S_1(k-1,k,v)$ is known to exist. For example, we have the following results.

Theorem 2.4. *There exists a* $PA_1(k-1,k,v)$ *whenever* $(k,v) = (5,11),(6,12),(5,23),(6,24),(5,47),(6,48),(5,83),(6,84),(5,71),$ *or* $(6,72)$.

Proof: The corresponding Steiner systems all exist ([1], [12], [15]). ∎

3. The arrays $PA_\lambda(3,k,v)$

In this section, we investigate the existence of $PA_1(3,4,v)$ and $PA_3(3,4,v)$. First, we give several examples of small arrays. In some of the following examples, we use some notation to economize the listing of starting blocks; namely, let $C(x_1,x_2,\cdots,x_k)$ represent the k cyclic shifts of the row $x_1x_2\cdots x_k$.

Example 3.1: A $PA_1(3,4,4)$. Develop the following row modulo 4.

0	1	2	3

Example 3.2: A $PA_1(3,5,5)$. Develop the following rows modulo 5.

0	1	2	3	4	0	2	4	1	3

Example 3.3: A $PA_3(3,6,6)$. Develop the following 12 rows modulo 5.

$$C(x\ \ 0\ \ 1\ \ 2\ \ 4\ \ 3) \qquad C(x\ \ 0\ \ 2\ \ 4\ \ 3\ \ 1)$$

Example 3.4: A $PA_1(3,4,7)$. Develop the following rows modulo 5.

x	y	0	1	0	2	x	y
0	x	1	3	y	0	1	4
0	1	2	x	0	2	y	4
0	1	3	4				

Example 3.5: A $PA_1(3,8,8)$ [14]. Develop the following rows modulo 7.

x	0	1	2	3	4	5	6	0	x	3	6	1	5	4	2
1	3	x	4	0	2	6	5	2	6	4	x	5	1	3	0
3	1	0	5	x	6	2	4	4	5	2	1	6	x	0	3
5	4	6	3	2	0	x	1	6	2	5	0	4	3	1	x

Remark: This PA has $AGL(1,8)$ as its automorphism group.

Example 3.6: A $PA_3(3,4,9)$. This is constructed by applying the tBD construction to a $(9,\{4,5\},3)$-$3BD$. To construct the $3BD$, take three copies of an $S_1(3,4,8)$, and adjoin a new point ∞ to all the blocks of one of these $S_1(3,4,8)$.

Example 3.7: A $PA_1(3,4,11)$. Obtain 15 rows by multiplying each row by all quadratic residues in Z_{11}. Then, develop modulo 11.

2	0	1	6	0	1	7	3
3	7	1	0				

Example 3.8: A $PA_1(3,4,13)$. Develop the following 26 blocks modulo 11, (i.e. points 12 and 13 are fixed).

1	2	5	6	1	5	6	12	1	10	5	3	1	13	10	2
1	2	6	7	1	6	3	8	1	11	6	8	12	1	6	2
1	2	9	5	1	6	4	10	1	11	12	9	12	4	2	1
1	2	11	3	1	6	9	3	1	11	13	7	13	1	5	3
1	3	8	9	1	8	4	5	1	12	4	7	13	1	12	6
1	4	2	13	1	9	13	4	1	12	5	13				
1	4	3	2	1	10	3	12	1	13	7	8				

Example 3.9: A $PA_3(3,4,15)$. Develop the following 91 blocks modulo 15.

1	2	7	8	1	4	2	5	1	6	12	11	1	11	13	8
1	2	7	9	1	4	2	11	1	7	2	11	1	11	14	12
1	2	8	10	1	4	2	14	1	7	8	15	1	12	3	13
1	2	9	11	1	4	3	2	1	7	9	11	1	12	6	13
1	2	9	13	1	4	5	10	1	7	10	2	1	12	7	11
1	2	9	14	1	4	7	10	1	7	12	3	1	12	8	2
1	2	10	12	1	4	7	12	1	7	12	9	1	12	8	7
1	2	10	14	1	4	8	11	1	7	15	12	1	12	11	10
1	2	11	13	1	4	8	12	1	8	5	4	1	12	13	14
1	2	12	14	1	4	9	2	1	8	11	12	1	13	2	4
1	2	13	10	1	4	10	9	1	8	14	15	1	13	5	14
1	2	14	11	1	4	15	13	1	9	3	5	1	13	8	9
1	3	4	9	1	5	3	13	1	9	4	8	1	13	10	11
1	3	5	11	1	5	6	2	1	9	6	3	1	13	12	4
1	3	5	12	1	5	7	3	1	9	6	5	1	14	10	15
1	3	7	9	1	5	8	6	1	9	11	4	1	14	11	5
1	3	7	10	1	5	12	13	1	9	13	11	1	14	11	15
1	3	7	11	1	6	2	14	1	9	14	7	1	14	15	6
1	3	8	12	1	6	3	8	1	10	4	2	1	14	15	12
1	3	8	13	1	6	3	12	1	10	9	7	1	15	5	2
1	3	9	12	1	6	7	10	1	10	15	11	1	15	11	6
1	3	9	13	1	6	8	2	1	11	3	2	1	15	14	7
1	3	10	13	1	6	11	3	1	11	7	4				

Example 3.10: A $PA_3(3,4,19)$. Multiply each of the following rows by the quadratic residues in Z_{19}, i.e. apply powers of the permutation (1 4 16 7 9 17 11 6 5)(2 8 13 14 18 15 3 12 10) to get $17 \cdot 9$ rows. Then develop modulo 19.

C(1	2	3	13)	1	5	2	4	1	13	18	19
C(1	2	5	14)	1	8	6	5	1	18	17	16
1	2	3	8	1	9	18	19	1	19	15	3
1	2	3	11	1	13	14	16				

Example 3.11: A $PA_1(3,4,23)$. Obtain 77 rows by multiplying each row by all quadratic residues in Z_{23}. Then, develop modulo 23.

11	0	1	5	4	3	0	1
0	2	1	5	0	1	14	5
2	0	19	1	1	0	4	18
5	0	1	22				

Example 3.12: A $PA_3(3,4,27)$. Let G be the group generated by (1 3 5 7 9 11 13 15 17 19 21 23 25)(2 4 6 8 10 12 14 16 18 20 22 24 26)(27) and (1 3 9)(2 12 21)(4 7 18) (5 20 17)(6 10 11)(8 25 15)(13 26 27)(14 22 16) (19 24 23). Then G is a group of order $27 \cdot 13$. Let G act on the following 25 rows

C(1	2	3	12)	1	2	23	3	1	15	7	2
C(1	2	3	15)	1	2	24	5	1	17	5	15
C(1	2	5	21)	1	4	2	5	1	23	24	2
C(1	2	7	16)	1	7	13	16				
1	2	6	7	1	12	15	7				

Example 3.13: A $PA_3(3,4,31)$. Let the permutation (1 9 19 16 20 25 8 10 28 4 5 14 2 18 7) (3 27 26 17 29 13 24 30 22 12 15 11 6 23 21)(31) act on the following 29 rows, yielding $29 \cdot 15$ rows. Then develop modulo 31.

C(1	2	3	16)	1	2	3	7	1	7	8	6
C(1	2	3	19)	1	2	7	31	1	28	2	3
C(1	2	4	5)	1	2	27	28	1	31	3	13
C(1	2	5	26)	1	2	30	4	1	31	12	5
C(1	2	5	10)	1	6	4	3				

Example 3.14: A $PA_1(3,32,32)$ [14]. The group $A\Gamma L(1,32)$ is a sharply 3-homogeneous permutation group of degree 32. If we write the $32 \cdot 31 \cdot 5$ permutations as rows of an array A, we get a $PA_1(3,32,32)$.

Define $P_4 = \{v : \text{there exists a } PA_1(3,4,v)\}$. From the examples above, we have that $4, 5, 7, 8, 11, 13, 23$, and $32 \in P_4$. First, we observe that we can determine precisely what even values are in P_4.

Theorem 3.1. *If v is even, then there is a $PA_1(3,4,v)$ if and only if $v \equiv 2$ or 4 modulo 6.*

Proof: This condition is necessary, by Corollary 1.3. Sufficiency follows from Theorem 2.2, noting that $S_1(3,4,v)$ exist for all $v \equiv 2$ or 4 modulo 6 ([4]). ∎

We can now show that several other small values of v are in P_4 by applying the tBD construction. Our main source of $3BD$s are inversive planes $IP(q)$, q a prime power. An inversive plane $IP(q)$ is an $S_1(3,q+1,q^2+1)$. These were first shown to exist by Witt [15], [16]. Also, note that if we truncate points from an $IP(q)$, we obtain a $3BD$ having different block sizes.

Only a few other general constructions for $3BD$s are known. One of the most useful (for our purposes) is due to Heinrich and Nonay ([8] p. 60) (see also Fu [2, Lemma 2.4]).

Lemma 3.2. *Suppose $m \geq 2, m \neq 3,5$. Then there is a $(8m+1,\{4,5,2m+1\},1)$-$3BD$.*

Corollary 3.3. *Suppose $v \geq 5$ is odd, $v \neq 7$ or 11. If a $PA_1(3,4,v)$ exists, then so too does a $PA_1(3,4,4v-3)$ exist.*

A generalization of Lemma 3.2 has been given by Hartman and Phelps in [7]. In order to state the construction, we need to define transversal t-designs. A $TD(t,k,v)$ is a triple $(X,\mathcal{G},\mathcal{B})$, where X is a set of kv elements (*points*), $\mathcal{G}$ is a partition of X into k *groups* containing v points each, and $\mathcal{B}$ is a set of k-subsets of X (*blocks*), each of which is a transversal of $\mathcal{G}$, such that every set of t points from distinct groups occurs in a unique block. The following construction is a straightforward modification of [7, Theorem 2.2].

Lemma 3.4. *Let K be a set of block sizes such that $4 \in K$. Suppose there is a $TD(3,4,v-w)$ containing w disjoint subdesigns $TD(2,4,v-w)$, where $v-w$ is even. Suppose also that there is a $(v,K,1)$-$3BD$ which contains at least one block of size w. Then there is a $(4(v-w)+w,K,1)$-$3BD$.*

The following theorem summarizes our knowledge about $PA_1(3,4,v)$ for odd $v < 100$.

Theorem 3.5. *There exists a $PA_1(3,4,v)$ for $v = 5,7,11,13,17,23,25,29,49,53,65,85,89,$ and 97.*

Proof: The cases $v = 5,7,11,13,$ and 23 were given in the examples. For $v = 25$ and 29, apply Construction 2.1 as follows. For $v = 25$ use a $(25,\{4,5\},1)$-$3BD$ which can be constructed by deleting a point from a $(26,\{5\},1)$-$3BD$ [6]. For $v = 29$, we employ a $(29,\{4,5\},1)$-$3BD$ constructed by K. T. Phelps (private communication). For $v = 17,49,65,89,$ and 97, apply Corollary 3.3. For $v = 53$, apply Lemma 3.4 and Construction 2.1 with the equation $53 = 4(17-5)+5$. The existence of a $TD(3,5,12)$ (Example 3.15) implies the existence a $TD(3,4,12)$ containing 12 disjoint $TD(2,4,12)$; and an inversive plane of order 4 is a $(17,\{5\},1)$-$3BD$ which contains at least one block of size 5. Finally, for $v = 85$, apply Lemma 3.4 and Construction 2.1 with the equation $85 = 4(25-5)+5$. The existence of a $TD(3,5,20)$ [7, Theorem 2.3 (b)] implies the existence of a $TD(3,4,20)$ containing 20 disjoint $TD(2,4,20)$; and a $(25,\{4,5\},1)$-$3BD$ which contains at least one block of size 5 was mentioned earlier in this proof. ∎

Example 3.15. *A* $TD(3,5,12)$. *For every* g *and* $h \in Z_2 \times Z_6$, *construct 12 blocks as follows.*

$$
\begin{array}{lllll}
\{g, & g, & h, & g+h, & h\} \\
\{g, & g+(0,1), & h+(1,1), & g+h+(0,3), & h\} \\
\{g, & g+(0,2), & h+(1,5), & g+h+(1,0), & h\} \\
\{g, & g+(0,3), & h+(1,2), & g+h+(0,1), & h\} \\
\{g, & g+(0,4), & h+(1,4), & g+h+(1,3), & h\} \\
\{g, & g+(0,5), & h+(0,2), & g+h+(1,5), & h\} \\
\{g, & g+(1,0), & h+(0,5), & g+h+(0,2), & h\} \\
\{g, & g+(1,1), & h+(0,4), & g+h+(1,2), & h\} \\
\{g, & g+(1,2), & h+(0,3), & g+h+(0,5), & h\} \\
\{g, & g+(1,3), & h+(1,3), & g+h+(0,4), & h\} \\
\{g, & g+(1,4), & h+(0,1), & g+h+(1,1), & h\} \\
\{g, & g+(1,5), & h+(1,0), & g+h+(1,4), & h\}
\end{array}
$$

We can completely determine the spectrum of $PA_3(3,4,v)$. Note that there are no congruential restrictions on v here.

Theorem 3.5. *There is a* $PA_3(3,4,v)$ *if and only if* $v \geq 4$.

Proof: Hanani showed in [5] that there is a $(v,\{4,5,6,7,9,11,13,15,19,23,27,29,31\},1)$-$3BD$ for any $v \geq 4$. From the examples, we already know that there is a $PA_3(3,4,v)$ for $v = 4,5,6,7,9,11,13,15,19,23,27,29$, and 31. Apply Construction 2.1 ∎

References

1. R. H. F. Denniston, *Some new 5-designs*, Bull. London Math. Soc. **8** (1976), 263–267.
2. Hung-Lin Fu, *Steiner quadruple systems with a spanning block design*, Cong. Numer. **60** (1987), 145–150.
3. A. Granville, A. Moisiadis and R. Rees, *Nested Steiner n-cycle systems and perpendicular arrrays*, J. Comb. Math. and Comb. Comput. 3 (1988), 163–167.
4. H. Hanani, *On quadruple systems*, Canad. J. Math. **12** (1960), 145–157.
5. H. Hanani, *Truncated finite planes*, Proceedings of Symposia in Pure Mathematics(A. M. S.) **29** (1971), 115–120.
6. H. Hanani, A. Hartman and E. S. Kramer, *On three-designs of small order*, Discrete Math. **45** (1983), 75–97.
7. A. Hartman and K. T. Phelps, *The spectrum of tetrahedral quadruple systems*, Utilitas Math. (to appear).
8. K. Heinrich and G. M. Nonay, *Exact coverings of 2-paths by 4-cycles*, J. Comb. Theory A **45** (1987), 50–61.
9. Dieter Jungnickel and S. A. Vanstone, *Hyperfactorizations of graphs and 5-designs*, J. Univ. Kuwait **14** (1987), 213–223.
10. C. C. Lindner and D. R. Stinson, *The spectrum for the conjugate invariant subgroups of perpendicular arrays*, Ars Combinatoria **18** (1984), 51–60.
11. C. C. Lindner , R. C. Mullin and G. H. J. van Rees, *Separable orthogonal arrays*, Utilitas Math. **31** (1987), 25–32.
12. W. H. Mills, *A new 5-design*, Ars Combinatoria **6** (1978), 193–195.
13. R. C. Mullin, P. J. Schellenberg, G. H. J. van Rees and S. A. Vanstone, *On the construction of perpendicular arrays*, Utilitas Math. **18** (1980), 141–160.
14. D. R. Stinson and L. Teirlinck, *A construction for authentication / secrecy codes from 3- homogeneous permutation groups*, Europ. J. Comb. (to appear).
15. E. Witt, *Die funffach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Hamburg **12** (1938), 256–264.
16. E. Witt, *Uber Steinersche Systeme*, Abh. Math. Sem. Hamburg **12** (1938), 265–275.

E. S. Kramer
Department of Mathematics
University of Nebraska
Lincoln Nebraska 68588
U.S.A.

D. L. Kreher
School of Computer Science
Rochester Institute of Technology
Rochester New York 14623
U.S.A.

R. Rees
Department of Mathematics
Mount Allison University
Sackville New Brunswick E0A 3C0
Canada

D. R. Stinson
Department of Computer Science
University of Manitoba
Winnipeg Manitoba R3T 2N2
Canada