Some t-homogeneous sets of permutations

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, MI 49931 (USA)

Stephen Black
IBM Heidelberg (Germany)

Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany)

Abstract

Perpendicular Arrays are ordered combinatorial structures, which recently have found applications in cryptography. A fundamental construction uses as ingredients **combinatorial designs** and **uniformly t-homogeneous sets of permutations.** We study the latter type of objects. These may also be viewed as generalizations of t-homogeneous groups of permutations. Several construction techniques are given. Here we concentrate on the **optimal** case, where the number of permutations attains the lower bound. We obtain several new optimal such sets of permutations. Each example allows the construction of infinite families of perpendicular arrays.

1 Introduction

Definition 1 *A* **perpendicular array** $PA_\lambda(t, k, v)$ *is a multiset* $\mathcal{A}$ *of injective mappings from a* k*-set* C *into a* v*-set* E*, which satisfies the following:*

- *for every t-subset $U \subseteq C$ and every t-subset $W \subseteq E$ the number of elements of $\mathcal{A}$ (eventually counted with multiplicities) mapping U onto W is λ, independent of the choice of U and W.*

Alternatively $\mathcal{A}$ may be viewed as an array with C as set of columns and E as set of entries, where each mapping contributes a row. Here we are primarily interested in the case $k = v = n$.

A $PA_\mu(t, n, n)$ may be described as a **μ-uniform t-homogeneous multiset of permutations on n objects.** We speak of a $PA(t, n, n)$ if we are not interested in the value of μ. A $PA(t, n, n)$ is **inductive**, equivalently is an $APA(t, n, n)$ if it is a $PA(w, n, n)$ for every $w, 1 \leq w \leq t$. Every $PA(t, n, n)$ is inductive provided $t \leq (n + 1)/2$ (see [8]). In the above APA stands for **authentication** perpendicular array. This term was coined by D.R. Stinson ([8]) and further generalized in [2]. The notation stems from an application in the cryptographical theory of unconditional secrecy and authentication.

The general definition is as follows:

Definition 2 *An* **authentication perpendicular array** $APA_\mu(t, k, v)$ *is a* $PA_\mu(t, k, v)$ *which satisfies in addition*

- *For any $t' < t$, and for any $t' + 1$ distinct entries we have, that among all the rows of the array $\mathcal{A}$ which contain all those entries, any subset of t' of those entries occurs in all possible subsets of t' columns equallly often.*

Thus PA and APA may be viewed as t-designs, where the blocks are ordered. The basic ingredients in the construction of general APA and related structures are

- t-designs, and
- $APA(t, n, n)$.

In fact the unordered structure underlying an $APA(t, k, v)$ is a t-design with block-size k. An $APA(t, k, k)$ may be used to yield the required ordered structure. (see [8]).
In the sequel we concentrate on sets (instead of multisets) of permutations. Such arrays may be called **simple**.
Examples of $APA(t, n, n)$ are furnished by t-homogeneous **groups** of permutations. However, as a consequence of the characterization of finite simple groups all the t-homogenous groups of permutations are known

$(2 \le t \le (n+1)/2)$. Aside from the alternating and symmetric groups there is no infinite family of t-homogeneous groups on n objects when $3 < t \le (n+1)/2$. It is therefore necessary to find different methods of constructing

$APA_\mu(t,n,n)$. Given t and n we consider the problem of constructing $APA_\mu(t,n,n)$ which are as small as possible. This is equivalent to minimizing μ. As the number of permutations of an $APA_\mu(t,n,n)$ is divisible by $\binom{n}{w}$ for every $w, 1 \le w \le t$, it follows that μ is divisible by $LCM\{\binom{n}{w}|w = 1,2,\dots t)\}/\binom{n}{t}$.

Definition 3 *Put*

$$\mu_0(t,n) = LCM\{\binom{n}{w}|w = 1,2,\dots t)\}/\binom{n}{t}.$$

An $APA_\mu(t,n,n)$ *is called* **optimal** *if* $\mu = \mu_0(t,n)$.

We list the values of this function for small t :

$$\mu_0(1,n) = 1.$$

$$\mu_0(2,n) = \begin{cases} 1 & \text{if } n \text{ odd} \\ 2 & \text{if } n \text{ even.} \end{cases}$$

$$\mu_0(3,n) = \begin{cases} 1 & \text{if } n \equiv 2(mod\ 3) \\ 3 & \text{otherwise.} \end{cases}$$

$$\mu_0(4,n) = \begin{cases} 1 & \text{if } n \equiv 3,11(mod\ 12) \\ 2 & \text{if } n \equiv 5,9(mod\ 12) \\ 3 & \text{if } n \equiv 7(mod\ 12) \\ 4 & \text{if } n \equiv 0,2,6,8(mod\ 12) \\ 6 & \text{if } n \equiv 1(mod\ 12) \\ 12 & \text{if } n \equiv 4,10(mod\ 12). \end{cases}$$

Our primary interest here is in the construction of optimal $APA(t,n,n)$. We may restrict attention to the case $t \le (n+1)/2$. This is due to the fact that a uniformly t-homogeneous set of permutations on n objects is also uniformly $(n-t)$-homogeneous.
For $t = 1$ there is no problem. An $APA_1(1,n,n)$ is nothing but a latin square of order n. For $t = 2$ and $n = q$ a prime-power, the affine group $AGL_1(q)$

is an $APA_2(2,q,q)$. This is optimal if q is a power of 2. If q is odd, then $AGL_1(q)$ contains an $APA_1(2,q,q)$ (see [7]). The projective group $PSL_2(q)$ is an $APA_3(3,q+1,q+1)$ if q is a prime-power, $q \equiv 3(mod\ 4)$. This is optimal if
$q \equiv 3, 11(mod\ 12)$. This yields optimal

$$APA_3(3,12,12), APA_3(3,24,24), APA_3(3,28,28), \ldots.$$

These are the only known infinite families of optimal $APA(t,n,n)$. In [5] an $APA_2(2,6,6)$ was constructed. In [3] it was shown that the group $PSL_2(q), q \not\equiv 3(mod\ 4)$, can be **halved** as a uniformly 2-homogeneous set of permutations on the projective line. The case $q=5$ yields another construction of an $APA_2(2,6,6)$. An $APA_3(3,6,6)$ is constructed in [6] and [1]. A recursive construction given in [2],Corollary 6 when applied to an $APA_1(2,5,5)$ (equivalently: an $APA_1(3,5,5)$) also yields $APA_3(3,6,6)$.
The affine group $AGL_1(8)$ is an $APA_1(3,8,8)$, the group $A\Gamma L_1(32)$ is an $APA_1(3,32,32)$. An $APA_3(3,9,9)$ was constructed in [5] as a subset of the group $PGL_2(8)$. To the best of our knowledge these are all the optimal $PA(t,n,n), t \leq (n+1)/2$ which have been known that far.
In sections 2 and 3 we describe new methods of construction. Our main result is the following:

Theorem 1

- *There exist (optimal)*
  - $APA_2(2,10,10)$
  - $APA_2(2,12,12)$
  - $APA_3(3,7,7)$
  - $APA_4(4,8,8)$
- *There is a (non-optimal)* $APA_4(3,11,11)$ *contained in the Mathieu group* M_{11}.
- *For* $q \in \{3,5,7,9\}$ *the group* $P\Gamma L_2(q^2)$ *contains an*

$APA_{q-1}(2, q^2+1, q^2+1)$.

The construction of optimal $APA(\lfloor n/2 \rfloor, n, n)$ is one of the central problems in the area. The authors are convinced that this is a very hard problem in general. It is obvious that an optimal $APA(\lfloor n/2 \rfloor, n, n)$ is also an optimal $APA(t, n, n)$ for every t, $\lfloor n/2 \rfloor \leq t \leq n$. We get:

Corollary 1 *There exist (optimal)*

$$APA_3(4,7,7), APA_5(5,7,7), APA_{15}(6,7,7), APA_{105}(7,7,7),$$

$$APA_5(5,8,8), APA_{10}(6,8,8), APA_{35}(7,8,8), APA_{280}(8,8,8).$$

Moreover a symmetry in the construction yields the following corollary:

Corollary 2 *There exist (optimal)*

- $APA_2(2,5,6)$
- $APA_2(2,9,10)$
- $APA_2(2,11,12)$

2 The double coset-method

Definition 4 *Let G and H be subgroups of the symmetric group on n letters. A multiset $\mathcal{A}$ of permutations of the ground set is (G, H)-**admissible** if for every $g \in G, h \in H, \sigma \in \mathcal{A}$ we have $g\sigma h \in \mathcal{A}$ (if $\mathcal{A}$ is not simple we demand that the multiplicity of σ and of $g\sigma h$ are the same).*

Let now $\mathcal{A}$ be an $APA(t, n, n)$. For arbitrary permutations g and h the multiset $g\mathcal{A}h$ is an $APA(t, n, n)$ again. Therefore the set $G = \{g | g\mathcal{A} = \mathcal{A}\}$ is a group, the stabilizer of $\mathcal{A}$ under the action of the symmetric group S_n from the left. By operation from the right the situation is analogous. If $\mathcal{A}$ is (G, H)-admissible and α, β are arbitrary permutations of the ground set, then $\alpha\mathcal{A}\beta$ is $(\alpha G\alpha^{-1}, \beta^{-1}H\beta)-$admissible. We may therefore replace G and H by conjugate subgroups. If $\mathcal{A}$ is a (G, H)-admissible $APA_\mu(t, n, n)$, then the multiset $\mathcal{A}^{-1}$ of inverses is a (H, G)-admissible $APA_\mu(t, n, n)$. A (G, H)-admissible set of permutations may equivalently be described as a union of

double cosets for G and H.
Let us visualize the multiset $\mathcal{A}$ of permutations as an array with n columns, where each element of $\mathcal{A}$, eventually counted with multiplicities, contributes a row, each row being a permutation. If $\mathcal{A}$ is (G, H)-admissible, then let H operate on the set of columns, whereas G permutes the entries of the array.
Consider first the problem of constructing $APA_2(2, n, n), n$ even. Such an array $\mathcal{A}$ has $n(n-1)$ elements. It is then conceivable that $\mathcal{A}$ is (G, G)-admissible, where G is a group of order $n-1$. Assume $G = Z_{n-1}$ in its natural action on n points, $G =< \zeta >, \zeta = (\infty)(0, 1, 2, \ldots n-2)$. Then $\mathcal{A}$ must be the union of two double cosets, one of which is Z_{n-1} itself:

$$\mathcal{A} = Z_{n-1} \cup Z_{n-1} \cdot \sigma_0 \cdot Z_{n-1}.$$

Thus $\mathcal{A}$ is determined by one permutation σ_0. Observe that σ_0 may be replaced by an arbitrary element of the same double coset. As $\mu = 2$, there must be an element in $Z_{n-1} \cdot \sigma_0 \cdot Z_{n-1}$ fixing the set $\{\infty, 0\}$. As $\mathcal{A}$ is an $APA_{n-1}(1, n, n)$, no element of $\mathcal{A} - Z_{n-1}$ can fix ∞. We choose σ_0 to be the unique element of $\mathcal{A}$ affording the operation $\sigma_0 : \infty \longleftrightarrow 0$. Write $\sigma_0 = (\infty, 0) \cdot \rho_0$, where ρ_0 is a permutation of $\{1, 2, \ldots n-2\}$.
Consider the circle $C = C_{n-1}$ of length $n-1$ with set $\{0, 1, 2, \ldots n-2\}$ of vertices and neighbourhoodrelation

$$i \perp j \iff |i - j| \equiv 1 (mod\, n-1).$$

Let $d(\, , \,)$ denote the distance in $C, \Delta = \{1, 2, \ldots \frac{n}{2} - 1\}$ the set of distances $\neq 0$. For every $\delta \in \Delta$ let P_δ be the set of unordered pairs $\{x, y\}$ of vertices of C satisfying $xy \neq 0, d(x, y) = \delta$. Observe that $|P_\delta| = n-3$ for every $\delta \in \Delta$.

Theorem 2 *Let n be an even number. Then the following are equivalent:*

- *There is a (Z_{n-1}, Z_{n-1})-admissible $APA_2(2, n, n)$.*
- *There is a permutation ρ of $\{0, 1, 2, \ldots n-2\}, \rho(0) = 0$ such that for every $\delta \in \Delta$ the following is satisfied:*

$$|\rho(P_\delta) \cap P_\delta| = 1.$$

$$|\rho(P_\delta) \cap P_{\delta'}| = 2 \; (\delta' \in \Delta, \delta' \neq \delta).$$

Proof. Write $Z_{n-1} = \{z(i) | i = 0, 1, 2, \ldots n-2\}$, where

$$z(i) : \tau \longmapsto \tau + i \ (mod\ n-1).$$

Then the typical element $z(i)\sigma_0 z(j)$ of $\mathcal{A} - Z_{n-1}$ affords the operation

$$\tau \longmapsto (\tau + i)^{\sigma_0} + j.$$

Let A, B be two unordered pairs of elements in $\{\infty, 0, 1, 2, \ldots, n-2\}$. We have to make sure that exactly two elements of $\mathcal{A}$ map A onto B. We have

$$z(l-j) : \infty \longrightarrow \infty, j \longrightarrow l.$$

$$z(-j)\sigma_0 z(l) : j \longrightarrow \infty \longrightarrow l.$$

$$z((l-k)^{\sigma_0^{-1}} - j)\sigma_0 z(k) : \infty \longrightarrow k, j \longrightarrow l.$$

$$z(-i)\sigma_0 z(l - (j-i)^{\sigma_0}) : i \longrightarrow \infty, j \longrightarrow l.$$

In fact the element of $\mathcal{A}$ affording one of these operations is uniquely determined in each case. This shows that the condition is satisfied whenever $\infty \in A$ or $\infty \in B$, independent of the choice of ρ_0.
Let now $A = \{i, j\}, B = \{k, l\}$, where $\infty \notin A \cup B, i \neq j, k \neq l$. Exactly then is there an element of Z_{n-1} mapping A onto B if $d(i, j) = d(k, l)$. This element is then uniquely determined. An element $z(\alpha)\sigma_0 z(\beta)$ affords the operation $i \mapsto k, j \mapsto l$ if and only if

$$(i + \alpha)^{\rho_0} + \beta = k$$

$$(j + \alpha)^{\rho_0} + \beta = l$$

The condition on α is $(i+\alpha)^{\rho_0} - (j+\alpha)^{\rho_0} = k - l$. Interchanging k and l we see that a necessary and sufficient condition for α is

$$d((i+\alpha)^{\rho_0}, (j+\alpha)^{\rho_0}) = d(k, l).$$

The Theorem is now obvious.■

Thus the existence of a (Z_{n-1}, Z_{n-1})-admissible $APA_2(2, n, n)$ is equivalent to the existence of a permutation on $n-1$ letters, which fixes one letter and destroys the metric given by a circle of length $n-1$ in the most effective way.

Theorem 3 *Let n be even. If n is a power of 2 or $n \in \{6, 12\}$, then there is a (Z_{n-1}, Z_{n-1})-admissible $APA_2(2, n, n)$.*

Proof. If $n = q$ is a power of 2, then the group $AGL_1(q)$ is an $APA_2(2, q, q)$. As it contains the multiplicative group of the field $\mathbb{F}_q$, it is (Z_{n-1}, Z_{n-1})-admissible.
For $n = 6$ and $n = 12$ it suffices, by the preceding theorem, to give the permutation ρ_0. If $n = 6$, then ρ_0 is uniquely determined: $\rho_0 = (1, 4)$. If $n = 12$, we may choose

$$\rho_0 \in \{\rho_1 = (1, 3, 9, 5, 4)(2, 8, 10, 7, 6), \rho_2 = \rho_1^{-1},$$

$$\rho_3 = (1, 7)(2, 5)(3, 10)(4, 6)(8, 9), \rho_4 = (1, 8)(2, 3)(4, 10)(5, 7)(6, 9)\}.$$

■

An exhaustive search showed that that for $n \in \{10, 14, 18, 20, 22\}$ there is no (Z_{n-1}, Z_{n-1})-admissible $APA_2(2, n, n)$.

Definition 5 *Fix $Z = Z_{n-1}$ and $C = C_{n-1}$ as before. Let $\Pi = \Pi_{n-1}$ be the set of permutations ρ_0 such that $\rho = (0)\rho_0$ satisfies the conditions of Theorem 2.*

In fact $\Pi_5 = \{(1, 4)\}, \Pi_{11} = \{\rho_1, \rho_1^{-1}, \rho_3, \rho_4\}$, where the permutations are given in the proof of the preceding Theorem.

Lemma 1 *If $\rho \in \Pi$, then $I(\rho) \in \Pi$ and $N(\rho) \in \Pi$, where the involutory operations I and N are defined by*

$$I(\rho)(\tau) = \rho^{-1}(\tau) \quad (1)$$
$$N(\rho)(\tau) = \rho(-\tau). \quad (2)$$

Moreover the group $< I, N >$ generated by I and N is dihedral of order 8.

Proof: This is a consequence of the following easily checked facts: I and N are involutory operations mapping Π onto itself. The product IN has order 4.■

The elements of Π_{11} are rather interesting.We have

$$\rho_3(x) = \prod_{x \in \boldsymbol{F}_{11}^{*2}} (x, -4x),$$

$$\rho_1(x) = x \cdot 3^{(\frac{x}{11})},$$

where $(\frac{a}{b})$ is the Legendre symbol. We tried to generalize this to larger fields but were not successful. If $\mathcal{A} = \mathcal{A}(\rho_0) = Z_{n-1} \cup Z_{n-1} \cdot \rho_0 \cdot Z_{n-1}$ is an $APA_2(2, n, n)$, then $\mathcal{A}(\rho_0^{-1})$ is simply the set of inverses. In contrast to this the relation between $\mathcal{A}(\rho_0)$ and $\mathcal{A}(g(\rho_0))$ for other $g \in < I, N >$ may be rather mysterious. It happens that one of them is sharply 2-transitive while the other is not. Even more can happen. Consider the case $n = 12$ again. The group $< I, N >$ operates transitively on Π_{11}. In spite of that the group generated by $\mathcal{A}(\rho_1)$
(and by $\mathcal{A}(\rho_1^{-1})$) is the full symmetric group S_{12}, whereas $\mathcal{A}(\rho_3)$ and $\mathcal{A}(\rho_4)$ generate a copy of the Mathieu group M_{12}.

The following constructions of (G, H)-admissible sets of permutations are computer-results. They were obtained by the third author. In each case we give G (operating on the columns of the array), H (operating on the entries of the array) and the **generator-matrix,** whose rows are the generators of double-cosets. The set of symbols is $\{1, 2, \ldots, n\}$. It is easy to check that the arrays have the desired properties.

Theorem 4 *Let $\mathcal{A}$ be a union of double cosets of groups G and H, where the double coset-representatives are the rows of the generator-matrix M.*

- *Let $G =< (1,2,3)(4,5,6)(7,8,9), (1,4,7)(2,5,8)(3,6,9) >$,*

  $H =< (1,5,6,7,10)(2,4,9,3,8) >$,

  $$M = \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 9 & 6 & 8 & 2 & 5 & 10 & 7 & 3 \end{array}$$

  Then $\mathcal{A}$ is an $APA_2(2, 10, 10)$.

- *Let $G =< (1,2,3,4,5,6,7) >$,*

  $H =< (2,3,4,5,6) >$,

$$M = \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 6 & 5 & 7 \\ 1 & 2 & 3 & 5 & 7 & 4 & 6 \\ 1 & 2 & 4 & 3 & 6 & 7 & 5 \end{array}$$

Then $\mathcal{A}$ *is an* $APA_3(3,7,7)$.

- *Let* $G =< (2,3,4,5,6,7,8) >$,

  $H =< (4,5,6,7,8) >$,

$$M = \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 5 & 6 & 8 & 7 \\ 2 & 5 & 1 & 3 & 4 & 6 & 8 & 7 \\ 2 & 4 & 6 & 1 & 3 & 5 & 8 & 7 \\ 2 & 6 & 3 & 1 & 4 & 7 & 8 & 5 \\ 2 & 7 & 8 & 1 & 4 & 6 & 3 & 5 \\ 2 & 8 & 4 & 1 & 6 & 3 & 5 & 7 \\ 2 & 8 & 6 & 1 & 4 & 7 & 3 & 5 \end{array}$$

Then $\mathcal{A}$ *is an* $APA_4(4,8,8)$.

- *Let* $G =< (1,2,3,4,5,6,7,8,9,10,11) >, H =< (2,3,4,5,6)(7,8,9,10,11) >$

$$M = \begin{array}{ccccccccccc} 1 & 2 & 4 & 6 & 3 & 11 & 9 & 7 & 8 & 5 & 10 \\ 1 & 2 & 6 & 7 & 10 & 11 & 8 & 5 & 3 & 4 & 9 \\ 1 & 2 & 11 & 5 & 3 & 10 & 4 & 8 & 6 & 7 & 9 \\ 1 & 2 & 4 & 10 & 6 & 5 & 11 & 9 & 3 & 7 & 8 \\ 1 & 2 & 10 & 9 & 8 & 5 & 3 & 7 & 6 & 4 & 11 \\ 1 & 4 & 8 & 5 & 10 & 3 & 2 & 11 & 7 & 6 & 9 \\ 1 & 2 & 10 & 5 & 4 & 6 & 8 & 9 & 7 & 11 & 3 \\ 1 & 7 & 6 & 5 & 4 & 11 & 2 & 8 & 9 & 3 & 10 \\ 1 & 2 & 8 & 3 & 10 & 6 & 9 & 4 & 5 & 7 & 11 \\ 1 & 5 & 8 & 6 & 9 & 4 & 2 & 7 & 10 & 3 & 11 \\ 1 & 2 & 7 & 6 & 4 & 9 & 5 & 8 & 3 & 10 & 11 \\ 1 & 7 & 9 & 4 & 10 & 5 & 2 & 6 & 3 & 8 & 11 \end{array}$$

Then $\mathcal{A}$ *is an* $APA_4(3,11,11)$.

Our construction of an $APA_2(2,10,10)$ will be generalized in the next section.
The second author found the first example of an $APA_2(2,10,10)$ in January 1992. His example is contained in the symmetric group S_6 in its 2-transitive action on 10 points. The construction was obtained by the probabilistic search technique **simulated annealing.**

3 The projective semi-linear group

The $APA_2(2,10,10)$ as constructed in the previous section is contained in the projective semi-linear group $P\Gamma L_2(9)$. More precisely the group $< \mathcal{A} >$ generated by $\mathcal{A}$ is $PSL_2(9) < \phi >$, where $PSL_2(9) \cong A_6$ is the special linear group and ϕ is the Frobenius automorphism of $\mathbb{F}_9$ over $\mathbb{F}_3$. The second author conjectures that this construction generalizes as follows:

Conjecture 1 *Let q be an odd prime-power. Then there is a subset $\mathcal{A} \subset P\Gamma L_2(q^2)$ such that $\mathcal{A}$ is an $(Z_{(q^2+1)/2}, E_{q^2})-$admissible*

$$APA_{q-1}(2, q^2+1, q^2+1).$$

Here $Z_{(q^2+1)/2}$ and E_{q^2} denote the cyclic respectively elementary abelian subgroup of $PSL_2(q^2)$ of the corresponding orders.

The conjecture has been verified for $q \leq 9$.

Proposition 1 *There exist*

- $APA_4(2,26,26) \subset P\Gamma L_2(25)$
- $APA_6(2,50,50) \subset P\Gamma L_2(49)$
- $APA_8(2,82,82) \subset P\Gamma L_2(81)$

We mention some more $APA_\mu(t,n,n)$, where μ is small without being optimal:
The unitary group $U_3(5) = PSU_3(5^2)$ is an $APA_{16}(2,126,126)$, the smallest Ree group ${}^2G_2(3) \cong P\Gamma L_2(8)$ is an $APA_4(2,28,28)$, whereas ${}^2G_2(27)$ is an $APA_{52}(2,19684,19684)$. The smallest Suzuki group ${}^2B_2(8)$ is an

$APA_{16}(2,65,65)$ and ${}^2B_2(32)$ is an $APA_{62}(2,1025,1025)$. Further $PSL_2(8)$ is an $APA_4(4,9,9)$ and $P\Gamma L_2(32)$ is an $APA_4(4,33,33)$.

4 Some authentication perpendicular arrays

Let $\mathcal{A}$ be an $APA_\lambda(2,k,v)$. The transitive kernel $C_0(\mathcal{A})$ was defined in [2] as the set of columns c which satisfy that for every column $c' \neq c$ the restriction $\mathcal{A}_{\{c,c'\}}$ of $\mathcal{A}$ to columns c and c' is an ordered design $OD_{\lambda/2}(2,2,v)$. It was proved that for $c \in C_0(\mathcal{A})$ the restriction of $\mathcal{A}$ to $C-\{c\}$ is an $APA_\lambda(2,k-1,v)$. We improve on [2],Proposition 3 and Corollary 15:

Proposition 2 *Let $\mathcal{A}$ be an $APA_2(2,n,n)$, which is $(G,1)$-admissible, where the group G of order $n-1$ fixes one column c and transitively permutes the remaining columns. Then $c \in C_0(\mathcal{A})$.*

Proof. It is easily seen that for every column $c' \neq c$ and every pair a,b of entries there is a row of $\mathcal{A}$ having a in column c and b in column c'. As the number of rows of $\mathcal{A}$ is $n(n-1)$, it follows that $\mathcal{A}_{\{c,c'\}}$ is an $OD_1(2,2,n)$. ∎

Application of this to our constructions of $APA_2(2,6,6)$, $APA_2(2,10,10)$ and $APA_2(2,12,12)$ yields Corollary 2.

References

[1] J.Bierbrauer: *The uniformly 3-homogeneous subsets of $PGL_2(q)$, Journal of algebraic combinatorics* **4**(1995),99-102.

[2] J.Bierbrauer,Y.Edel: *Theory of perpendicular arrays, Journal of Combinatorial Designs* **6**(1994),375-406.

[3] J.Bierbrauer,Y.Edel: *Halving $PSL_2(q)$*, to appear in *Journal of Geometry.*

[4] J.Bierbrauer,T.v.Tran: *Halving $PGL_2(2^f)$, f odd:a Series of Cryptocodes, Designs, Codes and Cryptography* **1**(1991),141-148.

[5] J.Bierbrauer,T.v.Tran: *Some highly symmetric Authentication Perpendicular Arrays, Designs, Codes and Cryptography* **1**(1992),307-319.

[6] E.S.Kramer,D.L.Kreher,R.Rees,D.R.Stinson: *On perpendicular arrays with* $t \geq 3$, *Ars Combinatoria* **28**(1989), 215-223.

[7] C.R.Rao: *Combinatorial Arrangements analogous to Orthogonal Arrays, Sankhya A***23**(1961),283-286.

[8] D.R.Stinson: *The Combinatorics of Authentication and Secrecy Codes, Journal of Cryptology* **2**(1990), 23-49.

[9] D.R.Stinson,L.Teirlinck: *A Construction for Authentication/Secrecy Codes from 3-homogeneous Permutation Groups,* European Journal of *Combinatorics* **11**(1990),73-79.