# Theory of perpendicular arrays

Jürgen Bierbrauer and Yves Edel
Institut für Reine Mathematik
Universität Heidelberg
Im Neuenheimer Feld 288
69120 HEIDELBERG
Germany

September 6, 2001

## 1 Introduction

A *perpendicular array* with parameters $PA_\lambda(t, k, v)$ is a multiset $\Sigma$ 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 $\Sigma$ (eventually counted with multiplicities) mapping $U$ onto $W$ is $\lambda$, independent of the choice of $U$ and $W$.

The notion of a perpendicular array may be viewed either as a generalization of $t-$homogeneous permutation groups or as a $t-$design with an additional structure given by ordering the blocks. We adopt here the first of these two points of view. If we generalize the notion of a $t-$homogeneous group of permutations of degree $v$ in the sense that we do not require the group-structure any more and that the elements are no longer permutations but injections from a $k-$set into a $v-$set, we arrive at the notion of a $PA$. The analogous procedure, when applied to $t-$transitive groups of permutations, leads to the notion of an *ordered design* ($OD$). If we drop the assumption of injectivity in the $t-$transitive case, we get *orthogonal arrays* ($OA$).

All these structures have been known for rather a long time. They all appear, although partly under different names, in [16]. Orthogonal arrays are the most popular of them. $OA$ and ordered designs are essential ingredients in the important work of Teirlinck ([21, 23]) on the construction of large sets of designs. For some obscure reason perpendicular arrays have attracted much less attention. This should not be so. Some use has been made of $PA$'s in the construction of sets of mutually orthogonal latin squares. One pertinent theorem is that a $PA_1(2,k,v)$ with a regular abelian group of automorphisms on the set of entries allows the construction of $k$-1 mutually orthogonal latin squares of order $v$. In [17] this has been used for instance to construct 4 mutually orthogonal latin squares of order 15. A similar construction, but with a group of automorphisms of order $v$-1 on the entries of an ordered design, is used in [26] for the construction of three mutually orthogonal latin squares of order 14.
The present authors have been inspired by [19]. Stinson gives an application of *inductive* $PA$'s (for this notion see [3]) in the cryptographical theory of unconditional secrecy. In order to meet the requirements of unconditional authentication Stinson introduces an additional condition. $PA$'s satisfying this property were termed *authentication perpendicular arrays* ($APA$). The present paper grew out of an attempt to develop a theory of $APA$'s. Our starting-point is the observation that the defining properties of inductive $PA$'s and of $APA$'s are not unrelated, but rather special cases of a 1-parameter family of homogeneity-conditions. This leads to the definition of an $s-PA_\lambda(t,k,v)$, where the value $s=0$ corresponds to inductive $PA$ and $s=1$ corresponds to $APA$. Further a general $tBD$-construction for $s-PA$ is given in section 2. As a first application we construct

$$3-PA_3(3,4,2w), w\geq 2.$$

In section 3 we derive general lower bounds on the size ( equivalently: on the parameter $\lambda$ ). An $s-PA$ is called *optimal* if this bound is met with equality. For instance the family mentioned above is optimal, even as $APA$. The lower bound is related to *residues*. The residue of an $s-PA$ $\Sigma$ with respect to an entry $e$ is defined as the multiset of those elements (rows) of $\Sigma$ not having $e$ in their image. It is proved that the residue of an $s-PA_\lambda(t,k,v)(k<v, s>0)$ is an $(s-1)-PA_{\lambda(v-k)/t}(t-1,k,v-1)$. Thus the residue of a 2-$PA$ is an $APA$. This justifies the definition of $s-PA$, even if one should only be interested in $APA$ or in inductive $PA$. In section 4 we describe an application of $s-PA$ in the theory of unconditional secrecy and authentication. This is analogous to Stinson's use of $APA$. In section 5 we introduce a general method of recursively constructing $s-PA$ if $s-PA$ with a smaller value of $k$ (and eventually also a $t-$design) are given. This is inspired by Tran's results in this direction ([27]). All the known constructions of this kind are special cases of our theorems. We note that the same type of construction also works for ordered designs. Section 6 explores the question when the restriction of an $s-PA$ to a subset of columns yields an $s-PA$ again. These considerations allow us to construct

$$APA_3(3,k,q+1)$$

for every prime-power $q \equiv 3(mod\ 4)$ and every $k$, $3 \leq k \leq q+1$, as well as $APA_2(2,5,6)$ and $APA_2(2,11,12)$. Most of these arrays are optimal. In section 7 we investigate more closely the affine group $AGL_1(q)$ in odd characteristic. Our method yields the construction of $APA_1(2,k,q)$ whenever $k$ is an odd
divisor of $q-1$, and of

$$APA_1(2,p^m,p^n)$$

for every odd prime $p$ and $1 \leq m \leq n$. The former result is not new ( see [10]). Stinson has constructed $APA_1(2,3,v)$ for all odd $v>5$ (see [18]). The next largest case where $APA_1(2,k,v)$ may exist occurs when $k=5$ and $v$ is odd. We construct here $APA_1(2,5,p)$ for all primes $p \equiv 3(mod\ 4), p>7$. Moreover we are able to apply a theorem of R.M.Wilson's ([28]) and obtain the existence of $APA_1(2,k,q)$, $k$ odd, for all prime-powers $q \equiv 3(mod\ 4), q > 2^{k(k-1)}$. In section 8 a link is established, under certain conditions, between $APA_1(2,k,q)$ and *skew Room k-spaces* (better known as Room *k-cubes*). As a corollary we obtain that $APA_1(2,3,5), APA_1(2,5,7), APA_1(2,7,9)$ and $2-PA_1(3,5,8)$ do not exist. We also obtain a short and conceptual proof of Dinitz' theorem ([8]) stating the existence of skew Room $k$-spaces of side $q$ whenever $q$ is an odd prime-power and $k$ is an odd divisor of $q$-1.
It is clear that the case $k=v$ of multisets of permutations plays a special role in the theory. The design- aspect vanishes in this case. These sets of permutations can be viewed as substitutes for $t-$homogeneous groups of permutations. Recall that as a corollary of the characterization of the finite simple groups all the $t-$homogeneous groups of permutations of degree $v$ (where $2 \leq t \leq (v+1)/2$) are known. These sets of permutations have

been studied in a series of recent papers ( see [1, 2, 4, 5, 6, 6, 20]). Here we concentrate on the case $k < v$. Note however that cases $k < v$ and $k = v$ are closely related. The $tBD$-construction shows how sets of permutations and partially balanced designs may be brought together to construct $s-PA$ with $k < v$. Furthermore it is shown in section 3 that each optimal $PA(\lfloor k/2 \rfloor, k, k)$ allows the construction of a certain family of optimal $s-PA$ satisfying $k < v$.

# 2 Basic facts

**Definition 1** *Let $C$ and $E$ be finite sets,$|C| = k, |E| = v$.*

*A $(C, E)-$*array *$\Sigma$ is defined as a mapping $\Sigma$ from the set of all the functions*

*:$C \longrightarrow E$ into the non-negative integers. Thus $\Sigma$ assigns a weight to every mapping $f : C \longrightarrow E$. If this weight is 0, we interpret this as the function $f$ being absent from the array. Let us visualize $\Sigma$ as an array with $C$ as set of columns and such that every function $f : C \longrightarrow E$ contributes $\Sigma(f)$ rows. We call $E$ the set of* entries*. If $\Sigma(f) > 0$, we say that $f$* belongs to *$\Sigma$. $\Sigma$ will be called* injective *if all the functions belonging to $\Sigma$ are injective (Teirlinck calls such arrays* rowwise simple*).*

- *Let $\Sigma$ be a $(C, E)-$array, $U \subseteq C, W \subseteq E$. Let $\Sigma_U^W$ denote the restriction of $\Sigma$ to the set $U$ of columns and to the rows $f$ satisfying $f(U) \supseteq W$. Put*
$$\Sigma_U = \Sigma_U^E, \Sigma^W = \Sigma_C^W.$$
- *Let $\Sigma$ be a $(C, E)-$array, $W \subseteq E, |W| = i$. Then $W$ is* uniformly distributed *in $\Sigma$ if*
  - *$f(C) \supseteq W$ for every $f \in \Sigma$, and*
  - *for every i-subset $U$ of $C$, the number of rows of $\Sigma$ with the elements of $W$ in the columns of $U$ (formally: $\sum_{f(U)=W} \Sigma(f)$) is independent of the choice of $U$.*

**Definition 2** *Let $\Sigma$ be an injective $(C, E)$-array, $0 \leq u \leq w$. $\Sigma$ satisfies property $P(u, w)$ if for all $E_1, E_2 \subseteq E, |E_1| = u, |E_2| = w - u, E_1 \cap E_2 = \emptyset$,*

*the cardinality of $\Sigma^{E_1 \cup E_2}$ is independent of the choice of $E_1, E_2$, and the set $E_2$ is uniformly distributed in $\Sigma^{E_1 \cup E_2}$.*
*In words: The number of (injective) functions $f \in \Sigma$ having a given $w-$set $E_1 \cup E_2$ in the image and mapping a given $(w-u)-$set $U$ onto the $(w-u)$-set $E_2$ is a constant $\lambda(u, w)$, independent of the choice of $U, E_1$ and $E_2$.*

**Definition 3** *Let $\Sigma$ be an injective $(C, E)$-array, $0 \leq s \leq t, |C| = k, |E| = v$. If $\Sigma$ satisfies properties $P(u, w)$ for all $w \leq t, u \leq min(s, w)$, then $\Sigma$ will be called an*

$$s - PA_\lambda(t, k, v),$$

*where $\lambda > 0$ is the number of rows of $\Sigma$ having the elements of a fixed $t$-set of entries in a fixed $t$-set of columns.*

Arrays satisfying $P(0, t)$ are called *perpendicular arrays* $PA_\lambda(t, k, v)$, the $0-PA_\lambda(t, k, v)$ are exactly the *inductive* $PA_\lambda(t, k, v)$, and the $1-PA_\lambda(t, k, v)$ are exactly Stinson/Teirlincks's *authentication perpendicular arrays* $APA_\lambda(t, k, v)$ (see [20]). Obviously an $s - PA_\lambda(t, k, v), s > 0$, is also an $s' - PA_\lambda(t, k, v)$, for all $0 \leq s' \leq s$. The conditions $P(u, w)$ are not independent.

**Lemma 1** *Let $\Sigma$ be an injective $(C, E)-$array.*

1. *Let $0 < u \leq w$. Then $P(u, w)$ implies $P(u-1, w-1)$.*
2. *Let $0 \leq u < w, 2(w-u) \leq k+1$. Then $P(u, w)$ implies $P(u, w-1)$.*

*Proof.* 1. Let $E_1, E_2 \subseteq E, |E_1| = u-1, |E_2| = w-u, E_1 \cap E_2 = \emptyset$. Choose $e \in E, e \notin E_1 \cup E_2$. Then $E_2$ is uniformly distributed in $\Sigma^{E_1 \cup E_2 \cup \{e\}}$ because of property $P(u, w)$. Let $U$ be a set of $w-u$ columns. The number $\mu$ of rows of $\Sigma^{E_1 \cup E_2 \cup \{e\}}$ with $E_2$ in the columns of $U$ is independent of the choice of $U$. It follows that the number of rows of $\Sigma^{E_1 \cup E_2}$ having the elements of $E_2$ in the columns of $U$ is $\mu \cdot (v-w+1)/(k-w+1)$, independent of the choice of $U$. Thus $E_2$ is uniformly distributed in $\Sigma^{E_1 \cup E_2}$.
2. The case $u = 0$ of perpendicular arrays is proved in [19]. Our proof will use the same method. We may assume $u > 0$. Let $A \cup B \subseteq E, |A| = u, |B| = w-u, A \cap B = \emptyset$. Let further $J$ be a $(w-u)$-set of columns. We know that the number $\lambda(u, w)$ of rows $f$ of $\Sigma$ satisfying $f(C) \supseteq A \cup B, f(J) = B$ is independent of the choice of $J$. Observe that by 1. the corresponding

number $\lambda(u-1, w-1)$ is defined. Let now $E_1, E_2 \subseteq E, |E_1| = u, |E_2| = w-u-1, E_1 \cap E_2 = \emptyset$. Count the rows $f$ of $\Sigma$ satisfying

$$f(C) \supseteq E_1 \cup E_2, f(J) \supseteq E_2.$$

Then $f(J) = E_2 \cup \{e\}$, where either $e \in E - E_1 \cup E_2$ or $e \in E_1$. We count $(v-w+1) \cdot \lambda(u, w)$ rows of the first type and $u \cdot \lambda(u-1, w-1)$ rows of the second type. Counting the other way around, we see that every $(w-u)$-set $J$ of columns yields an equation

$$\sum_{J' \subset J, |J'| = w-u-1} x(J', E_1, E_2) = (v-w+1) \cdot \lambda(u, w) + u \cdot \lambda(u-1, w-1) = c.$$

Here $x(J', E_1, E_2)$ denotes the number of rows $f$ of $\Sigma$ satisfying $f(C) \supseteq E_1 \cup E_2, f(J') = E_2$. We saw above that the right-hand side is a constant $c$, independent of the choice of $E_1$ and $E_2$. This yields a system of $\binom{k}{w-u}$ equations for $\binom{k}{w-u-1}$ unknowns. The matrix of coefficients is the inclusion-matrix between the $(w-u-1)-$subsets and the $(w-u)-$subsets of a $k-$set. By a well-known theorem of Kantor's (see [12]), this matrix has maximal rank. If $2(w-u) \leq k+1$, then $\binom{k}{w-u-1} \leq \binom{k}{w-u}$ and the rank of the inclusion-matrix is $\binom{k}{w-u-1}$. It follows that the system has exactly one solution, namely

$$x(J', E_1, E_2) = c/(w-u).$$

■

Observe further that the conditions $P(u, u)$ are empty.

**Corollary 1** *Let $\Sigma$ be an injective $(C, E)$-array.*

- *If $P(0, t), P(1, t), \ldots P(s, t), P(s, t-1), \ldots P(s, s+1)$ hold, then $\Sigma$ is an $s - PA_\lambda(t, k, v)$.*
- *If $2(t-s) \leq k+1$ and $P(0, t), P(1, t), \ldots P(s, t)$ hold, then $\Sigma$ is an $s - PA_\lambda(t, k, v)$.*
- *A $(t-1) - PA_\lambda(t, k, v)$ is also a $t - PA_\lambda(t, k, v)$.*

If $v = k$, then obviously the condition $P(0, w)$ implies the condition $P(u, w)$ for every $u > 0$. More generally we get

**Theorem 1** *Let $\Sigma$ be a $(v-k)-PA_\lambda(t,k,v), v-k \leq t$. Then $\Sigma$ is a $t-PA_\lambda(t,k,v)$.*

*Proof.* Use induction over $d = v-k$. The case $d=0$ is trivial. So let $d>0, v-k \leq t$, let $\Sigma$ be an $s-PA_\lambda(t,k,v), v-k \leq s < t$. We want to show that $\Sigma$ is an $(s+1)-PA_\lambda(t,k,v)$. It suffices to establish the validity of property $P(s+1,t)$. Let $E_1, E_2 \subseteq E, |E_1| = s+1, |E_2| = t-s-1, E_1 \cap E_2 = \emptyset$. Choose $e \in E_1$. We have

$$\Sigma^E = \Sigma^{E-\{e\}} - res_e(\Sigma)^{E-\{e\}}.$$

Here $res_e(\Sigma)$, the *residue* of $\Sigma$ with respect to entry $e$, consists of the rows of $\Sigma$, which do not contain $e$. Residues will be studied in the next section. We shall see in Theorem 4 that $res_e(\Sigma)$ is an $(s-1)-PA(t-1,k,v-1)$. By induction it is an $s-PA(t-1,k,v-1)$. Here we have used the convention of omitting $\lambda$ if the value of parameter $\lambda$ is not specified. $E_2$ is uniformly distributed in $res_e(\Sigma)^{E-\{e\}}$. Further $E_2$ is uniformly distributed in $\Sigma^{E-\{e\}}$ because of property $P(s,t-1)$. We are done. ∎

The following Theorem gives a rather general method of construction for arrays $s-PA_\lambda(t,k,v)$ with arbitrary $s$. It uses $t$-wise balanced designs. Here a *$t$-wise balanced design* (tBD) with parameters $t-(v,L,\lambda)$ is a multiset of subsets ( called *blocks*) of a fixed ground-set of cardinality $v$ such that the cardinalities of blocks are in the set $L$ of natural numbers and every set of $t$ points is contained in exactly $\lambda$ blocks. Here the blocks have to be counted with their multiplicities. If $|L| = 1$, then we have a not necessarily simple $t$-design.

**Theorem 2 ($tBD$-construction)** *Assume there is a $t$-wise balanced design with parameters $t-(v,L,\lambda)$ and for every $l \in L$ there is an array $s-PA_\mu(t,k,l)$. Let the design be defined on the $v$-set $E$. Construct an injective $(C,E)$-array $\Sigma$, where $|C| = k$, by replacing every block $B$ of the design by a copy of the $s-PA_\mu(t,k,l)$ defined on $B$. Then $\Sigma$ is an $s-PA_{\lambda\cdot\mu}(t,k,v)$.*

*Proof.* Property $P(0,t)$ holds by construction.

1.Let $0<w<t$. We want to show that $P(0,w)$ holds.Fix a $w$-set $U$ of columns and a set $Y$ of $w$ entries. We have to show that the number $x$ of

rows $f$ of $\Sigma$ satisfying $f(U)=Y$ is independent of the choice of $U$ and $Y$. Let $B \supseteq Y$ be a block of the design, $|B|=l$. The contribution of $B$ to $x$ is

$$\mu \cdot \binom{l}{t} / \binom{l}{w}.$$

It follows

$$x = \mu \cdot \sum_{B\ block, B \supseteq Y} \binom{|B|}{t} / \binom{|B|}{w}.$$

Count pairs $(T,B), |T|=t, Y \subseteq T \subseteq B, B$ *block*. Counting in two ways we get

$$\binom{v-w}{t-w} \cdot \lambda = \sum_{B\ block, B \supseteq Y} \binom{|B|-w}{t-w} = \binom{t}{w} \sum \binom{|B|}{t} / \binom{|B|}{w}.$$

It follows

$$x = \mu\lambda \binom{v-w}{t-w} / \binom{t}{w}.$$

Thus $\Sigma$ satisfies $P(0,w)$.

2. Let us prove $P(u,w)$, where $w \leq t, 0 \leq u \leq min(s,w)$. The procedure is analogous to the above. Let $E \supseteq Y = E_1 \cup E_2, |E_1| = u, |E_2| = w-u$, fix a $(w-u)$-set $U$ of columns and denote by $x$ the number of rows $f$ of $\Sigma$ satisfying $f(C) \supseteq Y, f(U) = E_2$. The contribution of a block $B \supseteq Y$ of cardinality $l$ to $x$ is

$$\binom{k}{w} \cdot \frac{\mu\binom{l}{t}}{\binom{l}{w}} / \binom{k}{w-u} = \mu \cdot \frac{\binom{k}{w}}{\binom{k}{w-u}} \cdot \frac{\binom{l}{t}}{\binom{l}{w}}.$$

Upon using the identity proved in 1. we get

$$x = \mu \cdot \frac{\binom{k}{w}}{\binom{k}{w-u}} \sum_{B \supseteq Y} \frac{\binom{|B|}{t}}{\binom{|B|}{w}} = \mu \cdot \frac{\binom{k}{w}}{\binom{k}{w-u}} \cdot \binom{v-w}{t-w} \cdot \lambda / \binom{t}{w}.$$

■

This generalizes Stinson's *design-construction*: if a design $t-(v,k,\lambda)$ and an $APA_\mu(t,k,k)$ exist, then there is an $APA_{\lambda \cdot \mu}(t,k,v)$ (see [19]). We give a first application of the $tBD$-construction.

**Theorem 3** *There is a*

$$3 - PA_6(3,4,2w+1)$$

*for every* $w \geq 2, w \neq 3$, *and a*

$$3 - PA_3(3,4,2w)$$

*for every* $w \geq 2$.

*Proof.* As an $OD_\lambda(t,k,v)$ clearly is a $t - PA_{t!\lambda}(t,k,v)$, it suffices in the case of odd $v$ to quote Teirlinck's construction of $OD_1(3,4,v)$ for every $4 \leq v \neq 7$ (see [24]).
Let $v = 2w$. By [11] there is a $3BD$ on $v$ points with block-sizes 4 and 6. By the $3BD$-construction it suffices to construct a $3 - PA_3(3,4,4)$ and a $3 - PA_3(3,4,6)$. The alternating group $A_4$ is certainly 3-homogeneous on 4 points, hence is a $3 - PA_3(3,4,4)$. The following table gives representatives for the 12 row-orbits of a $3 - PA_3(3,4,6)$ under the action of the group generated by $\rho = (\infty)(0,1,2,3,4)$ on the set $E = \{\infty,0,1,2,3,4\}$ of entries:

| | | | |
|---|---|---|---|
| $\infty$ | 0 | 4 | 2 |
| $\infty$ | 0 | 3 | 4 |
| 0 | $\infty$ | 1 | 2 |
| 0 | $\infty$ | 3 | 1 |
| 0 | 4 | $\infty$ | 3 |
| 0 | 2 | $\infty$ | 4 |
| 0 | 4 | 1 | $\infty$ |
| 0 | 2 | 3 | $\infty$ |
| 0 | 1 | 2 | 3 |
| 0 | 4 | 3 | 2 |
| 0 | 3 | 1 | 4 |
| 0 | 2 | 4 | 1 |

By Corollary 1 it suffices to check properties $P(0,3), P(1,3)$ and $P(2,3)$. The group $< \rho >$ of automorphisms has only 4 orbits on 3-subsets of entries. ■

# 3 Bounds, optimality and residues

**Definition 4** *Let $\Sigma$ be an $s - PA_\lambda(t,k,v)$, $Y$ an $i$-set of entries, where $0 < i \leq min(s, v-k)$. The* residue $res_Y(\Sigma)$ *of $\Sigma$ with respect to $Y$ is the $(C, E-Y)-$subarray of $\Sigma$ consisting of those rows of $\Sigma$ whose set of entries is disjoint from $Y$.*

**Theorem 4** *Let $\Sigma$ be an $s - PA_\lambda(t,k,v)$, $Y$ an $i$-set of entries, where $0 < i \leq min(s, v-k)$. Then $res_Y(\Sigma)$ is an*

$$(s-i) - PA_{res_i(\lambda)}(t-i, k, v-i),$$

*where*

$$res_i(\lambda) = \lambda \cdot \binom{v-k}{i} / \binom{t}{i}.$$

*Proof.* It suffices to prove the Theorem for $i = 1$. In that case $res(\lambda) = res_1(\lambda) = \lambda \cdot (v-k)/t$. So let $E \supseteq Y = E_1 \cup E_2, |E_1| = u \leq s-1, |E_2| = w - u, |Y| = w \leq t-1$, and let $e \in E - Y$. We have

$$res_e(\Sigma) = \Sigma - \Sigma^e.$$

The set $E_2$ is uniformly distributed in $\Sigma^Y$ as $\Sigma$ has property $P(u,w)$. It is uniformly distributed in $\Sigma^{Y \cup \{e\}}$ as $\Sigma$ has property $P(u+1, w+1)$. Thus $E_2$ is uniformly distributed in $res_e(\Sigma)^Y$. ■

We shall repeatedly make use of the following identity which was derived by R.M.Wilson from block-intersection numbers of designs (see [30]):

**Lemma 2 (Block-intersection identity)** *Let $0 < t \leq k \leq v, i + j \leq v$. Then the following holds:*

$$\sum_{r=0}^{j} (-1)^r \binom{j}{r} \frac{\binom{k}{i+r}}{\binom{v}{i+r}} = \frac{\binom{v-i-j}{k-i}}{\binom{v}{k}}.$$

**Definition 5** *Let $\Sigma$ be an $s - PA_\lambda(t,k,v)$. Put*

$$\lambda(0,t) = \lambda, \lambda(0,w) = \lambda(0,t)\binom{v}{t} / \binom{v}{w}, \lambda(u,w) = \lambda(0,w)\binom{k}{w} / \binom{k}{w-u},$$

*where* $0 \leq u \leq w \leq t$. *For* $0 < i \leq min(s, v-k)$ *let* $res_i(\lambda)$ *be the number defined in Theorem 4. We consider* $res_i(\lambda)$ *as the* $\lambda-$*parameter of* $res_Y(\Sigma)$ *as in Theorem 4. Therefore we put*

$$res_i(\lambda)(0,w) = res_i(\lambda)\binom{v-i}{t-i}/\binom{v-i}{w}$$

*for every* $0 \leq w \leq t-i$.

**Lemma 3** *In the situation of the foregoing Lemma, for every* $w \leq t-i$ *the following hold:*

$$res_i(\lambda)(0,w) = \lambda(0, w+i)\binom{v-k}{i}/\binom{w+i}{i}.$$

$$res_i(\lambda)(0,w) = \sum_{j=0}^{i}(-1)^j\binom{i}{j}\lambda(j, w+j).$$

*Proof.* The first equation reduces to a standard identity between binomial coefficients. After substitution of the definitions and factoring out obvious common factors, the second equation becomes

$$\sum_{j=0}^{i}(-1)^j\binom{i}{j}\binom{k}{w+j}/\binom{v}{w+j} = \frac{\binom{k}{w}\binom{v-k}{i}}{\binom{v}{w+i}\binom{w+i}{i}}.$$

Use the block-intersection identity to simplify the left-hand side. It remains to prove

$$\binom{v}{k}\binom{k}{w}\binom{v-k}{i} = \binom{v}{w+i}\binom{w+i}{i}\binom{v-w-i}{k-w}.$$

Both sides count triples $(W, K, I)$ of subsets of cardinalities $w, k$, and $i$, respectively, of a fixed $v$-set satisfying $K \supseteq W, K \cap I = \emptyset$. ∎

If $\Sigma$ is an $s - PA_\lambda(t,k,v)$, then $\lambda(u,w), 0 \leq w \leq t, 0 \leq u \leq min(w,s)$ is the number of rows of $\Sigma$ containing a fixed $w$-set $Y$ of entries and such that a fixed $(w-u)$-subset of $Y$ is in a fixed set of $w-u$ columns. Necessary conditions for the existence of an $s - PA_\lambda(t,k,v)$ are that the relevant numbers $\lambda(u,w)$ and $res_i(\lambda)(u,w)$ be integers.

**Definition 6** *Let $0 < t \leq k \leq v$. Put*

$$\mu_o(t,k,v) = \mu_o(t,v) = LCM(\binom{v}{i} | i = 1, \ldots t) / \binom{v}{t}.$$

*For $0 < s \leq t$ put*

$$\mu_s(t,k,v) = min\{\lambda | res_i(\lambda) \equiv 0 (mod\ \mu_0(t-i, v-i)); i = 0, \ldots min(s, v-k)\}.$$

*Let $\Sigma$ be an $s - PA_\lambda(t,k,v)$. We know that $\lambda \equiv 0(mod\ \mu_s(t,k,v))$. We shall call $\Sigma$* optimal *if $\lambda = \mu_s(t,k,v)$.*

Optimality may be expressed in various different ways:

**Theorem 5** *Let $(s,t,k,v,\lambda)$ be a quintuple of natural numbers, where $0 \leq s \leq t \leq k \leq v$. Then the following are equivalent:*

1. $\lambda(u,w) \in \mathbb{Z}, 0 \leq w \leq t, 0 \leq u \leq min(w,s)$.
2. $\lambda(0,w) \cdot \binom{k+1}{u} / \binom{w}{u} \in \mathbb{Z}, 0 \leq w \leq t, 0 \leq u \leq min(w,s)$.
3. $res_i(\lambda) \equiv 0(mod\ \mu_0(t-i, v-i)), i = 0, \ldots min(s, v-k)$.
4. $res_i(\lambda)(0,w) \in \mathbb{Z}, w = 0, \ldots t-i, i = 0, \ldots min(s, v-k)$.

*Proof* The equivalence of 1. and 4. follows from the inclusion-exclusion identity in Lemma 3. The equivalence of 3. and 4. follows from the first identity in Lemma 3. It remains to prove that 1. and 2. are equivalent. We first show 1. $\longrightarrow$ 2. The definition shows

$$\lambda(u,w) = \lambda(u-1,w) \cdot (\frac{k+1}{w-u+1} - 1)\ (u > 0).$$

If $\lambda(u,w)$ and $\lambda(u-1,w)$ are integers, then $\lambda(u-1,w) \cdot \frac{k+1}{w-u+1} \in \mathbb{Z}$. We shall prove by induction that

$$e(i,u,w) = \lambda(u-i,w) \cdot \binom{k+1}{i} / \binom{w-u+i}{i} \in \mathbb{Z},$$

$(0 \leq i \leq u \leq min(w,s), 0 \leq w \leq t)$. Express $\lambda(u-i,w)$ in terms of $\lambda(u-i-1,w)$, if $i < u$. This yields the equation

$$e(i,u,w) = e(i+1,u,w) - e(i,u-1,w).$$

This proves our claim by induction on $i$. Setting $i = u$ we get the statement in 2. The same equation shows that this process is reversible. We have proven the equivalence of 1. and 2. ■

It is easy to calculate the numbers $\mu_s(t, k, v)$ for small parameter-values. As an example we mention

$$\mu_1(3, 4, 2w + 1) = 6, \mu_1(3, 4, 2w) = 3.$$

It follows that the arrays constructed in Theorem 3 are optimal as APA.

**Definition 7** *Let $\Sigma$ be an $s - PA_\lambda(t, k, v), 0 \leq w \leq t, 0 \leq u \leq min(w, s)$, $u = u_+ + u_-$. Define $\lambda(u_+, u_-; w)$ to be the number of rows $Z$ of $\Sigma$ satisfying*

1. *$Z$ contains a fixed $(w - u_-)-$set $Y$ of entries.*
2. *$Z$ is disjoint from a fixed $u_- -$set of entries.*
3. *$Z$ contains a fixed $(w-u)-$set $Y' \subseteq Y$ of entries in a given $(w-u)-$set of columns.*

**Lemma 4** *Let $\Sigma$ be an $s - PA_\lambda(t, k, v), 0 \leq w \leq t, 0 \leq u \leq min(w, s), u = u_+ + u_-$. Then*

$$\lambda(u_+, u_-; w) = \sum_{i=0}^{u_-} (-1)^i \binom{u_-}{i} \lambda(u_+ + i, w - u_- + i) = \lambda \cdot \frac{\binom{v}{t}\binom{v-w}{k+u_- - w}}{\binom{v}{k}\binom{k}{w-u}}.$$

*Proof.* The first equation follows from the principle of inclusion and exclusion. It follows

$$\lambda(u_+, u_-; w) = \sum_{i=0}^{u_-} (-1)^i \binom{u_-}{i} \cdot \frac{\lambda\binom{v}{t}}{\binom{v}{w-u_-+i}} \cdot \frac{\binom{k}{w-u_-+i}}{\binom{k}{w-u}} =$$

$$= \lambda \cdot \frac{\binom{v}{t}}{\binom{k}{w-u}} \cdot \sum_{i=0}^{u_-} (-1)^i \frac{\binom{u_-}{i}\binom{k}{w-u_-+i}}{\binom{v}{w-u_-+i}}.$$

The last sum can now be calculated by Lemma 2. ■

The inclusion/exclusion-identity in Lemma 4 shows that the seemingly sharper conditions that all the numbers $\lambda(u_+, u_-; w)$ be integers are automatically satisfied if the conditions of Theorem 5 are met. The same is true for the conditions $res_i(\lambda) \equiv 0(mod\ \mu_{s-i}(t-i, v-i)), i = 0, \ldots min(s, v-k)$.

A central problem in the theory is the construction of *optimal* $0 - PA(\lfloor k/2 \rfloor, k, k)$. The number of rows of such an array is

$$\lambda^*(k) = LCM(\binom{k}{j} | j = 1, 2, \ldots k).$$

We draw a first consequence from the existence of such an array:

**Theorem 6** *Assume an (optimal)* $0 - PA_\lambda(\lfloor k/2 \rfloor, k, k)$ *exists, where*

$$\lambda = \mu_0(\lfloor k/2 \rfloor, k) = \lambda^*(k) / \binom{k}{\lfloor k/2 \rfloor}.$$

*Then arrays with the following parameters exist:*

$$t - PA_\lambda(t, k, k+i), \lambda = \mu_i(t, k, k+i),$$

*where*

$$i = 0, \ldots \lceil k/2 \rceil; t = \lfloor k/2 \rfloor + i, \ldots k.$$

*Proof.* An optimal $0 - PA(\lfloor k/2 \rfloor, k, k)$ is a $t - PA_{\lambda^*(k)/\binom{k}{t}}(t, k, k)$ for every $k \geq t \geq \lfloor k/2 \rfloor$. As $\mu_0(t, k) = \lambda^*(k)/\binom{k}{t}$ in these cases, this is optimal. Use Theorem 2 with the complete design

$$t - (k+i, k, \binom{k+i-t}{i}).$$

This yields

$$t - PA_\lambda(t, k, k+i),$$

where

$$\lambda = \lambda_{i,t,k} = \lambda^*(k) \binom{k+i-t}{i} / \binom{k}{t}.$$

We claim $\lambda_{i,t,k} = \mu_i(t, k, k+i)$, i.e. the array is optimal as an $i - PA(t, k, k+i)$ for the parameter-range in question. For $i = 0$ this is obvious. Use induction on $i$, where $i > 0$. We have $res_1(\lambda_{i,t,k}) = \lambda_{i,t,k} \cdot \frac{i}{t} = \lambda_{i-1,t-1,k}$. By induction

$$\lambda_{i-1,t-1,k} = \mu_{i-1}(t-1, k, k+i-1) =$$

$$= LCM(\mu_0(t-1-j, k+i-1-j)\binom{t-1}{j}/\binom{i-1}{j}|j = 0, 1, \ldots i-1).$$

Here we use [Theorem 5,3.] The parameters have been chosen such that $\mu_0(t-1-j, k+i-1-j) = \lambda^*(k+i-1-j)$. Setting $r = j+1$, we get

$$\lambda_{i-1,t-1,k} = LCM(\lambda^*(k+i-r) \cdot \frac{\binom{t}{r}}{\binom{i}{r}} \cdot \frac{i}{t}|r = 1, 2, \ldots i).$$

As $\lambda_{i,t,k} = \frac{t}{i} \cdot \lambda_{i-1,t-1,k}$ and $\lambda^*(k+i-r) \cdot \frac{\binom{t}{r}}{\binom{i}{r}}|\mu_i(t, k, k+i)$, it follows $\lambda_{i-1,t-1,k}|\mu_i(t, k, k+i)$. Equality follows. ∎

Optimal arrays $0-PA_\lambda(\lfloor k/2 \rfloor, k, k)$ are known to exist for $k \leq 6$. The present authors succeeded in constructing (optimal) $0-PA_3(3, 7, 7)$ and $0-PA_4(4, 8, 8)$. Details will be given elsewhere. We apply Theorem 6 to the $0-PA_\lambda(\lfloor k/2 \rfloor, k, k), k \leq 8$.

**Corollary 2** *The following arrays exist and are optimal:*

| | | | |
|---|---|---|---|
| $APA_1(1,3,3)$ | $APA_1(2,3,3)$ | $APA_3(3,3,3)$ | $APA_2(2,4,4)$ |
| $APA_3(3,4,4)$ | $APA_{12}(4,4,4)$ | $APA_1(2,5,5)$ | $APA_1(3,5,5)$ |
| $APA_2(4,5,5)$ | $APA_{10}(5,5,5)$ | $APA_3(3,6,6)$ | $APA_4(4,6,6)$ |
| $APA_{10}(5,6,6)$ | $APA_{60}(6,6,6)$ | $APA_3(3,7,7)$ | $APA_3(4,7,7)$ |
| $APA_5(5,7,7)$ | $APA_{15}(6,7,7)$ | $APA_{105}(7,7,7)$ | $APA_4(4,8,8)$ |
| $APA_5(5,8,8)$ | $APA_{10}(6,8,8)$ | $APA_{35}(7,8,8)$ | $APA_{280}(8,8,8)$ |
| $APA_2(2,3,4)$ | $APA_3(3,3,4)$ | $APA_6(3,4,5)$ | $APA_{12}(4,4,5)$ |
| $APA_3(3,5,6)$ | $APA_4(4,5,6)$ | $APA_{10}(5,5,6)$ | $APA_{12}(4,6,7)$ |
| $APA_{20}(5,6,7)$ | $APA_{60}(6,6,7)$ | $APA_{12}(4,7,8)$ | $APA_{15}(5,7,8)$ |
| $APA_{30}(6,7,8)$ | $APA_{105}(7,7,8)$ | $APA_{20}(5,8,9)$ | $APA_{30}(6,8,9)$ |
| $APA_{70}(7,8,9)$ | $APA_{280}(8,8,9)$ | $2-PA_3(3,3,5)$ | $2-PA_{12}(4,4,6)$ |
| $2-PA_6(4,5,7)$ | $2-PA_{10}(5,5,7)$ | $2-PA_{30}(5,6,8)$ | $2-PA_{60}(6,6,8)$ |
| $2-PA_{30}(5,7,9)$ | $2-PA_{45}(6,7,9)$ | $2-PA_{105}(7,7,9)$ | $2-PA_{60}(6,8,10)$ |
| $2-PA_{105}(7,8,10)$ | $2-PA_{280}(8,8,10)$ | $3-PA_{10}(5,5,8)$ | $3-PA_{60}(6,6,9)$ |
| $3-PA_{60}(6,7,10)$ | $3-PA_{105}(7,7,10)$ | $3-PA_{140}(7,8,11)$ | $3-PA_{280}(8,8,11)$ |
| $4-PA_{105}(7,7,11)$ | $4-PA_{280}(8,8,12)$ | | |

Remark that $2-PA_3(3,3,5), 2-PA_6(4,5,7)$ and $2-PA_{10}(5,5,7)$ are optimal as $APA$, $3-PA_{10}(5,5,8), 3-PA_{60}(6,7,10)$ and $3-PA_{105}(7,7,10)$ are optimal as 2-$PA$, and $4-PA_{105}(7,7,11)$ is optimal as 3-$PA$.

What happens if two of the parameters $t, k, v$ are equal? If $k = v$, we are in the case of multisets of permutations of a $k$-set. The value of the parameter $s$ is then irrelevant. A $0 - PA_\lambda(t, k, k)$ is also a $t - PA_\lambda(t, k, k)$ and may be described as a uniformly $t$-homogeneous set of permutations on $k$ letters. The theory of $0 - PA_\lambda(t, k, k)$ generalizes the theory of $t$-homogeneous *groups* of permutations. We refer to [1, 2, 4, 5, 20]. Stinson's design construction for $APA$'s shows how these multisets of permutations may be used in the construction of more general perpendicular arrays.
In the special case $t = k = v$, a $0 - PA_b(k, k, k)$ is equivalent to a $0 - PA_\lambda(\lfloor k/2 \rfloor, k, k)$ with $b = \lambda \cdot \binom{k}{\lfloor k/2 \rfloor}$ rows. Such an array is optimal if $b = \lambda^*(k)$.
In the next chapter we will make use of $s - PA_\lambda(k, k, v)$.

**Theorem 7** *Let $s \geq \lfloor k/2 \rfloor$. Then an $s - PA_\lambda(k, k, v)$ exists if and only if a $0 - PA_{\lambda/\binom{k}{\lfloor k/2 \rfloor}}(\lfloor k/2 \rfloor, k, k)$ exists.*

*Proof.* Let $\Sigma$ be an $s - PA_\lambda(k, k, v)$. The properties $P(0, k), \ldots P(s, k)$ show that for every $k$-set $F$ of entries the array $\Sigma^F$ is a $0 - PA_\mu(s, k, k)$ with $\lambda$ rows, i.e. $\lambda = \mu \cdot \binom{k}{s}$. As $s \geq \lfloor k/2 \rfloor$, a $0 - PA(s, k, k)$ is also a $0 - PA(t, k, k)$ for every $1 \leq t \leq k$. In particular $\Sigma^F$ is a $0 - PA_{\lambda/\binom{k}{\lfloor k/2 \rfloor}}(\lfloor k/2 \rfloor, k, k)$ (and a $0 - PA_\lambda(k, k, k)$).
Assume a $0 - PA_{\lambda/\binom{k}{\lfloor k/2 \rfloor}}(\lfloor k/2 \rfloor, k, k)$ or equivalently a $0 - PA_{\lambda/\binom{k}{s}}(s, k, k)$ or equivalently a $0 - PA_\lambda(k, k, k)$ exists. Use the design-construction with the complete design $k - (v, k, 1)$. This yields $k - PA_\lambda(k, k, v)$. ■

**Corollary 3** *If $\lfloor k/2 \rfloor \leq s \leq k \leq 8$, then (optimal)*

$$s - PA_{\lambda^*(k)}(k, k, v)$$

*exist for all $v \geq k$.*

*Proof.* As $k \leq 8$, we may use our (optimal) $k - PA_{\lambda^*(k)}(k, k, k)$ again. The preceding Theorem yields the arrays given in the statement of the Corollary. It also follows that $\lambda^*(k)$ is the minimum value of $\lambda$. How about optimality? We have $\lambda(u, k) = \mu_s(k, k, v)/\binom{k}{u}$. It follows from [Theorem 5, 1.] that $\lambda^*(k)$

divides $\mu_s(k,k,v)$. ■

In particular we get that $APA_1(1,1,v), 2-PA_2(2,2,v)$ and $3-PA_3(3,3,v)$ always exist and are optimal as $APA$.

# 4 An application in cryptography

We use the model of a secrecy and authentication-system based on an injective $(C,E)$-array $\Sigma$ as described in [19]. Thus the columns are interpreted as *source states*, the rows as *keys* and the entries as *messages*. The source is assumed to be a stationary probability-space, i.e. every source state c occurs with a fixed probability $Pr(c)$. Each key is an injective mapping from the source states into the messages. Each key is used with the same probability $1/b$. If row $\sigma$ is chosen as key, then source state (column) $c$ is encrypted into $\sigma(c) \in E$. Once a key has been chosen it will be used for a certain number of messages. It was shown in [19] that a $0-PA_\lambda(t,k,v)$ yields perfect $t$-fold secrecy. We consider authentication. Let us speak of a *spoofing attack* of *order* $w-u$ and *strength* $u$ if the opponent observes $w-u$ distinct messages and then sends $u$ more messages himself. His goal is to have all of his messages accepted. The following is obvious:

**Proposition 1** *Let $Pd$ (the* probability of deception*) be the probability of success of a spoofing attack of order $w-u$ and strength $u$. If the opponent follows an optimal strategy, then*

$$Pd \geq \binom{k-w+u}{u} / \binom{v-w+u}{u}.$$

**Theorem 8** *If $\Sigma$ is an $s-PA_\lambda(t,k,v)$, then the opponent's probability $Pd$ of success in a spoofing attack of order $w-u$ and strength $u$ is*

$$Pd = \binom{k-w+u}{u} / \binom{v-w+u}{u}$$

*whenever $w \leq t, u \leq min(s,w)$.*

*Proof.* Let $E_0 \subset E$ be the $(w-u)$-set of messages observed by the opponent, $E_1$ the $u$-set of messages inserted into the channel by the opponent,

$E_0 \cap E_1 = \emptyset$. Clearly the probability $p$ of success of the attack is a conditional probability:

$$p = \frac{\sum_{T:T(C)\supseteq E_0\cup E_1} Pr(T)Pr(T^{-1}(E_0))}{\sum_{T:T(C)\supseteq E_0} Pr(T)Pr(T^{-1}(E_0))}.$$

Here $T$ runs through the keys. Further $Pr(T) = 1/b$ by construction. Thus the denominator is $\frac{1}{b}\lambda(0, w-u)\sum_{Y\subseteq C,|Y|=w-u} Pr(Y) = \frac{1}{b}\lambda(0, w-u)$. The numerator is

$$\frac{1}{b}\sum_{Y\subseteq C,|Y|=w-u} Pr(Y)|\{T|T(Y) = E_0, T(C) \supseteq E_1\}|.$$

Property $P(u, w)$ shows that this simplifies to $\frac{1}{b}\sum_{Y\subseteq C,|Y|=w-u} Pr(Y)\lambda(u, w) = \frac{1}{b}\lambda(u, w)$. It follows

$$p = \frac{\lambda(u, w)}{\lambda(0, w-u)}.$$

By Definition 5 we have

$$p = \frac{\binom{v}{w-u}\binom{k}{w}}{\binom{v}{w}\binom{k}{w-u}} = \binom{k-w+u}{u}\Big/\binom{v-w+u}{u}.$$

As this holds for every choice of $E_1$, we are done. ■

We conclude that an $s - PA_\lambda(t, k, v)$ yields the best possible protection against spoofing attacks if the same key is used for no more than $t$ messages and the opponent inserts no more than $s$ messages into the channel while the same key is being used for encryption. All this is independent of the probability-distribution on the source states. The case $s = 1$, corresponding to $APA$'s has been discussed in [19].

# 5 Blowing-up

**Theorem 9** *Assume an $s - PA_\lambda(t, k, v)$ and an $x - PA_\mu(y, l, v-k)$ exist, where $x = min(l, s), y = min(l, t)$. Then there is an*

$$s - PA_{\lambda\mu\binom{v-k}{y}}(t, k + l, v).$$

*Proof.* Let $A$ be an $s - PA_\lambda(t,k,v)$, defined on the set $E$ of entries. For every row $Z$ of $A$ let $B(Z)$ be an $x - PA_\mu(y,l,v-k)$ defined on the set $E - Z$ of entries. Define an array $C(Z)$ with $k+l$ columns and $\mu \cdot \binom{v-k}{y}$ rows, where the restriction of each row to the first $k$ coordinates equals $Z$, and the restriction of $C(Z)$ to the last $l$ columns equals $B(Z)$. Define the array $C$ as the union of $C(Z)$ over all rows $Z$ of $A$. We claim that $C$ is an $s - PA_{\lambda\mu\binom{v-k}{y}}(t,k+l,v)$.
Let $E_1, E_2 \subseteq E, |E_1| = s, |E_2| = t-s, E_1 \cap E_2 = \emptyset$. Further let $S$ be a $(t-s)$-set of columns, $S_1$ the intersection of $S$ with the $k$ first columns of $C$, put $|S_1| = n$. Denote by $x = x(S)$ the number of rows of $C$ containing $E_1 \cup E_2$, and with the elements of $E_2$ in the columns of $S$. We have to show $x(S) = \lambda\mu\binom{v-k}{y}\binom{k+l}{t}/\binom{k+l}{t-s}$. Use the notation of section 3, where $\lambda_A(u,w)$ and $\lambda_B(u,w)$ denote the parameters of the arrays $A$ and $B(Z)$, respectively. As a natural generalization of Definition 7 denote by $\lambda(U_+, U_-; W; S)$ the number of rows $Z$ (of a given array) satisfying

- $W - U_- \subseteq Z$
- $Z \cap U_- = \emptyset$
- The entries in $W - (U_+ \cup U_-)$ occur in the given set $S$ of columns.

Put

$$x_m = \sum_{F_1 \subseteq E_1, |F_1|=m} \; \sum_{F_2 \subseteq E_2, |F_2|=n} \lambda_A(F_1, (E_1 - F_1) \cup (E_2 - F_2); E_1 \cup E_2; S_1) \cdot$$

$$\cdot \lambda_B(s-m, t-m-n).$$

As $(s-m) + (t-s-n) \leq l$, we have to consider the range $t - l - n \leq m \leq s$. Thus

$$x(S) = \sum_{m=t-l-n}^{s} x_m.$$

Fix $m$. Use the principle of inclusion and exclusion. We get

$$x_m = \lambda_B(s-m, t-m-n) \cdot \sum_{i=0}^{s-m} \sum_{j=0}^{t-s-n} (-1)^{i+j} \binom{s}{m}\binom{s-m}{i}\binom{t-s}{n+j}\binom{k-n}{j} \cdot$$

$$\cdot \lambda_A(m+i, m+n+i+j).$$

Upon reordering terms and substituting the value of $\lambda_A(m+i, m+n+i+j)$ we obtain

$$x_m = \lambda \cdot \binom{v}{t}\binom{s}{m}\lambda_B(s-m, t-m-n)\sum_{j=0}^{t-s-n}(-1)^j \frac{\binom{t-s}{n+j}\binom{k-n}{j}}{\binom{k}{n+j}} \cdot$$

$$\cdot \sum_{i=0}^{s-m}(-1)^i \binom{s-m}{i}\binom{k}{m+n+i+j} / \binom{v}{m+n+i+j}.$$

The last sum can be calculated by Lemma 2. We get

$$x_m = \frac{\lambda \cdot \binom{v}{t}\binom{s}{m}}{\binom{v}{k}}\lambda_B(s-m, t-m-n) \cdot \sum_{j=0}^{t-s-n}(-1)^j \frac{\binom{t-s}{n+j}\binom{k-n}{j}}{\binom{k}{n+j}} \binom{v-(n+s+j)}{k-(m+n+j)}.$$

Use $\frac{\binom{k-n}{j}}{\binom{k}{n+j}} = \frac{\binom{n+j}{n}}{\binom{k}{n}}$ and $\binom{t-s}{n+j}\binom{n+j}{n} = \binom{t-s}{n}\binom{t-s-n}{j}$. It follows

$$x_m = \frac{\lambda \cdot \binom{v}{t}\binom{s}{m}\binom{t-s}{n}}{\binom{v}{k}\binom{k}{n}}\lambda_B(s-m, t-m-n)\sum_{j=0}^{t-s-n}(-1)^j \binom{t-s-n}{j}\binom{v-(n+s+j)}{k-(m+n+j)}.$$

Substitute $\binom{v-s}{k-m} \cdot \binom{k-m}{m+j} / \binom{v-s}{m+j}$ for the last binomial number above. Upon reordering terms and making use of Lemma 2 again, we get

$$x_m = \lambda \cdot \frac{\binom{v}{t}\binom{s}{m}\binom{t-s}{n}\binom{v-t}{k-m-n}}{\binom{v}{k}\binom{k}{n}}\lambda_B(s-m, t-m-n).$$

Substitute the value of $\lambda_B(s-m, t-m-n)$ as given in Definition 5:

$$x_m = \lambda\mu \cdot \binom{v-k}{y}\frac{\binom{v}{t}\binom{t-s}{n}}{\binom{v}{k}\binom{k}{n}\binom{l}{t-s-n}} \cdot \binom{s}{m}\binom{v-t}{k-m-n}\binom{l}{t-m-n} / \binom{v-k}{t-m-n}.$$

The last terms simplify: $\binom{v-t}{k-m-n}\binom{l}{t-m-n} / \binom{v-k}{t-m-n} = \binom{v-t}{k-t}\binom{l+k-t}{k-m-n} / \binom{l+k-t}{k-t}$. After substituting this expression and simplifying again ($\binom{v}{t}\binom{v-t}{k-t} / \binom{v}{k} = \binom{k}{t}$), we get

$$x_m = \lambda\mu \cdot \binom{v-k}{y}\frac{\binom{k}{t}\binom{t-s}{n}}{\binom{k}{n}\binom{l}{t-s-n}\binom{l+k-t}{k-t}}\binom{s}{m}\binom{l+k-t}{k-m-n}.$$

By a well-known identity

$$\sum_{m=t-l-n}^{s} \binom{s}{m}\binom{l+k-t}{k-m-n} = \binom{l+k+s-t}{k-n}.$$

We get

$$x(S) = \sum_{m=t-l-n}^{s} x_m = \lambda\mu \cdot \binom{v-k}{y} \frac{\binom{k}{t}\binom{t-s}{n}\binom{l+k+s-t}{k-n}}{\binom{k}{n}\binom{l}{t-s-n}\binom{l+k-t}{k-t}}.$$

After simplification we obtain

$$x(S) = \lambda\mu\binom{v-k}{y}\binom{k+l}{t}/\binom{k+l}{t-s} = \lambda_C(s,t),$$

as desired. ■

**Theorem 10** *Assume an $s - PA_\lambda(t,u,k)$, an $x - PA_\nu(y,l,v-k)$ and a design $t-(v,k,\mu)$ exist, where $x = min(l,s), y = min(l,t)$. Then there is an*

$$s - PA_{\lambda\mu\nu\binom{v-k}{y}}(t, u+l, v).$$

*Proof.* Let $\mathcal{D}$ be a design $t-(v,k,\lambda)$, defined on the set $E$. For each block $D$ of $\mathcal{D}$ let $A(D)$ be an $s - PA_\lambda(t,u,k)$ defined on $D$ and $B(D)$ an $x - PA_\nu(y,l,v-k)$ defined on $E - D$. For every row $Z$ of $A(D)$ define an array $C(Z,D)$ with $u+l$ columns and $\nu \cdot \binom{v-k}{y}$ rows, where the restriction of each row to the first $u$ coordinates equals $Z$, and the restriction of $C(Z,D)$ to the last $l$ columns equals $B(D)$. Define the array $C$ as the union of $C(Z,D)$ over all blocks $D$ of $\mathcal{D}$ and all rows $Z$ of $A(D)$. We claim that $C$ is an $s - PA_{\lambda\mu\nu\binom{v-k}{y}}(t,u+l,v)$. The proof is very similar to the proof of the preceding Theorem, but it is easier.
As before let $E_1, E_2 \subseteq E, |E_1| = s, |E_2| = t-s, E_1 \cap E_2 = \emptyset$. Further let $S$ be a $(t-s)$-set of columns, $S_1$ the intersection of $S$ with the $k$ first columns of $C$, put $|S_1| = n$. Denote by $x = x(S)$ the number of rows of $C$ containing $E_1 \cup E_2$, and with the elements of $E_2$ in the columns of $S$. We have to show $x(S) = \lambda\mu\nu\binom{v-k}{y}\binom{u+l}{t}/\binom{u+l}{t-s}$. Let $\lambda_{\mathcal{D}}(i,j), i+j \leq t$, be the number of blocks

of the design $\mathcal{D}$ intersecting a given $(i+j)$-set in a fixed $i$-set. By a well-known theorem we have

$$\lambda_{\mathcal{D}}(i,j) = b(\mathcal{D})\binom{v-i-j}{k-i}/\binom{v}{k},$$

where $i+j \leq t$ and $b(\mathcal{D})$ denotes the number of blocks. With the notation of the proof of the foregoing theorem put

$$x_m = \sum_{F_1 \subseteq E_1, |F_1|=m} \sum_{F_2 \subseteq E_2, |F_2|=n} \lambda_{\mathcal{D}}(m+n, t-n-m)\lambda_A(m, m+n)\lambda_B(s-m, t-m-n).$$

We have to calculate $x(S) = \sum_m x_m$. Fix $m$. By substituting the values of the $\lambda-$parameters and reordering terms we get

$$x_m = \lambda\mu\nu\binom{v-k}{y} \cdot \frac{\binom{t-s}{n}\binom{v}{t}}{\binom{v}{k}\binom{u}{n}\binom{l}{t-s-n}} \cdot \frac{\binom{s}{m}\binom{v-t}{k-m-n}\binom{u}{m+n}\binom{l}{t-m-n}}{\binom{k}{m+n}\binom{v-k}{t-m-n}}.$$

This simplifies to

$$x_m = \lambda\mu\nu\binom{v-k}{y} \cdot \frac{\binom{t-s}{n}\binom{u}{t}}{\binom{u}{n}\binom{l}{t-s-n}\binom{l+u-t}{l}} \cdot \binom{s}{m}\binom{l+u-t}{u-m-n}.$$

As $\sum_m \binom{s}{m}\binom{l+u-t}{u-m-n} = \binom{l+u+s-t}{u-n}$, we get

$$x(S) = \sum_m x_m = \lambda\mu\nu\binom{v-k}{y} \cdot \frac{\binom{t-s}{n}\binom{u}{t}}{\binom{u}{n}\binom{l}{t-s-n}\binom{l+u-t}{l}} \cdot \binom{l+u+s-t}{u-n}.$$

This expression is easily simplified. We get

$$x(S) = \lambda\mu\nu\binom{v-k}{y}\binom{u+l}{t}/\binom{u+l}{t-s} = \lambda_C(s,t),$$

as desired. ■

Theorem 10 is applicable even if $l=0$. In that case one of the ingredients degenerates to a $0-PA_1(0,0,v-k)$, which should be interpreted as the empty array. We obtain:

**Corollary 4** *If an $s-PA_\lambda(t,u,k)$ and a design $t-(v,k,\mu)$ exist, then there is an*

$$s - PA_{\lambda\mu}(t,u,v).$$

Case $s=1$ of this Corollary is Tran's generalization of

Stinson's design-construction (see [27]). In case $l = 1$ we may use the existence of $1 - PA_1(1,1,v)$ for every $v$ and get as a Corollary of Theorem 10:

**Corollary 5** *If an $s - PA_\lambda(t,u,k)$ and a design $t-(v,k,\mu)$ exist, then there is an*

$$s - PA_{\mu\lambda(v-k)}(t,u+1,v).$$

The special case $s = 1, k = u$ of this Corollary is Tran's theorem [27],2.8. Upon specializing to $s = 1, k = u, v = k+1$ and the complete design we get [27],2.2:

**Corollary 6** *If there is an $APA_\lambda(t,k,k)$, then there is an $APA_{\lambda(k+1-t)}(t,k+1,k+1)$.*

It is worth noting that this Corollary may produce optimal APA in nontrivial situations. As an example, when applied to an $APA_1(3,5,5)$ we get an (optimal) $APA_3(3,6,6)$. An $APA_1(3,5,5)$ is the same as an $APA_1(2,5,5)$ and can be found as a subset of the group $AGL_2(5)$ of order 20 (see [19]). Remark that $APA_3(3,6,6)$ has been constructed before ([13, 2]). Three more such situations occur in cases $t \in \{4,5\}$. We use the notation $A \longrightarrow B$ to denote that the (eventual) existence of array $A$ entails the existence of $B$ :

$$APA_2(4,9,9) \longrightarrow APA_{12}(4,10,10)$$

$$APA_1(4,15,15) \longrightarrow APA_{12}(4,16,16)$$

$$APA_2(5,9,9) \longrightarrow APA_{10}(5,10,10).$$

All the parameters listed above are optimal, but none of these arrays has been constructed that far. Observe further that $APA_2(4,9,9)$ and $APA_2(5,9,9)$ are different names for the same structure.

Case $l = 1$ of Theorem 9 yields:

**Corollary 7** *The existence of $s - PA_\lambda(t,k,v)$ implies the existence of*

$$s - PA_{\lambda(v-k)}(t,k+1,v).$$

This last Corollary appears to be new even in the cases $s = 0$ and $s = 1$ of inductive $PA$'s and $APA$'s, respectively. It has some interesting consequences:

**Proposition 2** *1. If for some (necessarily odd) $k$ there is an $APA_1(2, k, k+2)$, then an (optimal) $APA_2(2, k+1, k+2)$ and an $APA_2(2, k+2, k+2)$ exist.*

2. *If there is an $APA_1(3, 6x+5, 6x+8)$, then there is an (optimal) $APA_3(3, 6x+6, 6x+8)$.*

3. *If there is an $APA_1(3, 6x+5, 6x+11)$, then there is an (optimal) $APA_6(3, 6x+6, 6x+11)$.*

4. *If there is an $APA_3(3, 6x+5, 6x+7)$, then there is an (optimal) $APA_6(3, 6x+6, 6x+7)$ and an $APA_6(3, 6x+7, 6x+7)$.*

5. *If there is an $APA_4(4, 5, 8)$, then there is an (optimal) $APA_{12}(4, 6, 8)$.*

6. *If there is an $APA_2(4, 5, 11)$, then there is an (optimal) $APA_{12}(4, 6, 11)$.*

Another application of Theorem 9 yields:

**Corollary 8** • *If there is an $s - PA_\lambda(t, k-2, k)$, then there is an $s - PA_{2\cdot\lambda}(t, k, k)$.*

- *If there is an $s - PA_\lambda(t, k-3, k)$, then there is an $s - PA_{3\cdot\lambda}(t, k, k)$.*

We mention some variants of our main theorems in this section:

**Theorem 11** *Assume an $s - PA_\lambda(t, u, k)$ and a design $t - (v, k, \mu)$ exist.*

1. *If in addition an $x - PA_\nu(y, l, k-u)$ exists, where $x = min(l, s), y = min(l, t)$, then there is an*

$$s - PA_{\lambda\mu\nu\binom{k-u}{y}}(t, u+l, v).$$

2. *If in addition an* $x - PA_\nu(y, l, v-u)$ *exists, where* $x = min(l, s), y = min(l, t)$, *then there is an*

$$s - PA_{\lambda\mu\nu\binom{v-u}{y}}(t, u+l, v).$$

3. *If in addition there is an* $x - PA_\nu(y, l, v-u)$ *containing an* $x - PA_\chi(y, l, v-k)$, *then there is an* $s - PA_{\lambda\mu\nu\binom{v-u}{y}}(t, u+l, v)$ *containing an* $s - PA_{\lambda\mu\chi\binom{v-k}{y}}(t, u+l, v)$.

*Proof.*

1. Application of Theorem 9 yields an $s - PA_{\lambda\nu\binom{k-u}{y}}(t, u+l, k)$. Apply then the design-construction.

2. The design-construction yields $s - PA_{\lambda\mu}(t, u, v)$. Apply Theorem 9 to get the result.

3. Containment of two arrays is to be interpreted in the usual multiset-sense. Under the present assumption the constructions of Theorem 10 and of 1. above yield arrays with the parameters in question, which are contained in each other. The (multiset-)difference yields an

$$s - PA_{\lambda\mu\{\nu\binom{v-u}{y} - \chi\binom{v-k}{y}\}}(t, u+l, v).$$

We note the following Corollary to case 1. of the preceding Theorem:

**Corollary 9** *Assume an* $s - PA_\lambda(t, u, k)$ *and a design* $t-(v, k, \mu)$ *exist. then there is an*

$$s - PA_{\lambda\mu(k-u)}(t, u+1, v).$$

This is better than Corollary 5 if $k - u < v - k$.

The constructions of Theorems 9 and 10 also work for ordered designs. The proofs are similar but much easier. We shall omit them here:

**Theorem 12**

- *If an* $OD_\lambda(t, k, v)$ *and an* $OD_\mu(y, l, v-k)$ *exist, where* $y = min(t, l)$, *then there is an*

$$OD_{\lambda\mu\binom{v-k}{y}\cdot y!}(t, k+l, v).$$

- *If an $OD_\lambda(t,u,k)$, a design $t-(v,k,\mu)$ and an $OD_\nu(y,l,v-k)$ exist, where $y = min(t,l)$, then there is an*

$$OD_{\lambda\mu\nu\binom{v-k}{y}\cdot y!}(t, u+l, v).$$

# 6 Restriction

In this section we study conditions on a set $L$ of columns of an $s-PA$ $\Sigma$ which ensure that the restriction $\Sigma_L$ of $\Sigma$ to the set $L$ of columns is again an $s-PA$.

**Definition 8** *Let $\Sigma$ be an $s-PA_\lambda(t,k,v)$. If for every set $L$ of columns the restriction $\Sigma_L$ is an $x-PA(y,l,v)$, where $x = min(l,s), y = min(l,t), |L| = l$, then we say that $\Sigma$ has the* restriction-property, *short: property (R).*

It is obvious that an $OD_\lambda(t,k,v)$ is a $t-PA_{\lambda\cdot t!}(t,k,v)$ with property $(R)$. We draw an immediate consequence: as the affine group $AGL(1,q) = \{\tau \longrightarrow \alpha\tau + \beta | 0 \neq \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q\}$ is an $OD_1(2,q,q)$ and an $APA_2(2,q,q)$ with property $(R)$, restriction always works.

**Corollary 10** *If $q$ is a prime-power and $2 \leq k \leq q$, then an $APA_2(2,k,q)$ exists.*

As

$$\mu_1(2,k,v) = \begin{cases} 1 & \text{if } k \cdot v \text{ odd} \\ 2 & \text{otherwise,} \end{cases}$$

this is optimal except when $k$ and $q$ both are odd.

**Theorem 13** *Let $\Sigma$ be an $s-PA_\lambda(t,k,v)$. Then the following are equivalent:*

- *$\Sigma$ has property (R).*

- *For every $u \leq w \leq t, w-u \leq s$, every $w$-set $W$ of entries and every $w$-set $L$ of columns, the array $\Sigma_L^W$ is a $0-PA(w-u,w,w)$.*

*(Here we omit parameter "$\lambda$" when we are not interested in its value.)*

*Proof.* Let $\Sigma$ have property $(R)$, let $u, w, L, W$ as above. It follows that $\Sigma_L$ is an $x - PA(w, w, v)$, where $x = Min(w, s)$. By definition of an $s - PA$ every $u$-subset of $W$ is uniformly distributed in $\Sigma_L^W$. It follows that the multiset $\Sigma_L^W$ of permutations is a
$PA(w - u, w, w)$.
The converse is rather obvious. ■

**Corollary 11** *If an $s - PA_\lambda(t, k, v)$ has property (R), then we have*

$$\lambda(0, w) \equiv 0(mod \binom{w}{u}\mu_0(w - u, w))$$

*for every $0 \leq u \leq w \leq t, w - u \leq s$.*

**Definition 9** *Let $\Sigma$ be an $s - PA_\lambda(t, k, v)$. Define $H = H(\Sigma)$ as the group of permutations on the columns of $\Sigma$ which induce automorphisms of $\Sigma$. Sometimes $H$ is called the* conjugate-invariant group *of $\Sigma$.*

**Corollary 12** *Let $\Sigma$ be an $s - PA_\lambda(t, k, v)$. For every subset $L$ of columns of $\Sigma$ denote by $H(\Sigma)_L$ the group of permutations of $L$ induced by the set-stabilizer of $L$ in the group $H(\Sigma)$.*
*If $H(\Sigma)_L$ contains the alternating group on $L$ for every $L$,$|L| \leq t$ and $|H(\Sigma)_L| = 2$ for $|L| = 2$, then $\Sigma$ has property (R).*

We apply this to the group $\Sigma = PSL_2(q)$, which is an $APA_3(3, q+1, q+1)$ if $q \equiv 3(mod\ 4)$. As $PSL_2(q)$ is a subgroup of $H(\Sigma)$ and induces $Z_3$ on triples, $Z_2$ on pairs of columns, we can apply the preceding Corollary and obtain:

**Theorem 14** *If $q$ is a prime-power, $q \equiv 3 (mod\ 4)$, then $PSL_2(q)$ is an $APA_3(3, q+1, q+1)$ with property (R). It follows that*

$$APA_3(3, k, q+1)$$

*exist for every $3 \leq k \leq q+1$.*

When is this optimal? The following values of the $\mu_1-$ function are easily calculated:

$$\mu_1(3, 2l, 2w) = \begin{cases} 1 & \text{if } w \equiv l \equiv 1 (mod\ 3) \\ 3 & \text{otherwise.} \end{cases}$$

$$\mu_1(3, 2l, 2w+1) = \begin{cases} 2 & \text{if } w \equiv 2 (mod\ 3), l \equiv 1 (mod\ 3) \\ 6 & \text{otherwise.} \end{cases}$$

$$\mu_1(3, 2l+1, 2w) = \begin{cases} 1 & \text{if } w \equiv 1 (mod\ 3), l \equiv 2 (mod\ 3) \\ 3 & \text{otherwise.} \end{cases}$$

$$\mu_1(3, 2l+1, 2w+1) = \begin{cases} 1 & \text{if } w \equiv l \equiv 2 (mod\ 3) \\ 3 & \text{otherwise.} \end{cases}$$

As $PGL_2(q)$ is an $OD_1(3, q+1, q+1)$ and thus an $APA_6(3, q+1, q+1)$ with property $(R)$ for every prime-power $q$, we obtain the following optimal $APA$'s:

**Theorem 15** *The following arrays exist:*

- $APA_6(3, 2l, 2^f+1), l \geq 2, f \geq 1,$ *which is optimal except when* $\{f\ even, l \equiv 1 (mod\ 3)\}$.
- $APA_3(3, k, q+1), 3 \leq k \leq q+1, q\ prime-power, q \equiv 3 (mod\ 4),$ *which is optimal except when* $\{q \equiv 7 (mod\ 12), k \equiv 2 (mod\ 3)\}$.

We concentrate on $APA$'s with $t = 2$ now.

**Definition 10** *Let $\Sigma$ be an $APA_\lambda(2, k, v)$. The* transitive kernel *$C_0(\Sigma)$ is the set of columns $c$ with the property that for every column $c' \neq c$ the restriction $\Sigma_{\{c,c'\}}$ is an $OD_{\lambda/2}(2, 2, v)$.*

Thus column $c$ belongs to the transitive kernel if for every pair of columns one of which is $c$ every *ordered* pair of entries occurs the same number of times. This number is then necessarily $\lambda/2$. Hence a nontrivial transitive kernel can exist only if $\lambda$ is even.

**Theorem 16** *Let $\Sigma$ be an $APA_\lambda(2,k,v)$ with set $C$ of columns. For every $c \in C$ the following are equivalent:*

- *$c \in C_0(\Sigma)$*
- *The restriction $\Sigma_{C-\{c\}}$ is an $APA_\lambda(2,k-1,v)$.*

*Proof.* Let $\{a,b\}$ be a pair of entries, $c' \neq c$ a column of $\Sigma$. There are exactly $\binom{k}{2}\lambda$ rows of $\Sigma$ containing $a$ and $b$. Property $P(1,2)$ shows that there are exactly $(k-1)\lambda/2$ rows of $\Sigma$ containing $b$ and having $a$ in column $c'$. Assume now $\Sigma_{C-\{c\}}$ is an $APA_\lambda(2,k-1,v)$. The same argument, when applied to $\Sigma_{C-\{c\}}$, shows that there are exactly $(k-2)\lambda/2$ rows of $\Sigma_{C-\{c\}}$ containing $b$ and having $a$ in column $c'$.
We conclude that exactly $(k-1)\lambda/2-(k-2)\lambda/2=\lambda/2$ rows of $\Sigma$ have $a$ in column $c'$ and $b$ in column $c$. Thus $\Sigma_{\{c,c'\}}$ is an $OD_{\lambda/2}(2,2,v)$. This argument is clearly reversible. ∎

**Corollary 13** *Let $\Sigma$ be an $APA_\lambda(2,k,v)$ with set $C$ of columns, $L \subseteq C_0(\Sigma)$ a set of columns contained in the transitive kernel. Then $\Sigma_{C-L}$ is an $APA_\lambda(t,k-|L|,v)$.*

We specialize to arrays $APA_2(2,k,k)$, equivalently $0-PA_2(2,k,k)$. In case $v=k$ we may identify the set of columns with the set of entries. We view an $APA_\lambda(t,k,k)$ as a multiset of permutations of a $k$-set.

**Proposition 3 (Double-coset construction)** *Let $E$ be a $k$-set, $H$ a permutation-group of order k-1 on $E$ having one fixed point $c$ and an orbit of length k-1. Assume there is a permutation $\sigma$ of $E$ such that*

$$\Sigma = H \cup H\sigma H$$

*is an $APA_2(2,k,k)$. (Equivalently: $\Sigma = H\Sigma H$)*
*Then the column corresponding to $c$ is contained in the transitive kernel.*

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

In [5] the double-coset construction has been used to get an $APA_2(2,6,6)$. The present authors constructed an $APA_2(2,12,12)$ using the same method [7]. By the preceding Proposition the transitive kernel is nonempty in both cases. We conclude:

**Corollary 14** *There exist (optimal)*

$$APA_2(2,5,6)$$

*and*

$$APA_2(2,11,12)$$

# 7 The affine group

Let $G = AGL_1(q)$, where $q$ is a prime-power. We know that $G$ is an $APA_2(2,q,q)$. This is optimal if $q$ is a power of 2.

**Definition 11** *Let $q$ be an odd prime-power. A* half-system *of $\mathbb{F}_q$ is a subset $U \subset \mathbb{F}_q^*$ satisfying*

$$|\{x,-x\} \cap U| = 1$$

*for every $0 \neq x \in \mathbb{F}_q$.*

The total number of half-systems of $\mathbb{F}_q$ is clearly $2^{(q-1)/2}$. If $U$ is a half-system and $0 \neq \alpha \in \mathbb{F}_q^*$, then $\alpha \cdot U$ is a half-system, too. Furthermore the set $U^{-1}$ of reciprocals is a half-system if $U$ is. Remark that the set $\mathbb{F}_q^{*2}$ is a half-system if and only if $q \equiv 3 (mod\, 4)$.
It was shown in [5] that

$$E_U(G) = \{\tau \longrightarrow \alpha\tau + \beta | \alpha \in U, \beta \in \mathbb{F}_q\}$$

is an $APA_1(2,q,q)$ if and only if $U$ is a half-system of $\mathbb{F}_q$.
We want to study the question when the restriction of $E_U(G)$ to a set of $k$ columns is an $APA_1(2,k,q)$. Recall that this is conceivable only if $k$ is odd.

**Definition 12**
- *Let $U$ be a half-system of $\mathbb{F}_q$, $K \subseteq \mathbb{F}_q$. Define a directed graph, more specifically a* tournament *$\Gamma(K,U)$ with $K$ as set of vertices, where the ordered pair $(c,c')$ is an edge if and only if $c - c' \in U$.*

- *Call a directed graph* $\Gamma$ balanced *if for every vertex* $x$ *indegree and outdegree of* $x$ *are the same.*

**Lemma 5** *Let* $G = AGL_1(q)$*,* $q$ *odd,* $U$ *a half-system of* $\mathbb{F}_q, K \subseteq \mathbb{F}_q$*. Then the following are equivalent:*

- *The restriction* $E_U(G)_K$ *is an* $APA_1(2,k,q)$*.*
- *The tournament* $\Gamma(K, \alpha \cdot U^{-1})$ *is balanced for every* $0 \neq \alpha \in \mathbb{F}_q$*.*

*Proof.* Restrictions of $PA$'s are certainly $PA$'s. We only have to take care of property $P(1,2)$. Put $K = \{\tau_1, \dots \tau_k\}$, $k$ odd, let $a, b \in \mathbb{F}_q, a \neq b$. Consider the system of equations

$$u\tau_i + \beta = a$$

$$u\tau_j + \beta = b$$

(where $\beta \in \mathbb{F}_q, u \in U, i \neq j$).Fix $i$. Property $P(1,2)$ holds if and only if there are exactly $(k-1)/2$ values of $j$ for which a solution $(u, \beta)$ exists. Equivalently we demand that $(\tau_i - \tau_j)/(a-b) \in U^{-1}$ for $(k-1)/2$ values of $j \neq i$, and consequently $(\tau_i - \tau_j)/(a-b) \in -U^{-1}$ for the remaining $(k-1)/2$ values of $j \neq i$. Equivalently we demand that the tournament $\Gamma(K, (a-b)U^{-1})$ be balanced. As this has to hold for every pair $a, b$, we arrive at the claim of the Lemma. ∎

Remark that $\Gamma(K, U)$ is balanced if and only if $\Gamma(K, -U)$ is. In case $q \equiv 3(mod\ 4)$ we may take $U = \mathbb{F}_q^{*2}$. Then $U^{-1} = U$ and $\{\alpha U, -\alpha U\} = \{\mathbb{F}_q^{*2}, -\mathbb{F}_q^{*2}\}$ for every $\alpha \in \mathbb{F}_q^*$. In this case the criterium of the preceding Lemma simplifies:

**Corollary 15** *Let* $q$ *be a prime-power,* $q \equiv 3(mod\ 4), U = \mathbb{F}_q^{*2}, K \subseteq \mathbb{F}_q$*,* $|K| = k$*. Then the following are equivalent:*

- $E_U(G)_K$ *is an* $APA_1(2,k,q)$*.*
- *The tournament* $\Gamma(K, \mathbb{F}_q^{*2})$ *is balanced.*

We quote a theorem of R.M.Wilson's ([28]):

**Theorem 17** *Let $q$ be a prime-power, $q-1 = e \cdot f, H_0, H_1, \ldots H_{e-1}$ the cosets of the subgroup of order $f$ ( and index $e$) of $\mathbb{F}_q^*$. For some natural number $k$ and for $1 \le i < j \le k$ let $C(i,j) \in \{H_0, H_1, \ldots H_{e-1}\}$ be given. Then the following holds:*
*If $q > e^{k(k-1)}$, then there is an ordered $k$-tuple $(x_1, x_2, \ldots, x_k)$ of elements $x_j \in \mathbb{F}_q$ satisfying $x_i - x_j \in C(i,j), 1 \le i < j \le k$.*

If we apply this in the situation of the preceding Corollary we get:

**Theorem 18** *Let $q \equiv 3 (mod\, 4)$ be a prime-power, $k$ odd, $q > 2^{k(k-1)}$. Then there is a $k$-set $K \subset \mathbb{F}_q$ such that $(E_{F_q^{*2}}(AGL_1(q)))_K$ is an $APA_1(2,k,q)$.*

Theorem 17 may as well be applied when $q \equiv 1 (mod\, 4)$. Let $q = 2^i t + 1$, where $t$ is odd, $T$ the subgroup of order $t$ of $\mathbb{F}_q^*$. Choose the half-system $U$ as a union of cosets of $T$, i.e. $U = TU$. As $T$ has odd order, such a half-system certainly exists. Let $K \subset \mathbb{F}_q, |K| = k$. The condition that $\Gamma(K, \alpha \cdot U^{-1})$ be balanced for every $0 \neq \alpha \in \mathbb{F}_q$ will certainly be satisfied if for every $x \in K$ the set of differences $x - y, y \in K, y \neq x$ is equally distributed on the cosets of $T$. We apply Theorem 17 and get:

**Theorem 19** *Let $q = 2^i t + 1$ be a prime-power, $t$ odd, $T$ the subgroup of order $t$ of $\mathbb{F}_q^*, k \equiv 1 (mod\, 2^i)$. If $q > 2^{ik(k-1)}$, then for every half-system $U$ of $\mathbb{F}_q$ satisfying $TU = U$ there is a set $K \subset \mathbb{F}_q, |K| = k$ such that $E_U(G)_K$ is an $APA_1(2,k,q)$.*

This generalizes Theorem 18. If $k|(q-1)$ or $k|q$ we can be more precise. The following notation will be handy: If $U$ is a half-system of $\mathbb{F}_q$, put

$$\chi_U(a) = \begin{cases} 0 & \text{if } a = 0. \\ 1 & \text{if } a \in U. \\ -1 & \text{if } a \in -U. \end{cases}$$

The values of $\chi_U$ are to be considered as integers.

**Theorem 20** *Let $q$ be an odd prime-power, $k$ an odd divisor of q-1, $K$ the subgroup of order $k$ of $\mathbb{F}_q^*$, $U$ a half-system of $\mathbb{F}_q$ satisfying $KU = U$.*
*Then $E_U(G)_K$ is an $APA_1(2,k,q)$.*

*Proof.* We have to check that $\Gamma(K, \alpha \cdot U^{-1})$ is balanced for every $0 \neq \alpha \in I\!F_q$. Put $V = \alpha \cdot U^{-1}$. Then $KV = V$ as $K$ is a group. Let $x \in K$, put $\psi_x = \sum_{y \in K} \chi_V(x-y)$. We have to show that $\psi_x = 0$. The property $KV = V$ shows that $\psi_x = \psi_{zx}$ for every $z \in K$. As $K$ is a group we get $\psi_x = \psi_y$ for every $y \in K$. It follows $k\psi_x = \sum_{y,z \in K} \chi_V(y-z)$. As $\chi_V(y-z) = -\chi_V(z-y)$, the sum vanishes. Thus $\psi_x = 0$. ∎

The same method can be used to handle the case $k|q$.

**Theorem 21** *Let $q$ be an odd prime-power, $k > 1$ a divisor of $q$, $A$ a subgroup of order $k$ of the additive group of $I\!F_q$, and $U$ an arbitrary half-system. Then $E_U(G)_A$ is an $APA_1(2, k, q)$.*

*Proof.* Let $a \in A$, put $\psi_a = \sum_{b \in A} \chi_U(a-b)$. We have to show $\psi_a = 0$. Let $c \in A$. Then $\psi_a = \sum_{b \in A} \chi_U((a+x)-(b+x)) = \psi_{a+x}$, hence $\psi_a = \psi_b$ for $a, b \in A$. Thus $k\psi_a = \sum_{b,c \in A} \chi_U(b-c) = 0$, consequently $\psi_a = 0$. ∎

We conclude that

$$APA_1(2, p^m, p^n)(\ m \leq n)$$

exist for every odd prime $p$.

**Theorem 22** *For every prime $p \equiv 3(mod\ 4), p \geq 11$ there exists a 5-set $K \subset I\!F_p$ such that $(E_{F_q^{*2}}(AGL_1(q)))_K$ is an $APA_1(2, 5, p)$.*

*Proof.* By Theorem 18 only the primes $p < 2^{20}$ are in doubt. It is easily seen that the construction doesn't work for $p = 7$. We shall see in the next section that an $APA_1(2, 5, 7)$ does not exist. Case $p = 11$ is covered by Theorem 19. We may therefore assume $p \geq 19$. Four cases will be distinguished, corresponding to the congruence of $p$ mod 24. In each case we give a table with two columns. The first column contains quintuples $K$ of integers, the second column gives sufficient conditions which ensure that the tournament $\Gamma(\overline{K}, I\!F_q^{*2})$ is balanced. Here $\overline{K}$ denotes the set $K$, where each element is read mod $p$. The entries "$lQ$" and "$lN$" stand for "$l$ is a quadratic residue mod $p$" and "$l$ is a quadratic non-residue mod $p$", respectively.
As an example, the first row of the first table says that for $K = \{0, 1, 5, 6, -4\}$ the above condition is met for all primes $p \equiv 23(mod\ 24)$ for which 5 is a

quadratic non-residue. It is of course easy to translate statements "$lQ$" and "$lN$" into statements concerning the congruence of $p$ mod $l$, using the quadratic reciprocity-law.

- Case $2Q, 3Q$, equivalently $p \equiv 23(mod\, 24), p = 23, 47, 71, \ldots$.

| | |
|---|---|
| 0,1,5,6,-4 | 5N |
| 0,1,4,7,-24 | 7N,31N |
| 0,1,4,7,-31 | 5Q,7N,31Q,19N |
| 0,1,2,-5,21 | 5Q,7N,19Q,13N |
| 0,1,-6,7,8 | 7N,13Q |
| 0,1,-10,11,-11 | 5Q,7Q,11N |
| 0,1,-12,13,-13 | 7Q,13N |
| 0,1,-16,17,-17 | 11Q,17N |
| 0,1,-22,23,-23 | 5Q,11Q,23N,$p \neq 23$ |
| 0,1,-40,41,-41 | 5Q,7Q,41N |
| 0,1,-52,53,-53 | 5Q,7Q,53N |
| 0,1,-187,188,-188 | 5Q,7Q,11Q,17Q,47N,$p \neq 47$ |
| 0,1,-94,95,-95 | 5Q,7Q,47Q,19N,$p \neq 47$ |
| 0,1,-28,29,-29 | 5Q,7Q,19Q,29N |
| 0,1,-110,111,-111 | 5Q,7Q,11Q,13Q,17Q,37N |
| 0,1,-92,93,-93 | 5Q,23Q,37Q,47Q,31N,$p \neq 23, 47$ |

- Case $2Q, 3N$, equivalently $p \equiv 7 (mod\ 24), p = 7, 31, 79, \ldots$.

| | |
|---|---|
| 0,1,-2,3,-3 | 5Q |
| 0,1,2,-8,-9 | 5N,11N |
| 0,1,2,-4,-25 | 5N,7Q,13Q |
| 0,1,2,-4,28 | 5N,7N,13Q |
| 0,1,2,-4,13 | 13N,17Q |
| 0,1,3,4,-16 | 5N,17N,19Q |
| 0,1,3,4,-22 | 11Q,13N,23N |
| 0,1,3,5,-29 | 5N,17N,29N |
| 0,1,2,-4,27 | 13N,31Q,$p \neq 31$ |
| 0,1,4,5,-32 | 5N,11Q,37N |
| 0,1,5,-4,-43 | 11Q,13N,43N |
| 0,1,3,5,-40 | 5N,41Q,43Q |
| 0,1,3,-10,-44 | 5N,11Q,13N,17N,47Q |
| 0,1,3,5,-48 | 5N,17N,53N,$p \neq 7$ |

- Case $2N, 3Q$, equivalently $p \equiv 11 (mod\, 24), p = 11, 59, 83, \ldots$.

| | |
|---|---|
| 0,1,2,-2,-5 | 5Q,7N |
| 0,1,2,-2,5 | 5N,7N |
| 0,1,2,-2,6 | 5Q |
| 0,1,-1,5,-6 | 5N,7Q,11Q |
| 0,1,3,-7,-10 | 5N,7Q,11N,13N |
| 0,1,3,-7,-17 | 5N,7Q,17Q |
| 0,1,3,-7,-23 | 5N,7Q,13Q,23Q |
| 0,1,3,-4,-16 | 5N,7Q,17N,19N |
| 0,1,3,-7,31 | 5N,7Q,19Q,31N |
| 0,1,3,-7,-34 | 5N,7Q,17N,37N |
| 0,1,4,5,-28 | 5N,7Q,11N,29Q |
| 0,1,4,5,-39 | 5N,11N,13Q,43N |
| 0,1,4,5,-40 | 5N,11N,41Q |

- Case $2N, 3N$, equivalently $p \equiv 19 (mod\, 24), p = 19, 43, 67, \ldots$.

| | |
|---|---|
| 0,1,2,3,5 | 5Q |
| 0,1,2,3,10 | 5N,7N |
| 0,1,2,3,-13 | 5N,7Q,13N |
| 0,1,2,-3,14 | 5N,7Q,13Q,17Q |
| 0,1,2,-3,-34 | 5N,7Q,17N,31N |
| 0,1,2,4,12 | 5N,11Q |
| 0,1,2,4,-25 | 13Q,29Q |
| 0,1,2,-4,15 | 5N,7Q,13Q,19N,$p \neq 19$ |
| 0,1,2,-4,-27 | 5N,7Q,29N,23Q |
| 0,1,4,-4,-36 | 5N,37N |
| 0,1,4,-4,-42 | 5N,7Q,23N,43N,$p \neq 19, 43$ |
| 0,1,2,-6,59 | 5N,7Q,13Q,19Q,29N,59Q,$p \neq 19$ |
| 0,1,5,-4,-45 | 5N,23N,41Q |
| 0,1,5,-4,-57 | 5N,19Q,29N,31Q,53Q,$p \neq 19$ |
| 0,1,5,-5,48 | 5N,43Q,53N,47Q,$p \neq 43$ |
| 0,1,5,-5,56 | 5N,7Q,11N,17N,61N |

It remains to be checked that there is no prime $p$, $19 \leq p < 2^{20}$ which satisfies one of the following

- 2Q,3Q,5Q,7Q,11Q,13Q,17Q,19Q,23Q,29Q,31Q,37Q,41Q,47Q,53Q

- 2Q,3N,5N,11Q,13N,17N,19N,23Q,29N,31N,37Q,41N,43Q,47N,53Q
- 2N,3Q,5N,7Q,11N,13Q,17N,19Q,23N,29N,31Q,37Q,41N,43Q
- 2N,3N,5N,7Q,11N,13Q,17N,19Q,23N,29N,31Q,37Q,41N,43Q,47N, 53N,59N,61Q

A little computer-program checks this in a few seconds. ■

A computer-search shows that many more $APA_1(2,k,q)$ of the form $E_U(G)_K$ exist than those which we have been able to explain theoretically. The most interesting sporadic example is an $APA_1(2,15,27)$. This is the first example with $k > v/2, k \neq v$.

# 8 Room spaces

We establish a link between $APA_1(2,*,*)$ and Room spaces.

**Definition 13** • *Let $S$ be a set of $n+1$ elements. A* Room square *of side $n$ with set $S$ of symbols is an $(n,n)$-array $F$ which satisfies the following properties:*

1. *Every cell of $F$ either is empty or contains an unordered pair of symbols.*
2. *Each symbol occurs exactly once in each row and column of $F$.*
3. *Each unordered pair of symbols occurs in precisely one cell of $F$.*

- *A Room square is* standardized *if for some symbol $\infty$ the entries in the diagonal are the unordered pairs $\{\infty, x\}, x \in S - \{\infty\}$.*
- *A Room square is* skew *if it is standardized and if for each pair of cells with coordinates $(i,j)$ and $(j,i)$,$j \neq i$, precisely one is empty.*
- *A* Room $d$-space *(usually called a* Room $d$-cube*) is a $d$-dimensional array of side $n$ each 2-dimensional projection of which is a Room square. A Room space is* skew *if each 2-dimensional projection is skew.*

**Theorem 23** *1. If there is an $APA_1(2,k+2,v)$ a restriction of which is an $APA_1(2,k,v)$, then there is a skew Room $k$-space of side $v$ ($k \geq 3$).*

2. *If there is an $APA_1(2, v-2, v)$, then there is a skew Room $(v-2)$-space of side $v$.*

*Proof.*

1. Let $\Sigma$ be an $APA_1(2, k+2, v)$ with set $E = \{1, 2, \ldots v\}$ of entries and set $C$ of columns, $c_1, c_2$ two columns of $\Sigma$ such that $\Sigma_{C-\{c_1,c_2\}}$ is an $APA_1(2, k, v)$. Define a $k$-dimensional array $F$ of side $v$ with set

   $S = E \cup \{\infty\}$ of symbols in the following way:

   - $F(i, i, \ldots i) = \{\infty, i\}, i = 1, 2, \ldots v.$
   - Each row $(a, b, x_1, x_2, \ldots x_k)$ of $\Sigma$ contributes a non-empty cell $F(x_1, x_2, \ldots, x_k) = \{a, b\}$. Here $c_1, c_2$ have been chosen as the first two columns. The remaining cells of F are empty.

   We claim that $F$ is a skew Room k-space. Clearly $F$ is standardized. Consider a 2-dimensional projection $F_{x,y}$ corresponding to columns $x$ and $y$. Property $P(0, 2)$ and $\lambda = 1$ show that $F_{x,y}$ is skew and that each unordered pair of symbols occurs in precisely one cell of $F_{x,y}$. It remains to show that each symbol occurs exactly once in each row and column of $F_{x,y}$. This is clear by construction if the symbol is $\infty$. Let $a \in E, a \neq i \in E$. The number of rows of $\Sigma$ containing $a$ and $i$ is $\binom{k+2}{2}$. Property $P(1, 2)$ shows that there are exactly $(k+1)/2$ rows of $\Sigma$ containing $a$ and with $i$ in column $x$. The same argument, when applied to $\Sigma_{C-\{c_1,c_2\}}$, shows that there are $(k-1)/2$ rows of $\Sigma_{C-\{c_1,c_2\}}$ containing $a$ and with $i$ in column $x$. We conclude that the number of rows of $\Sigma$ with $i$ in column $x$ and $a$ in column $c_1$ or in column $c_2$ is $(k+1)/2 - (k-1)/2 = 1$. This shows that entry $a$ occurs exactly once in row $i$ of $F_{x,y}$. Entry $i$ is to be found in cell $(i, i)$.

2. Let $\Sigma$ be an $APA_1(2, v-2, v)$. Define $F$ in the following way:

   - $F(i, i, \ldots i) = \{\infty, i\}, i = 1, 2, \ldots v.$
   - Each row $(x_1, x_2, \ldots x_{v-2})$ of $\Sigma$ contributes a non-empty cell

$F(x_1, x_2, \ldots, x_{v-2}) = E - \{x_1, x_2, \ldots x_{v-2}\}$. The remaining cells of $F$ are empty.

An argument very similar to the one above shows that each symbol occurs exactly once in each row and column of each 2-dimensional projection. In order to show that each unordered pair of symbols occurs in precisely one cell of $F$, we have to see that each such pair is disjoint from exactly one row of $\Sigma$, equivalently that the design given by the rows of $\Sigma$ is the complete design. This is indeed true as follows from the fact that the residue with respect to one entry is a $0 - PA_1(1, v-2, v-1)$. Alternatively we may invoke a theorem of Wilson's ([29]).

It is well-known (see [9]) that Room $(v-2)$-spaces of side v do not exist for $5 \leq v \leq 9$. We conclude:

**Corollary 16** *$APA_1(2,3,5), APA_1(2,5,7), APA_1(2,7,9)$ and $2 - PA_1(3,5,8)$ do not exist.*

It is in fact an easy exercise to prove the nonexistence of $APA_1(2,3,5)$ directly. The nonexistence of $2 - PA_1(3,5,8)$ follows from the fact that its residue would be an $APA_1(2,5,7)$ ( see Theorem 4). We may use our method to construct skew Room spaces. As in the previous section put $G = AGL_1(q)$, where $q$ is an odd prime-power.

**Definition 14** *Let $L \subseteq \mathbb{F}_q - \{0,1\}, L = \{\tau_1 \ldots, \tau_k\}$, $U$ a half-system of $\mathbb{F}_q$. Define a k-dimensional array $F(L,U)$ as follows:*

- *$F(i, i, \ldots i) = \{\infty, i\}, i = 1, 2, \ldots q$.*
- *Each element $\tau \longrightarrow u\tau + \beta$ of $G$, where $u \in U, \beta \in \mathbb{F}_q$, yields a cell*

$$F(u\tau_1 + \beta, \ldots, u\tau_k + \beta) = \{\beta, u + \beta\}$$

This is the construction of the preceding Theorem. Note that because of the 2-transitivity of G in its action on the columns there is no restriction in choosing the columns indexed by 0 and 1 to yield the entries of the array. Instead of looking for $APA$'s we ask the more modest question when $F(L,U)$ is a Room space.

**Proposition 4** *Let $G = AGL_1(q)$, $q$ an odd prime-power, $U$ a half-system of $\mathbb{F}_q$, $L \subseteq \mathbb{F}_q - \{0,1\}$. Then the following are equivalent:*

- *$F(L,U)$ is a skew Room $k$-space of side $q$.*
- *For every $\tau \in L$ we have $(\frac{1}{\tau} - 1)U = U$.*

*Proof.* Let $\Sigma = E_U(G)$. As in the proof of the preceding Theorem we see that only one condition is in doubt. For every $\tau \in L$ the column $c_\tau$ indexed by $\tau$ has to satisfy the following:
for every entry $a \in \mathbb{F}_q$ the union of the entries of $\Sigma$ in columns $c_0$ and $c_1$ and in the rows with entry $a$ in $c_\tau$ is exactly $\mathbb{F}_q - \{a\}$. Thus a column $c_\tau$ violates the condition if and only if for some $a, b \in \mathbb{F}_q, a \neq b$ and $u_1, u_2 \in U$ we have

$$u_1\tau + \beta_1 = a, \beta_1 = b$$

$$u_2\tau + \beta_2 = a, u_2 + \beta_2 = b,$$

equivalently $u_1\tau = u_2\tau - u_2$, equivalently $(\frac{1}{\tau} - 1)u_1 = -u_2$. Put $N(U) = \{\alpha | \alpha \in \mathbb{F}_q^*, \alpha U = U\}$. We have seen that $F(L,U)$ is a Room space if and only $(\frac{1}{\tau} - 1) \in N(U)$ for every $\tau \in L$. ∎

We may choose $K$ to be a subgroup of odd order of $\mathbb{F}_q^*$ and $U$ to be a union of cosets of $K$. The preceding Proposition yields:

**Corollary 17** *Let $q$ be an odd prime-power, $t$ an odd divisor of $q-1$. Then there is a skew Room $t$-space of side $q$.*

This is a well-known Theorem of Dinitz ([8]). Unfortunately our method does not yield more. This is due to the obvious fact that for every half-system $U$ the set $N(U)$ as defined in the proof of the Proposition above is a subgroup of odd order of $\mathbb{F}_q^*$.

# References

[1] J.Bierbrauer: *Monotypical uniformly homogeneous Sets of Permutations,* Archiv der Mathematik 58(1992),338-344.

[2] J.Bierbrauer: *The uniformly 3-homogeneous subsets of* $PGL_2(q)$, submitted for publication in the Journal of Algebraic Combinatorics.

[3] J.Bierbrauer:*A Family of Perpendicular Arrays achieving perfect 4-fold Secrecy,* to appear in the Proceedings of the $13^{th}$ British Combinatorial Conference.

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

[7] J.Bierbrauer,S.Black,Y.Edel: $t-$*homogeneous sets of permutations,* manuscript.

[8] J.H.Dinitz: *New lower bounds for the number of pairwise orthogonal symmetric Latin squares,* Congr. Numerantium 23(1979), 393-398.

[9] J.H.Dinitz,D.R.Stinson: *Room squares and related designs,* in: Contemporary Design Theory: A Collection of Surveys, J.H.Dinitz and D.R.Stinson (ed.), Wiley 1992.

[10] A.Granville,A.Moisiadis,R.Rees: *Nested Steiner* $n$*-cycle Systems and perpendicular Arrays,* J.Comb Math and Comb Comput. 3(1988), 163-167.

[11] Haim Hanani: *Truncated finite planes,* Proc. Symposia in Pure Mathematics, AMS 19(1971), 115-120.

[12] W.M.Kantor: *On incidence matrices of finite projective and affine spaces,* Mathematische Zeitschrift 124(1972), 315-318.

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

[14] E.S.Kramer,S.S.Magliveras,T.v.Trung,Q.Wu: *Some perpendicular arrays for arbitrarily large* $t$, Discrete Mathematics 96(1991),101-110.

[15] R.C.Mullin,P.J.Schellenberg,G.H.J.van Rees, S.A.Vanstone: *On the Construction of Perpendicular Arrays,* Utilitas Mathematica 18(1980),141-160.

[16] C.R.Rao: *Combinatorial Arrangements analogous to Orthogonal Arrays,* Sankhya A23(1961),283-286.

[17] P.J.Schellenberg,G.H.J.van Rees, S.A.Vanstone: *Four pairwise orthogonal latin squares of order 15,* Ars Combinatoria 6(1978),141-150.

[18] D.R.Stinson: *The Spectrum of nested Steiner Triple Systems,* Graphs and Combinatorics 1(1985),189-191.

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

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

[21] Luc Teirlinck: *Non-trivial $t$-designs without repeated blocks exist for all* $t$, Discrete Mathematics 65(1987), 301-311.

[22] Luc Teirlinck: *On large Sets of disjoint ordered Designs,* Ars Combinatoria 25(1988), 31-37.

[23] Luc Teirlinck: *Locally trivial designs and $t$-designs without repeated blocks,* Discrete Mathematics 77(1989), 345-356.

[24] Luc Teirlinck: *Generalized idempotent orthogonal arrays,* in: Coding Theory and Design Theory, Part II: Design Theory , D.Ray-Chaudhury (ed.), IMA Vol.Math. Appl. 21, Springer 1990, 368-378.

[25] Luc Teirlinck: *Large sets of disjoint designs and related structures,* in: Contemporary Design Theory: A Collection of Surveys, J.H.Dinitz and D.R.Stinson (ed.), Wiley 1992.

[26] D.T.Todorov: *Three mutually orthogonal latin squares of order 14,* Ars Combinatoria 20(1985), 45-48.

[27] Tran van Trung: *On the Construction of Authentication and Secrecy Codes,* Universität GH Essen Preprint Series 17 (1991).

[28] Richard M.Wilson: *Cyclotomy and difference families in elementary abelian groups,* Journal of Number Theory 4(1972), 17-47.

[29] Richard M.Wilson: *The necessary conditions for $t$-designs are sufficient for something,* Utilitas Mathematica 4(1973), 207-215.

[30] Richard M.Wilson: *Inequalities for $t$-designs,* Journal of Combinatorial Theory A 34(1983), 313-324.