A family of perpendicular arrays achieving perfect 4-fold secrecy

Jürgen Bierbrauer

Institut für Reine Mathematik, Universität Heidelberg, Im Neuenheimer Feld 288, W-6900 Heidelberg 1, Germany

Received 12 July 1991
Revised 6 December 1991

1. Introduction

A perpendicular array $PA_\lambda(t, k, v)$ is a $\lambda(\ell)$ by $k$ array $A$ of $v$ distinct symbols, which satisfies:

(i) every row of $A$ contains $k$ distinct symbols,

(ii) for any $t$ columns, and for any $t$ distinct symbols, there are precisely $\lambda$ rows with the given symbols in the given columns.

Such a structure may also be described as a $\lambda$-uniform, $t$-homogeneous set of injective mappings from a $k$-set into a $v$-set.

A close connection with $t$-designs is obvious. In contrast to the situation with designs, it is not clear if a perpendicular $t$-array $PA_\lambda(t, k, v)$ is also a perpendicular $s$-array $PA_{\lambda(s)}(t, k, v)$ for $s < t$, where

$$\lambda(s) = \lambda \times \frac{v-s}{t-s} \binom{t}{s}$$

If this is the case for all $s \leq t$, we shall call $A$ an inductive perpendicular array.

Especially a necessary condition for the existence of an inductive $PA_\lambda(t, k, v)$ is

$$\lambda \times \begin{pmatrix} v-s \\ t-s \end{pmatrix} \equiv 0 \pmod{\begin{pmatrix} t \\ s \end{pmatrix}}.$$  

An application to cryptography was given in [7, proof of Theorem 2.3], where it was shown that an inductive $PA_\lambda(t, k, v)$ gives rise to a cryptocode for $k$ source states with $v$ messages and $\lambda(\ell)$ encoding rules, which achieves perfect $t$-fold secrecy.
No infinite family of inductive perpendicular $t$-arrays with $t > 3$ and reasonably small $\lambda$ seems to be known. In [6] the marriage theorem is used to construct PA's from $t$-designs with $k = t + 1$. Especially Alltop's series of 4-designs with parameters $4 - (2^f + 1, 5, 5)$ (see [1]) yields $PA_1(4, 5, 2^f + 1)$ and the (nonsimple) designs with parameters $5 - (2^f + 2, 6, 15)$ of [4] yield $PA_5(5, 6, 2^f + 2)$ for $f \geq 2$. However, these arrays have no chance to be inductive as the above necessary condition is violated for $s = 3$.

In this paper we use the families of designs with parameters $4 - (2^f + 1, 6, 10)$ ($f$ odd) and $4 - (2^f + 1, 9, 84)$ ($f; 6) = 1$ as constructed in [2, 3] to produce inductive PAS with $t = 4$.

**Theorem 1.1.** (i) If $f$ is odd, there is an inductive $PA_{12}(4, 6, 2^f + 1)$.

(ii) If $(f, 6) = 1$, there is an inductive $PA_{36}(4, 9, 2^f + 1)$.

This construction is possible because the designs are highly symmetric. They are defined on the projective line and have the projective group $PGL(2, 2^f)$ as their group of automorphisms.

**Corollary 1.2.** (i) Let $f$ be odd. Then there is a cryptocode for 6 source states with $2^f + 1$ messages and $12(2^f + 1)$ encoding rules, which achieves perfect 4-fold secrecy.

(ii) If $(f, 6) = 1$, there is a cryptocode for 9 source states with $2^f + 1$ messages and $36(2^f + 1)$ encoding rules, which achieves perfect 4-fold secrecy.

It is not clear if a variation of our method could produce inductive PAs with the same values of $t, k, v$ and smaller $\lambda$. The necessary conditions given above show that $\lambda$ must be even.\textsuperscript{1}

2. Constructions and proofs

Let $q = 2^f, f$ odd. Consider the operation of the projective group $G = PGL(2, q)$ on the projective line $PG(1, q)$. Elements of order 3 are fixed-point-free. Define blocks of a design $B_1$ to be unions of two point-orbits of elements of order 3 in $G$. We get a design with parameters $4 - (q + 1, 6, 10)$ (see [2]). It was shown in [2] that blocks of $B_1$ are exactly the 6-subsets of $PG(1, q)$ which have the symmetric group $S_3$ as stabilizer in $G$. If $B$ is such a block, we write $B = B_1 \cup B_2$, where $B_1$ and $B_2$ are orbits of the group of order 3 operating on $B$. We call $B_1, B_2$ the **triples** of $B$.

**Definition 2.1.** Let $q = 2^f, f$ odd. The array $A_1$ with 6 columns and $PG(1, q)$ as set of symbols is defined as follows.

From each block $B \in B_1$ construct a row, where the triples of $B$ are written in the first three and the last three positions, respectively. Then every such row is replaced

\textsuperscript{1} I wish to thank Tran van Trung for introducing me to this subject.
A family of perpendicular arrays

by an $18 \times 6$ array $A_1(B)$ consisting of the images of the initial row under the action of the wreath-product $Z_3 \wr Z_2$ with the first and last three columns as regions of imprimitivity.

Remark that $A_1(B)$ is not uniquely determined by $B$.

**Theorem 2.2.** Let $q = 2^f$, $f$ odd. The array $A_1$ is an inductive 

\[ PA_{12}(4, 6, q+1). \]

**Proof.** It is sufficient to show that $A_1$ is a $PA_{12}(4, 6, q+1)$ and a $PA_{3(q-2)}(3, 6, q+1)$. (see [5, Theorem 1.1].)

(1) Consider first the case $t = 3$. Only two 3-subsets $T$ of columns have to be considered:

(a) Let $T = \{1, 2, 3\}$, $S = \{\infty, 0, 1\}$. Whichever symbol of $S$ appears in column 4 (three choices), there remain $q - 2$ choices for the symbol in column 3. We have $3(q - 2)$ blocks $B \ni S$ in the appropriate position. The array $A_1(B)$ has exactly one row with a given symbol in column 4 and a given set of symbols in columns 1, 2.

(b) Let $T = \{1, 2, 4\}$, $S = \{0, 1, a\}$. Whichever symbol of $S$ appears in column 4 (three choices), there remain $q - 2$ choices for the symbol in column 3. We have $3(q - 2)$ blocks $B \ni S$ in the appropriate position. The array $A_1(B)$ has exactly one row with a given symbol in column 4 and a given set of symbols in columns 1, 2.

(2) Consider the case $t = 4$. We have two essentially different 4-sets of columns. The sets of symbols appearing there may be chosen to be $S = \{\infty, 0, 1, a\}$.

(a) Let $T = \{1, 2, 3, 4\}$. There are four blocks $B \ni S$ having one of their triples in $S$. Each such block contributes three lines of $A_1(B)$ to our counting problem.

(b) Let $T = \{1, 2, 4, 5\}$. There are six blocks $B \ni S$ having no triple in $S$. Each corresponding $A_1(B)$ contributes two rows to our problem. 

Let $q = 2^f$, $(f; 6) = 1$. In [3] we constructed a block design, here called $B_2$, with parameters $4 - (q + 1, 9, 84)$, whose blocks are the unions of the nonregular and a regular orbit of a subgroup $S_3$ of $G$. If $B$ is a block of $B_2$, $K$ the stabilizer of $B$ in $G$, we write $B = B_0 \cup B_1 \cup B_2$, where $B_0$ is the nonregular orbit of $K$ and $B_1, B_2$ are orbits of the subgroup of order 3 of $K$. Let us call $B_1, B_2$ the triples of $B$, and $B_0$ the center of $B$.

**Definition 2.3.** Let $q = 2^f$, $(f; 6) = 1$. The array $A_2$ with 9 columns and entries from $PG(1, q)$ is defined as follows. Every block $B \in B_2$ yields a row, where the center of $B$ appears in the first three columns, the triples in the middle and final three columns, respectively. Then each such row is replaced by a $54 \times 9$ array $A_3(B)$ consisting of the images of the initial row under the action of the group $Z_3 \times (Z_3 \wr Z_2)$ of order 54, operating in the natural way.
Theorem 2.4. Let $q = 2^f$, $(f, 6) = 1$. The array $A_2$ is an inductive $PA_{36}(4, 9, q + 1)$.

Proof. By [5, Theorem 1.1] it suffices to show that $A_2$ is a $PA_{36}(4, 9, q + 1)$. Let $T$ be a set of four columns, $S$ a set of four entries. We can choose, without restriction, $S = \{\infty, 0, 1, a\}$. We have to count the rows of $A_2$, where the symbols from $S$ appear in the positions of $T$. The expected number is 36. If $T \subset \{4, 5, 6, 7, 8, 9\}$, we are done, by Theorem 1, for by deleting the first three columns of $A_2$ we get three copies of $A_1$. Five essentially different cases of $T$ have to be considered.

Case 1: $T = \{1, 2, 3, 4\}$. There are exactly four blocks $B$ containing $S$ and having their center in $S$. Each such $A_2(B)$ contributes 9 rows to our counting problem.

Case 2: $T = \{1, 2, 4, 5\}$. We have to count blocks $B \supset S$ having two center points and two points of a triple in $S$. This reverts to Case (2(b)) of the proof of Theorem 2.2. We counted 6 blocks there. Here the order, in which the pairs of elements of $S$ occur, has to be taken into account. We get 12 blocks in our case. Each corresponding $A_2(B)$ produces three rows which we have to count.

Case 3: $T = \{1, 2, 4, 7\}$. We use the counting done in the proof of the main theorem of [3]. Cases 2 and 3 in the present situation correspond to case $d = 2$ in [3]. Thus we get $30 - 12 = 18$ blocks $B \supset S$ having two center points in $S$ and having the two remaining points of $S$ in different triples. The array $A_2(B)$ contributes 2 rows to our problem for every such $B$.

Case 4: $T = \{1, 4, 5, 6\}$. Obviously, there are four blocks $B \supset S$ having a triple in $S$ and a center point in $S$. Each corresponding $A_2(B)$ contributes 9 rows.

Case 5: $T = \{1, 4, 5, 7\}$. By case $d = 1$ of the proof of the main theorem of [3], which corresponds to Cases 4 and 5 here, there are 36 blocks $B$ in the proper position with respect to $S$. Each corresponding array $A_2(B)$ contributes exactly one row.

References