An Effective Algorithm for Construction of Special Types of Finite Projective Geometries and Steiner Systems

Marija Mihova

"Ss Cyril and Methodius" University,
Institute of Informatics, P. O. Box162, Skopje, Republic of Macedonia
e-mail: marija@ii.edu.mk

Abstract. We give a formula for very effective construction of special types of finite projective geometry, that are also special types of Steiner systems.

Key words: projective geometry, Stainer system

AMS Mathematics Subject Classification (2000): 51E15, 51E10, 20N05

1 Introduction

In this paper we consider a special kind of finite projective geometries that can be constructed quite easily and very fast. They consist of n^2+n+1 points and n^2+n+1 lines, for prime number n. It is well known that there is a procedure for generating a projective geometry with n^2+n+1 lines and points, for integers n that are powers of prime numbers [1]. The procedure we are proposing is restricted to prime numbers only, but we earned effectiveness for that price. The projective planes constructed in our ways give immediately a Stainer system too.

In the sequel we give the definitions of a projective geometry and of a Stainer system.

Definition 1. *A projective plane is an incidence structure* $(\mathcal{P}, \mathcal{L})$ *of points and lines such that:*

P1: *Any two distinct points are incident with exactly one line.*
P2: *Any two distinct lines are incident with exactly one point.*
P3: *There exist a quadrangle, i.e., there are four points such that no three of them are collinear.*

Definition 2. *Given three integers* t, k, v *such that* $2 \leq t < k < v$, *a Stainer system* $S(t,k,v)$ *is a* v*-set* V *together with a family* $\mathcal{B}$ *of* k*-subsets of* V *(blocks) with the property that every* t*-subset of* S *is contained in exactly one block.*

The next proposition implies that each finite projective plane is a Stainer system $S(2, n+1, n^2+n+1)$ [1].

Proposition 1. *All lines in a projective geometry have the same cardinality. If the projective plane is finite* ($|\mathcal{P}|, |\mathcal{L}| \in \mathbb{N}$)*, then there is an integer* $n \geq 2$*, such that all lines have* $n+1$ *points and the plain contains* n^2+n+1 *points and* n^2+n+1 *lines.*

2 A new formula for construction of projective geometries

Let n be an integer and let define an integer function $MOD(i,n)$ by $MOD(i,n) = j$ iff $i \equiv j \ (mod\ n)$ and $1 \leq j \leq n$. Using this function we define the integers $p_{i,j}$ as follows.

$$p_{i,j} = \begin{cases} 0, & i = j = 0 \\ \left\lfloor \dfrac{i-1}{n} \right\rfloor, & 1 \leq i \leq n(n+1),\ j = 0 \\ n \cdot i + j, & 0 \leq i \leq n,\ 1 \leq j \leq n \\ n \cdot j + MOD\left((j-1)\left(\left\lfloor \dfrac{i-1}{n} \right\rfloor - 1 \right) + i, n \right), & i > n,\ j \neq 0 \end{cases} \tag{1}$$

Now, for each $i,\ 0 \leq i \leq n^2+n$, we define sets L_i by

$$L_i = \{p_{i,j} | j = \overline{0,n}\}. \tag{2}$$

Proposition 2. $|L_i| = n+1,\ \forall i = \overline{0, n^2+n}$.

In order to proof that $(\mathcal{P}, \mathcal{L})$ for $\mathcal{P} = \{0, 1, ..., n^2+n\}$ and $\mathcal{L} = \{L_i | i = \overline{0, n(n+1)}\}$ is projective geometry, we need the following lemma:

Lemma 1. *Let* n *be a prime. For any integer* $a,\ 1 \leq a \leq n-1$*, and any* $b \in \mathbb{Z}$ *there is only one integer* k*,* $0 \leq k \leq n-1$*, such that* $a \cdot k \equiv b \ (mod\ n)$.

Proof. Let $1 \leq a \leq n-1$ and $b \in \mathbb{Z}$.

Regard the group $\mathbb{Z}_n(\cdot)$. Since n is a prime, for i_1 and i_2 such that $0 \leq i_1, i_2 \leq n-1$, from $a \cdot_n i_1 = a \cdot_n i_2$ follows $i_1 = i_2$. So, we have that $|\{a \cdot_n i | i = \overline{0, n-1}\}| = n$. From the other side, $\{a \cdot_n i | i = \overline{0, n-1}\} \subseteq \{0, 1, \ldots, n-1\}$, so $\{a \cdot_n i | i = \overline{0, n-1}\} = \{0, 1, \ldots, n-1\}$. From this we have that for any integer $a,\ 1 \leq a \leq n-1$, and any $j \in \mathbb{Z}_n$ there is only one integer k, $0 \leq k \leq n-1$, such that $a \cdot_n k = j$ (i.e. $a \cdot k \equiv j \ (mod\ n)$).

Now, let $j \in \mathbb{Z}_n$ such that $b \equiv j \ (mod\ n)$. Then, there is only one integer k, $0 \leq k \leq n-1$, such that $a \cdot k \equiv b \ (mod\ n)$.

Theorem 1. *Let* n *be a prime number,* $\mathcal{P} = \{0, 1, ..., n^2+n\}$ *and* $\mathcal{L} = \{L_i | i = \overline{0, n(n+1)}\}$*. Then* $(\mathcal{P}, \mathcal{L})$ *is a projective geometry with* n^2+n+1 *lines and* n^2+n+1 *points.*

Proof. Let n be a prime number.

P1: Let $f_1, f_2 \in \mathcal{P}$. We will proof that there is a set $L_i, i \in \{0, 1, 2, \ldots, n\}$ such that $\{f_1, f_2\} \in L_i$. There are four cases:

1. For $f_1 = 0, f_2 = kn + b,\ 1 \leq b \leq n$ and $0 \leq k \leq n$, then $\{f_1, f_2\} \subseteq L_k$.
2. If $f_1 = kn + b_1, f_2 = kn + b_2,\ 0 \leq k \leq n,\ 1 \leq b_1, b_2 \leq n$, then $\{f_1, f_2\} \subseteq A_k$.
3. For $1 \leq f_1 \leq n$ and $f_2 = kn + b,\ 1 \leq k \leq n$, we we will proof that $\{f_1, f_2\} \subseteq A_i$, where $i = nf_1 + MOD(b - (k-1)(f_1 - 1), n)$.
   Let $i = nf_1 + MOD(b - (k-1)(f_1 - 1), n)$, then
   $$\left\lfloor \frac{i-1}{n} \right\rfloor = \left\lfloor \frac{nf_1 + MOD(b - (k-1)(f_1 - 1), n) - 1}{n} \right\rfloor = f_1.$$
   and $i \equiv b - (k-1)(f_1 - 1)(mod\ n)$, i.e. $b \equiv (k-1)(f_1 - 1) + i(mod\ n)$
   Now, $p_{i,0} = \left\lfloor \frac{i-1}{n} \right\rfloor = f_1 \Rightarrow f_1 \in L_i$. Also,
   $$\begin{aligned} p_{i,k} &= nk + MOD\left((k-1)\left(\left\lfloor \frac{i-1}{n} \right\rfloor - 1\right) + i, n\right) \\ &= nk + MOD\left((k-1)(f_1 - 1) + i, n\right) \\ &= nk + MOD(b, n) = nk + b. \end{aligned}$$
   It follows that $f_2 = p_{i,k} \in L_i$.
4. Let $f_1 = k_1 n + b_1, f_2 = k_2 n + b_2$ for $1 \leq k_1 < k_2 \leq n,\ 1 \leq b_1, b_2 \leq n$. Since n is a prime, from Lemma 1 we have that there is $t \in \{0, \ldots, n-1\}$ such that $b_2 - b_1 \equiv t(k_2 - k_1)$. Let $b_1 - (k_1 - 1)t \equiv s\ (mod\ n)$ and $1 \leq s \leq n$. Then $MOD(b_1 - (k_1 - 1)t, n) = s$ and $MOD(s + (k_1 - 1)t, n) = b_1$. Now,
   $$\begin{aligned} & b_2 - (k_2 - 1)t \equiv b_1 + t(k_2 - k_1) - (k_2 - 1)t\ (mod\ n) \\ \Leftrightarrow\ & b_2 - (k_2 - 1)t \equiv b_1 - t(k_1 - 1)\ (mod\ n) \\ \Leftrightarrow\ & b_2 - (k_2 - 1)t \equiv s\ (mod\ n) \\ \Leftrightarrow\ & b_2 \equiv s + (k_2 - 1)t\ (mod\ n) \end{aligned}$$
   Let $i = n(t+1) + s$. Then,
   $$\left\lfloor \frac{i-1}{n} \right\rfloor - 1 = \left\lfloor \frac{n(t+1) + s - 1}{n} \right\rfloor - 1 = (t+1) - 1 = t.$$
   Now we will show that f_1 and f_1 are in L_i, for $i = n(t+1) + s$.
   $$\begin{aligned} p_{i,k_1} &= nk_1 + MOD((k_1 - 1)\left(\left\lfloor \frac{i-1}{n} \right\rfloor - 1\right) + n(t+1) + s, n) \\ &= nk_1 + MOD((k_1 - 1)t + n(t+1) + s, n) \\ &= nk_1 + MOD((k_1 - 1)t + s, n) = nk_1 + b_1. \end{aligned}$$
   On the same way it can be obtained that $p_{i,k_2} = nk_2 + b_2$.

P2: Let $i, j \in \mathcal{P}$ and $i < j$. To proof that $|L_i \cap L_j| = 1$ we will regard five cases:

1. If $i = 0$, then $L_0 \cap L_j = \{p_{j,0}\}$, because the other elements in L_0 are smaller or equal to n, and the other elements in L_j are bigger then n.
2. If $1 \leq i < j \leq n$, then $p_{i,0} = p_{j,0} = 0 \in L_i \cap L_j$. Suppose that there is another element in $L_i \cap L_j$. Then, there are $k_1, k_2 \neq 0$ such that $p_{i,k_1} = p_{j,k_2}$. So,

$$ni + k_1 = nj + k_2 \Rightarrow n(j - i) = k_1 - k_2.$$

Since $n(j-i) \geq n$ and $k_1 - k_2 < n$, the last equation is not true, and we proof that in this case $|L_i \cap L_j| = 1$.
3. Let $1 \leq i \leq n < j$ and $p_{i,k_1} = p_{j,k_2}$, then

$$ni + k_1 = nk_2 + MOD((k_2 - 1)\left(\left\lfloor \frac{j-1}{n} \right\rfloor - 1\right) + j, n).$$

It follows that $k_2 = i$ and $k_1 = MOD((i-1)\left(\left\lfloor \frac{j-1}{n} \right\rfloor - 1\right) + j, n)$, so $|L_i \cap L_j| = 1$.
4. If $nk + 1 \leq i < j \leq n(k+1)$ for $k > 0$, then $p_{i,0} = p_{j,0} = k \in L_i \cap L_j$. Note that $\left\lfloor \frac{i-1}{n} \right\rfloor = \left\lfloor \frac{j-1}{n} \right\rfloor = k$.
Suppose that there are $k_1, k_2 \neq 0$, such that $p_{i,k_1} = p_{j,k_2}$. Then

$$nk_1 + MOD((k_1-1)(k-1)+i, n) = nk_2 + MOD((k_2-1)(k-1)+j, n).$$

From the last equation we have that $k_1 = k_2$. Using this we have that $(k_1 - 1)(k-1) + i \equiv (k_1 - 1)(k-1) + j \ (mod\ n)$, i.e. $i \equiv j \ (mod\ n)$. Since $nk + 1 \leq i, j \leq n(k+1)$ from $i \equiv j \ (mod\ n)$ we have that $i = j$. We obtain that $L_i \cap L_j = \{k\}$.
5. Let $nk_1 + 1 \leq i \leq n(k_1 + 1)$ and $nk_2 + 1 \leq j \leq n(k_2 + 1)$, for $1 < k_1 < k_2 \leq n$. Then, $\left\lfloor \frac{i-1}{n} \right\rfloor = k_1 = p_{i,0}$ and $\left\lfloor \frac{j-1}{n} \right\rfloor = k_2 = p_{j,0}$. It is clear that $p_{i,0} \neq p_{j,0}$, so if $p_{i,t_1} = p_{j,t_2}$, then $t_1, t_2 > 0$. Let $p_{i,t_1} = p_{j,t_2}$, then

$$\begin{aligned} &nt_1 + MOD\left((t_1 - 1)\left(\left\lfloor \frac{i-1}{n} \right\rfloor - 1\right) + i, n\right) \\ &= nt_2 + MOD\left((t_2 - 1)\left(\left\lfloor \frac{j-1}{n} \right\rfloor - 1\right) + j, n\right) \end{aligned}$$

From this, $t_1 = t_2$ and

$$MOD\left((t_1 - 1)(k_1 - 1) + i, n\right) = MOD\left((t_2 - 1)(k_2 - 1) + j, n\right).$$

Now we have

$$\begin{aligned} &(t_1 - 1)(k_1 - 1) + i \equiv (t_1 - 1)(k_2 - 1) + j \ (mod\ n) \\ \Leftrightarrow\ &(t_1 - 1)(k_1 - k_2) \equiv j - i \ (mod\ n) \end{aligned}$$

From Lemma 1, only one t_1 satisfies $(t_1 - 1)(k_1 - k_2) \equiv j - i \ (mod\ n)$, so, $|L_i \cup L_j| = 1$.

P3: It is clear that 0, 1, $n+1$ and $n+2$ are not collinear.

In such a way we completed the proof of the theorem.

Note that the theorem is not true when n is not a prime number. In that case there are integers $1 < n_1, n_2 < n$ such that $n = n_1 n_2$. We will show that the sets L_{n+1} and $L_{(n_2+1)n+1}$ have at last two equal elements. Set $b = (n_2+1)n+1$. Then

$$\begin{aligned}
p_{n+1,1} &= n + MOD(0(1-1) + n + 1, n) = n+1 \\
p_{b,1} &= n + MOD(0 + (n_2+1)n + 1, n) = n+1 \\
p_{n+1,n_1+1} &= (n_1+1)n + MOD(n_1\left(\left\lfloor \frac{n}{n} \right\rfloor - 1\right) + n + 1, n) \\
&= (n_1+1)n + 1 \\
p_{b,n_1+1} &= (n_1+1)n + MOD(n_1\left(\left\lfloor \frac{(n_2+1)n+1}{n} \right\rfloor - 1\right) + (n_2+1)n + 1, n) \\
&= (n_1+1)n + MOD(n_1(n_2+1-1)+1, n) \\
&= (n_1+1)n + MOD(n_1 n_2 + 1, n) \\
&= (n_1+1)n + MOD(n+1, n) = (n_1+1)n + 1
\end{aligned}$$

So, we obtain that $\{n+1, (n_1+1)n+1\} \subseteq L_i \cap L_j$. This imply that $L_i = L_j$.

Example for construction of the projective plane

We will construct the projective plane for $n = 3$.

$$\begin{aligned}
L_0 &= \{p_{0,0}, p_{0,1}, p_{0,2}, p_{0,3}\} = \{0, 3\cdot 0+1, 3\cdot 0+2, 3\cdot 0+3\} = \{0,1,2,3\} \\
L_1 &= \{p_{1,0}, p_{1,1}, p_{1,2}, p_{1,3}\} = \{\left\lfloor \frac{1-1}{3} \right\rfloor, 3\cdot 1+1, 3\cdot 1+2, 3\cdot 1+3\} = \{0,4,5,6\} \\
L_2 &= \{p_{2,0}, p_{2,1}, p_{2,2}, p_{2,3}\} = \{\left\lfloor \frac{2-1}{3} \right\rfloor, 3\cdot 2+1, 3\cdot 2+2, 3\cdot 2+3\} = \{0,7,8,9\} \\
L_3 &= \{\left\lfloor \frac{3-1}{3} \right\rfloor, 3\cdot 3+1, 3\cdot 3+2, 3\cdot 3+3\} = \{0,10,11,12\}
\end{aligned}$$

For $i = 4$, $i = 5$ and $i = 6$, $\left\lfloor \frac{i-1}{3} \right\rfloor = 1$, $\left\lfloor \frac{i-1}{3} \right\rfloor - 1 = 0$, so,

$$MOD((j-1)\left(\left\lfloor \frac{i-1}{3} \right\rfloor - 1\right) + i, 3) = MOD(i, 3).$$

Now,

$$\begin{aligned}
L_4 &= \{1, 3\cdot 1 + MOD(4,3), 3\cdot 2 + MOD(4,3), 3\cdot 3 + MOD(4,3)\} \\
&= \{1,4,7,10\} \\
L_5 &= \{1, 3\cdot 1 + MOD(5,3), 3\cdot 2 + MOD(5,3), 3\cdot 3 + MOD(5,3)\} \\
&= \{1,5,8,11\} \\
L_4 &= \{1, 3\cdot 1 + MOD(6,3), 3\cdot 2 + MOD(6,3), 3\cdot 3 + MOD(6,3)\} \\
&= \{1,6,9,12\}
\end{aligned}$$

For $i \in \{7,8,9\}$, $\left\lfloor \frac{i-1}{3} \right\rfloor = 2$, $\left\lfloor \frac{i-1}{3} \right\rfloor - 1 = 1$, so,

$$MOD((j-1)\left(\left\lfloor \frac{i-1}{3} \right\rfloor - 1\right) + i, 3) = MOD(j-1+i, 3).$$

Now,

$$\begin{aligned} L_7 = \{\ & 2, 3\cdot 1 + MOD(1-1+7,3), 3\cdot 2 + MOD(2-1+7,3), \\ & 3\cdot 3 + MOD(3-1+7,3)\} = \{2,4,8,12\} \\ L_8 = \{\ & 2, 3\cdot 1 + MOD(1-1+8,3), 3\cdot 2 + MOD(2-1+8,3), \\ & 3\cdot 3 + MOD(3-1+8,3)\} = \{2,5,9,10\} \\ L_9 = \{\ & 2, 3\cdot 1 + MOD(1-1+9,3), 3\cdot 2 + MOD(2-1+9,3), \\ & 3\cdot 3 + MOD(3-1+9,3)\} = \{2,6,7,11\} \end{aligned}$$

And for $i \in \{10,11,12\}$, $\left\lfloor \frac{i-1}{3} \right\rfloor = 3$,

$$MOD((j-1)\left(\left\lfloor \frac{i-1}{3} \right\rfloor - 1\right) + i, 3) = MOD(2j-2+i, 3).$$

So,

$$\begin{aligned} L_{10} = \{\ & 3, 3\cdot 1 + MOD(2-2+10,3), 3\cdot 2 + MOD(4-2+10,3), \\ & 3\cdot 3 + MOD(6-2+10,3)\} = \{3,4,6,11\} \\ L_{11} = \{\ & 3, 3\cdot 1 + MOD(2-2+11,3), 3\cdot 2 + MOD(4-2+11,3), \\ & 3\cdot 3 + MOD(6-2+11,3)\} = \{3,5,7,12\} \\ L_{12} = \{\ & 3, 3\cdot 1 + MOD(2-2+12,3), 3\cdot 2 + MOD(4-2+12,3), \\ & 3\cdot 3 + MOD(6-2+12,3)\} = \{3,6,8,10\}. \end{aligned}$$

3 Conclusion

In this paper was present an easy and fast construction of finite projective geometry with set of points $\mathcal{P} = \{0,1,...,n^2+n\}$ for prime number n, and set of lines $\mathcal{L} = \{L_i | i = \overline{0, n(n+1)}\}$, where L_i are defined by (1) and (2). The proposed procedure is restricted to prime numbers only, but it is very useful for construction of projective geometry with great number of points. Also, it can be used to make a quick algorithm for generating projective geometries.

References

1. Charles J. Colbourn Jeffrey H. Dinitz, The CRC handbook of combinatorial designs, CRC Press, 1996