PROJECTIVE COVERING DESIGNS

YEOW MENG CHEE AND SAN LING

ABSTRACT

A $(2,k,v)$ covering design is a pair $(X,\mathscr{F})$ such that X is a v-element set and $\mathscr{F}$ is a family of k-element subsets, called blocks, of X with the property that every pair of distinct elements of X is contained in at least one block. Let $C(2,k,v)$ denote the minimum number of blocks in a $(2,k,v)$ covering design. We construct in this paper a class of $(2,k,v)$ covering designs using number theoretic means, and determine completely the functions $C(2,6,6^n\cdot 28)$ for all $n \geqslant 0$, and $C(2,6,6^n\cdot 28-5)$ for all $n \geqslant 1$. Our covering designs have interesting combinatorial properties.

1. *Introduction*

A *t-covering design*, or more specifically a (t,k,v) covering design, of *order* v and *block size* k, is a pair $(X,\mathscr{F})$ such that X is a v-element set and $\mathscr{F}$ is a family of k-element subsets, called *blocks*, of X, with the property that every t-element subset of X occurs in at least one block.

Let $C(t,k,v)$ denote the minimum number of blocks in a (t,k,v) covering design. A (t,k,v) covering design $(X,\mathscr{F})$ with $|\mathscr{F}| = C(t,k,v)$ is called a *minimum* covering design. The problem of evaluating $C(t,k,v)$ is a generalization of the existence problem for Steiner systems, since $C(t,k,v) = \binom{v}{t}\Big/\binom{k}{t}$ if and only if there exists a Steiner system $S(t,k,v)$.

Let

$$L(t,k,v) = \left\lceil \frac{v}{k}\left\lceil \frac{v-1}{k-1}\left\lceil \cdots \left\lceil \frac{v-t+1}{k-t+1}\right\rceil \cdots \right\rceil\right\rceil\right\rceil.$$

Schönheim [**10**] proved that $C(t,k,v) \geqslant L(t,k,v)$ for all $v \geqslant k \geqslant t \geqslant 1$. Fort and Hedlund [**3**] have shown that $C(2,3,v) = L(2,3,v)$ for all $v \geqslant 3$. Recently, a simple proof of this was provided by Stanton and Rogers [**12**]. Mills [**8, 9**] has proved that $C(2,4,v) = L(2,4,v)$ for all $v \geqslant 4$ and $v \notin \{7,9,10,19\}$, and that $C(2,4,v) = L(2,4,v)+1$ for $v = 7$, 9 and 10, and $C(2,4,19) = L(2,4,19)+2$. The problem of determining $C(2,k,v)$ has not been completely solved for any $k \geqslant 5$. Recently, progress on the problem for $k = 5$ has been made by Lamken, Mills, Mullin and Vanstone [**6**] who showed that $C(2,5,v)$ can be determined for $v \equiv 1$ and 2 modulo 4 if $v \geqslant 13449$.

We are concerned in this paper with the construction of 2-covering designs and the evaluation of $C(2,6,v)$ for some values of v.

2. *Projective spaces over rings*

Let R be a commutative ring with unity and let S_k be the set of all $(k+1)$-tuples $(a_0,\ldots,a_k)$ of elements of R such that $a_0,\ldots,a_k$ generate R, that is, $\langle a_0,\ldots,a_k\rangle = R$.

We define the *projective k-space* over R, denoted $\mathbf{P}^k(R)$, to be a pair $(\mathscr{V}, \mathscr{B})$, such that both $\mathscr{V}$ and $\mathscr{B}$ are the sets of equivalence classes of elements of S_k under the equivalence relation given by

$$(a_0, \ldots, a_k) \sim (b_0, \ldots, b_k)$$

if and only if there exists $\lambda \in R^\times$ such that $a_i = \lambda b_i$ for $0 \leqslant i \leqslant k$, where $R^\times$ denotes the set of all units of R.

If $\mathbf{P}^k(R) = (\mathscr{V}, \mathscr{B})$, we call the elements of $\mathscr{V}$ *points* and the elements of $\mathscr{B}$ *hyperplanes* (or *lines* in the case $k = 2$). To differentiate between elements of $\mathscr{V}$ and $\mathscr{B}$ in notation, we denote a point $P \in \mathscr{V}$ by $(a_0 : \ldots : a_k)$ if $(a_0, \ldots, a_k)$ lies in the equivalence class P, and we denote a hyperplane $H \in \mathscr{B}$ by $[x_0 : \ldots : x_k]$ if $(x_0, \ldots, x_k)$ lies in the equivalence class H.

The point-hyperplane incidence relation in $\mathbf{P}^k(R)$ is defined as follows. A point $(a_0 : \ldots : a_k)$ lies on the hyperplane $[x_0 : \ldots : x_k]$ if and only if

$$a_0 x_0 + \ldots + a_k x_k = 0.$$

We remark that this definition of $\mathbf{P}^k(R)$ satisfies the principle of duality.

In the remainder of this section, we establish some properties of $\mathbf{P}^k(R)$. Throughout this paper, p denotes a prime and ϕ denotes Euler's totient function.

PROPOSITION 2.1. *The number of points (and hence the number of hyperplanes) in* $\mathbf{P}^k(\mathbf{Z}/n\mathbf{Z})$ *is*

$$n^k \prod_{p \mid n} \left(1 + \frac{1}{p} + \ldots + \frac{1}{p^k}\right).$$

Proof. A $(k+1)$-tuple $(a_0, \ldots, a_k)$ gives rise to a point in $\mathbf{P}^k(\mathbf{Z}/n\mathbf{Z})$ if and only if $\gcd(a_0, \ldots, a_k, n) = 1$. The number of such $(k+1)$-tuples is, by the principle of inclusion and exclusion,

$$n^{k+1} - \sum_{p \mid n} \left(\frac{n}{p}\right)^{k+1} + \sum_{p_i \mid n,\, p_1 \neq p_2} \left(\frac{n}{p_1 p_2}\right)^{k+1} - \ldots = n^{k+1} \prod_{p \mid n} \left(1 - \frac{1}{p^{k+1}}\right).$$

Taking the action of $(\mathbf{Z}/n\mathbf{Z})^\times$ into consideration, the number of points in $\mathbf{P}^k(\mathbf{Z}/n\mathbf{Z})$ is

$$\frac{n^{k+1} \prod_{p \mid n} (1 - 1/p^{k+1})}{\phi(n)} = n^k \prod_{p \mid n} \left(1 + \frac{1}{p} + \ldots + \frac{1}{p^k}\right).$$

We now compute the number of points on a hyperplane in $\mathbf{P}^k(\mathbf{Z}/n\mathbf{Z})$.

THEOREM 2.1 ([5, Theorem 6.2]). *A necessary and sufficient condition for the congruence*

$$a_1 x_1 + \ldots + a_m x_m + b \equiv 0 \bmod n$$

to have a solution $(x_1, \ldots, x_m)$ *is that* $\gcd(a_1, \ldots, a_m, n) \mid b$. *If this condition is satisfied, then the number of incongruent* mod n *solutions is*

$$n^{m-1} \gcd(a_1, \ldots, a_m, n).$$

COROLLARY 2.1. *The number of points on a hyperplane in* $\mathbf{P}^k(\mathbf{Z}/n\mathbf{Z})$ *is*

$$n^{k-1}\prod_{p|n}\left(1+\frac{1}{p}+\ldots+\frac{1}{p^{k-1}}\right).$$

By the principle of duality, this is also the number of hyperplanes passing through a point.

Proof. Let $[x_0:\ldots:x_k]$ be a fixed hyperplane in $\mathbf{P}^k(\mathbf{Z}/n\mathbf{Z})$. A point $(a_0:\ldots:a_k)$ in $\mathbf{P}^k(\mathbf{Z}/n\mathbf{Z})$ lies on $[x_0:\ldots:x_k]$ if and only if

$$a_0x_0+\ldots+a_kx_k\equiv 0 \bmod n. \tag{1}$$

From Theorem 2.1, the number of solutions $(a_0,\ldots,a_k)$ to (1) is n^k. However, $(a_0:\ldots:a_k)$ is a point if and only if $\gcd(a_0,\ldots,a_k,n)=1$. Hence, by the principle of inclusion and exclusion, the number of $(k+1)$-tuples $(a_0,\ldots,a_k)$ such that $\gcd(a_0,\ldots,a_k,n)=1$ is

$$n^k-\sum_{p|n}\left(\frac{n}{p}\right)^k+\sum_{p_i|n,\,p_1\neq p_2}\left(\frac{n}{p_1p_2}\right)^k-\ldots=n^k\prod_{p|n}\left(1-\frac{1}{p^k}\right).$$

Therefore the number of points on a line $[x_0:\ldots:x_k]$ is

$$\frac{n^k\prod_{p|n}(1-1/p^k)}{n\prod_{p|n}(1-1/p)}=n^{k-1}\prod_{p|n}\left(1+\frac{1}{p}+\ldots+\frac{1}{p^{k-1}}\right). \tag{2}$$

3. *A family of 2-covering designs*

In this section, we prove that the projective 2-space over $\mathbf{Z}/n\mathbf{Z}$, that is, $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})=(\mathscr{V},\mathscr{B})$, is a 2-covering design $(X,\mathscr{F})$ if we take $X=\mathscr{V}$ and $\mathscr{F}=(B_H)_{H\in\mathscr{B}}$, where $B_H=\{P\in\mathscr{V}:\ P \text{ lies on the line } H\}$. Henceforth, when we talk about $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$ as a covering design, we are actually referring to the ordered pair $(X,\mathscr{F})$.

THEOREM 3.1. *Let* $(a:b:c)$ *and* $(d:e:f)$ *be two points of* $\mathbf{P}^2(\mathbf{Z}/p^r\mathbf{Z})$. *If* $\gcd(ae-bd, af-cd, bf-ce, p^r)=p^\alpha, \alpha\leqslant r$, *then the number of lines passing through both points is*

(i) $p^{r-1}(p+1)$ *if* $\alpha=r$;

(ii) p^α *if* $\alpha<r$.

Proof. If there is a line in $\mathbf{P}^2(\mathbf{Z}/p^r\mathbf{Z})$ passing through $(a:b:c)$ and $(d:e:f)$, then let it be $[x:y:z]$. Without loss of generality, we may assume that a is a unit in $\mathbf{Z}/p^r\mathbf{Z}$. By the definition of $\mathbf{P}^2(\mathbf{Z}/p^r\mathbf{Z})$, we have

$$ax+by+cz\equiv 0 \bmod p^r, \tag{3}$$

$$dx+ey+fz\equiv 0 \bmod p^r. \tag{4}$$

Eliminating x, we obtain

$$(ae-bd)y+(af-cd)z\equiv 0 \bmod p^r. \tag{5}$$

Suppose $\gcd(ae-bd, af-cd, p^r)=p^\beta, \alpha\leqslant\beta\leqslant r$. We have $p^\beta\mid -c(ae-bd)+b(af-cd)$, that is, $p^\beta\mid a(bf-ce)$. Since $p\nmid a$, we have that $p^\beta\mid(bf-ce)$. Therefore, $\gcd(ae-bd, af-cd, p^r)=p^\alpha=\gcd(ae-bd, af-cd, bf-ce, p^r)$.

Case (I). If $\alpha=r$, then any y,z will satisfy (5). Note that if $p\mid y$ and $p\mid z$, then (3) implies that $p\mid x$. Hence, in order to find triples (x,y,z) such that $\gcd(x,y,z,n)=1$,

we need to have $p \nmid y$ or $p \nmid z$ (or both). The number of (y, z) (and hence (x, y, z), since x is uniquely determined by y, z) satisfying this condition is $p^{2r} - p^{2r-2}$. Hence the number of lines $[x:y:z]$ through these two points is

$$\frac{p^{2r} - p^{2r-2}}{\phi(p^r)} = p^{r-1}(p+1).$$

Case (II). If $\alpha < r$, (5) results in

$$\left(\frac{ae-bd}{p^\alpha}\right)y + \left(\frac{af-cd}{p^\alpha}\right)z \equiv 0 \bmod p^{r-\alpha}. \tag{6}$$

Without loss of generality, we may assume that $p^\alpha \| (ae-bd)$, and hence $\gcd(p, (ae-bd)/p^\alpha) = 1$. Note that if $p \mid z$, then $p \mid y$, and, by (3), $p \mid x$. Therefore we need $p \nmid z$ in order to find triples (x, y, z) such that $\gcd(x, y, z, n) = 1$. The number of such $(x, y, z) \bmod p^r$ is given as follows. For a given z, there is a unique $y \bmod p^{r-\alpha}$ satisfying (6), hence p^α such $y \bmod p^r$ satisfying (5). For $p \nmid z$, there are $\phi(p^r)$ choices for z. The value of x is uniquely determined by (y, z). Hence, the number of $(x, y, z) \bmod p^r$ satisfying $\gcd(x, y, z, n) = 1$ is $\phi(p^r) \cdot p^\alpha$. Therefore the number of lines $[x:y:z]$ through these two points is

$$\frac{\phi(p^r) \cdot p^\alpha}{\phi(p^r)} = p^\alpha.$$

THEOREM 3.2. *Let $(a:b:c)$ and $(d:e:f)$ be two points of $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$. If $n = \prod p^{r_p}$ and $\gcd(ae-bd, af-cd, bf-ce, n) = \prod p^{\alpha_p}$, $\alpha_p \leqslant r_p$ (for all $p \mid n$), then the number of lines passing through both points is*

$$\prod_{p \mid n : \alpha_p < r_p} p^{\alpha_p} \cdot \prod_{p \mid n : \alpha_p = r_p} p^{r_p - 1}(p+1).$$

Proof. This follows immediately from Theorem 3.1 by applying the Chinese Remainder Theorem.

COROLLARY 3.1. *The $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$ constructed is a 2-covering design for all $n > 1$.*

COROLLARY 3.2.

$$C\left(2, n\prod_{p \mid n}\left(1+\frac{1}{p}\right), n^2\prod_{p \mid n}\left(1+\frac{1}{p}+\frac{1}{p^2}\right)\right) \leqslant n^2\prod_{p \mid n}\left(1+\frac{1}{p}+\frac{1}{p^2}\right)$$

for all $n > 1$.

COROLLARY 3.3. *Any two points in $\mathbf{P}^2(\mathbf{Z}/p\mathbf{Z})$ lie on one and only one line.*

We remark that Corollary 3.3 implies that our definition of $\mathbf{P}^2(R)$ gives the classical projective plane when R is a finite field with p elements.

An *imbrical design* $\mathrm{ID}(v, k, b)$ is a $(2, k, v)$ covering design $(X, \mathscr{F})$ with $|\mathscr{F}| = b$ such that for every $B \in \mathscr{F}$, there exists a pair $\{x, y\} \subseteq B$ that is contained in no other elements of $\mathscr{F}$, that is,

$$|\{B' \in \mathscr{F} \setminus B : \{x, y\} \subseteq B'\}| = 0.$$

Imbrical designs are introduced by Mendelsohn and Assaf in [7], where they studied the *spectrum*

$$\mathrm{Spec}(v,k) = \{b\text{: there exists an ID}(v,k,b)\}$$

for $k = 3$ and 4. Our next result establishes an infinite family of imbrical designs.

THEOREM 3.3. $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$ *is an imbrical design for all* $n > 1$.

Proof. By Corollary 3.1, we need only show that for every line H in $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$, there exist two (distinct) points P_1 and P_2 lying on H such that no other line passes through both P_1 and P_2.

Let $[x:y:z]$ be a fixed line in $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$. Without loss of generality, assume $x \equiv 1 \bmod p^r$, where $p^r \| n$. Let $a = -y, b = 1, c = 0, d = -z, e = 0$ and $f = 1$. Then (3) and (4) are satisfied, and

$$\begin{aligned}\gcd(ae-bd, af-cd, bf-ce, p^r) &= \gcd(z, -y, 1, p^r)\\ &= 1.\end{aligned}$$

It then follows from Theorem 3.1 that there is one and only one line in $\mathbf{P}^2(\mathbf{Z}/p^r\mathbf{Z})$ passing through these two points. This can be done similarly to all the prime divisors of n. By the Chinese Remainder Theorem, one obtains two points $(a:b:c)$ and $(d:e:f)$ of $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$ and $\gcd(ae-bd, af-cd, bf-ce, n) = 1$. By Theorem 3.2, these can be chosen as our desired P_1 and P_2.

COROLLARY 3.4.

$$n^2 \prod_{p|n}\left(1+\frac{1}{p}+\frac{1}{p^2}\right) \in \mathrm{Spec}\left(n^2 \prod_{p|n}\left(1+\frac{1}{p}+\frac{1}{p^2}\right), n\prod_{p|n}\left(1+\frac{1}{p}\right)\right)$$

for all $n > 1$.

4. *Minimum covering designs*

The results in the previous sections show that $\mathbf{P}^2(\mathbf{Z}/4\mathbf{Z})$ gives a $(2,6,28)$ covering design $(X, \mathscr{F})$ with 28 blocks. Since $L(2,6,28) = 28$, this covering design is a minimum $(2,6,28)$ covering design. If we take $X = \{0,1,\ldots,27\}$, then the 28 blocks of this covering design can be given as follows.

1 2 5 9 12 15	0 2 4 8 11 14	0 1 3 7 10 13	2 13 18 23 24 27
1 14 16 22 24 26	0 15 17 22 23 25	13 14 15 19 20 21	2 10 12 17 21 26
1 9 11 17 21 27	0 8 12 16 20 27	2 7 11 16 20 25	1 8 10 18 19 25
0 7 9 18 19 26	2 3 6 19 22 27	1 4 6 20 23 26	0 5 6 21 24 25
4 9 10 20 22 24	5 7 8 21 22 23	3 11 12 19 23 24	6 11 12 13 18 22
6 9 10 14 16 23	6 7 8 15 17 24	4 5 13 16 17 19	3 5 14 17 18 20
3 4 15 16 18 21	5 10 11 15 26 27	4 7 12 14 25 27	3 8 9 13 25 26

We record this result as the following.

LEMMA 4.1. $C(2,6,28) = 28$.

An *orthogonal array* $\mathrm{OA}(v,k)$ is a $v^2 \times k$ array, $\mathscr{A}$, of symbols from a v-element set X which satisfies the following property: for any two columns i and j of $\mathscr{A}$, and for

any $(x,y)\in X\times X$, there is a unique row r such that $(\mathscr{A}(r,i),\mathscr{A}(r,j))=(x,y)$. The following generalization of the quadrupling construction of Stanton, Kalbfleish and Mullin [11] was obtained by Gardner [4]. We include its proof here for completeness.

THEOREM 4.1 (k-tupling construction). *Let $(X,\mathscr{F})$ be a $(2,k,v)$ covering design and let $0\leqslant a\leqslant v$. If there exists an orthogonal array $\mathrm{OA}(v-a,k)$, then there exists a $(2,k,kv-(k-1)a)$ covering design with $k|\mathscr{F}|+(v-a)^2$ blocks.*

Proof. We form k copies of the $(2,k,v)$ covering design on the sets $X_i=\{1,2,\ldots,a,x_{i,a+1},x_{i,a+2},\ldots,x_{i,v}\}$, $1\leqslant i\leqslant k$. We denote the corresponding family of blocks by $\mathscr{F}_i$. Now take an orthogonal array $\mathrm{OA}(v-a,k)$, $\mathscr{A}$, on the set of symbols $\{a+1,a+2,\ldots,v\}$. In this array $\mathscr{A}$, we replace $\mathscr{A}(r,i)$ by $x_{i,\mathscr{A}(r,i)}$ for all rows r and columns i. The rows of the array are now taken as a set $\mathscr{B}$ of blocks. It is straightforward to verify that $(\bigcup_{i=1}^{k}X_i,\mathscr{B}\cup(\bigcup_{i=1}^{k}\mathscr{F}_i))$ is a $(2,k,kv-(k-1)a)$ covering design.

Let $\mathrm{OA}(k)=\{v\colon$ there exists an $\mathrm{OA}(v,k)\}$. We require the following result (see [1]).

LEMMA 4.2. *If $t>4$ and $t\notin\{6,10,14,18,22,26,30,34,38,42,44\}$, then $t\in\mathrm{OA}(6)$.*

We now prove the two main results of this section.

THEOREM 4.2. *For any nonnegative integer n,*

$$C(2,6,6^n\cdot 28)=\frac{6^{n-1}(840+784(6^n-1))}{5}.$$

Proof. We proceed by induction on n. The statement of the theorem is true for $n=0$, by Lemma 4.1. Suppose that $C(2,6,6^{n-1}\cdot 28)=(6^{n-2}(840+784(6^{n-1}-1)))/5$. Then the k-tupling construction of Gardner (with $a=0$) shows that

$$C(2,6,6^n\cdot 28)\leqslant 6\cdot\frac{6^{n-2}(840+784(6^{n-1}-1))}{5}+(6^{n-1}\cdot 28)^2,$$

thus implying

$$C(2,6,6^n\cdot 28)\leqslant\frac{6^{n-1}(840+784(6^n-1))}{5}.$$

We note that all the orthogonal arrays required in the above constructions exist by Lemma 4.2. Now,

$$L(2,6,6^n\cdot 28)=\left\lceil\frac{6^n\cdot 28}{6}\left\lceil\frac{6^n\cdot 28-1}{5}\right\rceil\right\rceil,$$

and since $6^n\cdot 28-1\equiv 2 \bmod 5$,

$$\begin{aligned}L(2,6,6^n\cdot 28)&=6^{n-1}\cdot 28\left(\frac{6^n\cdot 28+2}{5}\right)\\&=\frac{6^{n-1}(840+784(6^n-1))}{5}.\end{aligned}$$

Therefore, $C(2,6,6^n\cdot 28) = (6^{n-1}(840+784(6^n-1)))/5$, which completes the proof.

THEOREM 4.3. *For any positive integer n,*

$$C(2,6,6^n\cdot 28-5) = \frac{(6^{n-1}\cdot 28-1)(6^n\cdot 28-3)+(6^{n-1}\cdot 28+2)}{5}.$$

Proof. Given any positive integer n, we use the k-tupling construction (with $a=1$) to obtain a $(2,6,6^n\cdot 28-5)$ covering design from a minimum $(2,6,6^{n-1}\cdot 28)$ covering design (provided by Theorem 4.2) and an orthogonal array $\mathrm{OA}(6^{n-1}\cdot 28-1, 6)$ (which exists by Lemma 4.2). The constructed covering shows that

$$\begin{aligned} C(2,6,6^n\cdot 28-5) &\leqslant \frac{6^{n-1}(840+784(6^{n-1}-1))}{5}+(6^{n-1}\cdot 28-1)^2 \\ &\leqslant \frac{(6^{n-1}\cdot 28-1)(6^n\cdot 28-3)+(6^{n-1}\cdot 28+2)}{5}. \end{aligned}$$

Now,

$$L(2,6,6^n\cdot 28-5) = \left\lceil \frac{6^n\cdot 28-5}{6}\left\lceil \frac{6^n\cdot 28-6}{5}\right\rceil\right\rceil,$$

and since $6^n\cdot 28-6 \equiv 2 \bmod 5$,

$$\begin{aligned} L(2,6,6^n\cdot 28-5) &= \left\lceil \frac{(6^n\cdot 28-5)(6^n\cdot 28-3)}{30}\right\rceil \\ &= (6^{n-1}\cdot 28-1)\left(\frac{6^n\cdot 28-3}{5}\right)+\left\lceil \frac{6^n\cdot 28-3}{30}\right\rceil. \end{aligned}$$

However, $6^n\cdot 28-3 \equiv 15 \bmod 30$ for all $n>0$, therefore we have

$$\begin{aligned} L(2,6,6^n\cdot 28-5) &= (6^{n-1}\cdot 28-1)\left(\frac{6^n\cdot 28-3}{5}\right)+\frac{6^n\cdot 28+12}{30} \\ &= \frac{(6^{n-1}\cdot 28-1)(6^n\cdot 28-3)+(6^{n-1}\cdot 28+2)}{5}. \end{aligned}$$

This proves the theorem.

5. *Regular coverings*

Let $(X,\mathscr{F})$ be a $(2,k,v)$ covering design. We can construct a multigraph G with vertex set X such that if $\{x,y\}\subseteq X$ occurs in λ blocks of $\mathscr{F}$, then the edge $\{x,y\}$ appears $\lambda-1$ times in G. The multigraph G is commonly called the *excess* of the covering design.

In [2], Bermond, Bond and Sotteau defined a regular covering to be a $(2,k,v)$ covering design whose excess is regular of degree Δ. They call a regular covering *minimum* if Δ is as small as possible, and posed the problem of constructing minimum regular coverings. In this section, we establish the existence of an infinite family of minimum regular coverings with block size 6.

The following two propositions are easy to prove.

PROPOSITION 5.1. *The degree Δ of the regular excess of a regular $(2,k,v)$ covering satisfies the following congruences*:

$$v-1+\Delta \equiv 0 \bmod k-1, \tag{7}$$

$$v(v-1+\Delta) \equiv 0 \bmod k(k-1). \tag{8}$$

PROPOSITION 5.2. *If $k=6$ and $v=6^n\cdot 28$, $n\geqslant 0$, then $\Delta=3$ is the minimum positive integer satisfying the congruences* (7) *and* (8).

We show that Gardner's k-tupling construction preserves the regularity of the excess when $a=0$.

LEMMA 5.1. *If there exists a regular $(2,k,v)$ covering with regular excess of degree Δ, and there exists an orthogonal array $\mathrm{OA}(v,k)$, then there exists a regular $(2,k,kv)$ covering with regular excess of degree Δ.*

Proof. Given a regular $(2,k,v)$ covering with regular excess G of degree Δ, we construct a $(2,k,kv)$ covering using Gardner's k-tupling construction given in the proof of Theorem 4.1. Each of the pairs $\{x_{i,j},x_{i',j'}\}, 1\leqslant i,i'\leqslant k, i\neq i', 1\leqslant j,j'\leqslant v$, appears in exactly one block of this $(2,k,kv)$ covering and hence contributes no edge to the excess. Consequently, the excess of this $(2,k,kv)$ covering is a disjoint union of k copies of G.

LEMMA 5.2. *There exists a minimum regular $(2,6,28)$ covering.*

Proof. The minimum $(2,6,28)$ covering design constructed in Section 4 has an excess that is the disjoint union of 7 K_4 (and hence regular of degree 3).

It follows from Lemmas 5.1 and 5.2 by induction that there exists a regular $(2,6,6^n\cdot 28)$ covering for all $n\geqslant 0$. Moreover, the excess of this covering is the disjoint union of $6^n\cdot 7$ K_4, and hence regular of degree 3. Therefore by Proposition 5.2, this regular $(2,6,6^n\cdot 28)$ covering is minimum. We record this result as follows.

THEOREM 5.1. *There exists a minimum regular $(2,6,6^n\cdot 28)$ covering for all $n\geqslant 0$. Moreover, each component of the excess is a K_4.*

6. *Conclusion*

We have provided in this paper a new number theoretic construction for 2-covering designs. As a result of this construction, we are able to completely determine the functions $C(2,6,6^n\cdot 28)$ and $C(2,6,6^{n+1}\cdot 28-5)$ for all $n\geqslant 0$, and prove the existence of an infinite family of imbrical designs and minimum regular coverings with block size 6.

We expect our 2-covering designs to possess many more interesting properties which may be useful in the construction of other combinatorial configurations.

References

1. R. J. R. ABEL, 'Four mutually orthogonal Latin squares of orders 28 and 52', *J. Combin. Theory Ser. A* 58 (1991) 306–309.

2. J.-C. BERMOND, J. BOND and D. SOTTEAU, 'On regular packings and coverings', *Ann. Discrete Math.* 34 (1987) 81–100.
3. M. K. FORT, JR and G. A. HEDLUND, 'Minimal covering of pairs by triples', *Pacific J. Math.* 8 (1958) 709–719.
4. B. I. GARDNER, 'On coverings and (r, λ)-systems', PhD Thesis, Department of Combinatorics and Optimization, University of Waterloo, Ontario, Canada, 1972.
5. L. K. HUA, *Introduction to number theory* (Springer, Berlin, 1982).
6. E. R. LAMKEN, W. H. MILLS, R. C. MULLIN and S. A. VANSTONE, 'Coverings of pairs by quintuples', *J. Combin. Theory Ser. A* 44 (1987) 49–68.
7. E. MENDELSOHN and A. ASSAF, 'On the spectrum of imbrical designs', *Ann. Discrete Math.* 34 (1987) 363–370.
8. W. H. MILLS, 'On the covering of pairs by quadruples I', *J. Combin. Theory Ser. A* 13 (1972) 55–78.
9. W. H. MILLS, 'On the covering of pairs by quadruples II', *J. Combin. Theory Ser. A* 15 (1973) 138–166.
10. J. SCHÖNHEIM, 'On coverings', *Pacific J. Math.* 14 (1964) 1405–1411.
11. R. G. STANTON, J. G. KALBFLEISH and R. C. MULLIN, 'Covering and packing designs', *Proceedings of the Second Chapel Hill Conference on Combinatorial Mathematics and its Applications* (University of North Carolina, Chapel Hill, 1970) 428–450.
12. R. G. STANTON and M. J. ROGERS, 'Packings and coverings by triples', *Ars Combin.* 13 (1982) 61–69.

Planning and Infrastructure Department
National Computer Board
71 Science Park Drive, S0511
Republic of Singapore

Department of Mathematics
National University of Singapore
Lower Kent Ridge Road, S0511
Republic of Singapore