Combinatorial Coverings from Geometries over Principal Ideal Rings

Yeow Meng Chee,[1] **San Ling**[2]

[1] *Internationalisation Office, National Computer Board, 71 Science Park Drive, Singapore 118253, Republic of Singapore*

[2] *Department of Mathematics, National University of Singapore, Singapore 119260, Republic of Singapore*

Received October 8, 1997; accepted June 13, 1998

Abstract: **A t-(v, k, λ) covering is an incidence structure with v points, each block incident on exactly k points, such that every set of t distinct points is incident on at least λ blocks. By considering certain geometries over finite principal ideal rings, we construct infinite families of t-(v, k, λ) coverings having many interesting combinatorial properties.** © 1999 John Wiley & Sons, Inc. J Combin Designs 7: 247–268, 1999

Keywords: *principal ideal rings; symmetric minimal coverings; imbrical designs; regular covering designs*

1. INTRODUCTION

A (*finite*) *incidence structure* is a triple $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$, where $\mathcal{P}$ and $\mathcal{B}$ are two nonempty disjoint finite sets, and I is a binary *incidence* relation between $\mathcal{P}$ and $\mathcal{B}$, that is, $I \subseteq \mathcal{P} \times \mathcal{B}$. The elements of $\mathcal{P}$ are called *points*, and the elements of $\mathcal{B}$ are called *blocks*. If $(P, B) \in I$, we say that P and B are *incident*. We also extend the notion of incidence to sets of points by saying that a set $\mathcal{Q} \subseteq \mathcal{P}$ is *incident* with a block $B \in \mathcal{B}$ if $(P, B) \in I$ for all $P \in \mathcal{Q}$. The *pencil* of a point $P \in \mathcal{P}$ is the set $(P) = \{B \in \mathcal{B} | (P, B) \in I\}$, and the *trace* of a block

Correspondence to: San Ling, Dept. of Mathematics, National University of Singapore, Lower Kent Ridge Road, Singapore 119260.

Contract grant sponsor: RP; contract grant number: 960668/M. The second author is funded by Grant No. RP 960668/M.

 CCC 1063 8539/99/040247-22

$B \in \mathcal{B}$ is the set $(B) = \{P \in \mathcal{P} | (P, B) \in I\}$. The order of $\mathcal{S}$ is $|\mathcal{P}|$. If $|\mathcal{P}| = |\mathcal{B}|$, then $\mathcal{S}$ is said to be *symmetric*. If $|(B)| = k$ for all $B \in \mathcal{B}$, then $\mathcal{S}$ is said to be k-*uniform*.

For integers $0 < t \leq k \leq v$ and $\lambda \geq 0$, a t-(v, k, λ) *design* is a k-uniform incidence structure $(\mathcal{P}, \mathcal{B}, I)$ of order v such that every set of t distinct points is incident with precisely λ blocks. A 2-(v, k, λ) design is commonly known as a *balanced incomplete block design* (BIBD). A t-(v, k, λ) design can only exist if the *divisibility conditions* $\lambda\binom{v-i}{t-i} \equiv 0 \bmod \binom{k-i}{t-i}$, for $0 \leq i \leq t$, are satisfied. The notion of *minimum coverings* is one of many possible generalizations of t-(v, k, λ) designs to encompass situations when the divisibility conditions are not met, or when t-(v, k, λ) designs do not exist. A $(t; \lambda)$-*covering*, or more precisely a t-(v, k, λ) *covering*, is a k-uniform incidence structure $(\mathcal{P}, \mathcal{B}, I)$ of order v such that every set of t distinct points is incident with *at least* λ blocks of $\mathcal{B}$. The minimum number of blocks in a t-(v, k, λ) covering is the *covering number*

$$C_\lambda(v, k, t) = \min\{|\mathcal{B}| \ | (\mathcal{P}, \mathcal{B}, I) \text{ is a } t\text{-}(v, k, \lambda) \text{ covering}\}.$$

We adopt the usual convention of writing $C(v, k, t)$ for $C_1(v, k, t)$. A t-(v, k, λ) covering $(\mathcal{P}, \mathcal{B}, I)$ is *minimum* if $|\mathcal{B}| = C_\lambda(v, k, t)$. So every t-(v, k, λ) design is a minimum t-(v, k, λ) covering.

The focus of this article is the construction of t-(v, k, λ) coverings from geometries over principal ideal rings. Geometry over rings constitutes an important part of the study of incidence geometry (see [12] for an excellent survey). In particular, we construct two new infinite families of minimum t-(v, k, λ) coverings, and show that coverings from certain geometries possess many interesting combinatorial properties. The results obtained generalize and extend previous ones in [4].

2. FINITE PRINCIPAL IDEAL RINGS

A. Some Definitions and Results

Definition 2.1. *A finite principal ideal ring (PIR) is a finite commutative ring with unity, in which every ideal is principal. A PIR is called* special *if it has only one prime ideal M and if M is nilpotent, that is, if $M^r = 0$ for some positive integer r.*

We recall the structure theorem for PIRs [13]:

Theorem 2.1 (Structure Theorem for PIRs). *A direct sum of PIRs is itself a PIR. Every PIR is a direct sum of PIDs and of special PIRs. (A PID is a principal ideal domain).*

Since we are interested only in finite PIRs, and since finite PIDs are fields (hence special PIRs), by the structure theorem for PIRs, it suffices for us to consider finite special PIRs.

For the remainder of this section, let R be a finite special PIR with maximal ideal $M = \langle \pi \rangle$, and let r denote the smallest positive integer such that $M^r = 0$. We note that the prime element π is unique up to multiplication by a unit of R. We suppose also that the quotient R/M is isomorphic to $\mathbb{F}_q$, where $q = p^n$, a power of a prime p.

We state without proof three facts on finite special PIRs that are of use later. The proofs are easy exercises in ring theory (cf. [6], Chapter 1).

1. If $r > 1$, then for $1 \leq i \leq r - 1$, M^i/M^{i+1} is an R/M-vector space of dimension one.
2. We have $|R| = q^r$ and $|M^i| = q^{r-i}$ for $1 \leq i \leq r$.
3. The only ideals in R are: $R, M, M^2, \ldots, M^r = 0$.

For an ideal $M^j = \langle \pi^j \rangle$ and $\alpha, \beta \in R$, by

$$\alpha \equiv \beta \bmod M^j \quad \text{or} \quad \alpha \equiv \beta \bmod \pi^j,$$

we mean that $\alpha - \beta \in M^j = \langle \pi^j \rangle$.

B. Examples of Finite Special PIRs

We give some examples of finite special PIRs that will be of use later in the construction of associated designs.

1. **Finite Fields.** By taking $R = \mathbb{F}_q$, where $q = p^n$ is a power of a prime p, we have our first examples of finite special PIRs with $M = 0$.
2. **The rings $\mathbb{Z}/p^r\mathbb{Z}$ (p prime).** For $R = \mathbb{Z}/p^r\mathbb{Z}$, it is clear that R is a finite special PIR with $M = \langle p \rangle$, and $M^r = 0$.
3. **Examples from Polynomial Rings.** For $q = p^n$ a prime power, let $R = \mathbb{F}_q[X]/\langle X^r \rangle$, where r is a positive integer. A maximal ideal M in R corresponds to a maximal ideal $\mathcal{I}$ of $\mathbb{F}_q[X]$ containing $\langle X^r \rangle$. Since $\mathcal{I}$ is a prime ideal, it follows that $X \in \mathcal{I}$; so $\langle X \rangle \subseteq \mathcal{I}$. Therefore, $\mathcal{I} = \langle X \rangle$ since $\mathbb{F}_q[X]/\langle X \rangle \simeq \mathbb{F}_q$. Consequently, R has only one maximal ideal, namely $M = \langle X \rangle / \langle X^r \rangle$. Clearly $M^r = 0$, hence $R = \mathbb{F}_q[X]/\langle X^r \rangle$ is a special PIR. The degenerate case $r = 1$ is the case when R is a finite field (Example 1).
4. **Examples from Function Fields.** Let F be a function field with field of constants $\mathbb{F}_q$. Let P be a place of F. The ring $\mathcal{O}_P = \{\alpha \in F | v_P(\alpha) \geq 0\}$ where v_P is the normalized valuation of the place P, is a discrete valuation ring with unique maximal (principal) ideal $\mathcal{M}_P = \{\alpha \in F | v_P(\alpha) > 0\}$. The quotient $\mathcal{O}_P/\mathcal{M}_P$ is a finite field extension of $\mathbb{F}_q$. Let $R = \mathcal{O}_P/\mathcal{M}_P^r$, where r is a positive integer. Then R is a finite special PIR with $M = \mathcal{M}_P/\mathcal{M}_P^r$.

Remark. Given any integer $r \geq 1$ and any prime power $q = p^n$, the construction in Example 3 ensures the existence of a finite special PIR R, with maximal ideal M, such that $R/M \simeq \mathbb{F}_q$ and $M^r = 0 (M^{r-1} \neq 0)$.

C. Rings of Stable Rank 2

Definition 2.2. *A commutative ring R with unity is said to be of stable rank 2 if, for all integers $n \geq 2$, the following condition is satisfied*:

(SR_n) *for every $x_1, \ldots, x_n \in R$ satisfying $\langle x_1, \ldots, x_n \rangle = R$, there exist $a_1, \ldots, a_{n-1} \in R$ such that $\langle x_1 + a_1 x_n, \ldots, x_{n-1} + a_{n-1} x_n \rangle = R$.*

(Actually, the notion of a ring of stable rank 2 exists even for noncommutative rings, but we do not need this more general version here.)

It is well known that rings satisfying condition (SR_n) automatically satisfy condition (SR_{n+1}) for all $n \geq 2$. It is also easy to see that all PIRs satisfy (SR_2), so they are rings of stable rank 2.

3. THE CONSTRUCTION

A. Projective Spaces over Rings

For a commutative ring R with unity, and let S_t be the set of all $(t+1)$-tuples $(a_0, \ldots, a_t)$ of elements of R such that $a_0, \ldots, a_t$ generate R, that is, $\langle a_0, \ldots, a_t \rangle = R$. We define the *projective t-space over R*, denoted $\mathbf{P}^t(R)$, to be an incidence structure $(\mathcal{P}, \mathcal{B}, I)$, such that both $\mathcal{P}$ and $\mathcal{B}$ are the sets of equivalence classes of elements of S_t under the equivalence relation given by

$$(a_0, \ldots, a_t) \sim (b_0, \ldots, b_t)$$

if and only if there exists $\lambda \in R^\times$ such that $a_i = \lambda b_i$ for $0 \leq i \leq t$, where $R^\times$ denotes the (multiplicative) group of all units of R. To differentiate between elements of $\mathcal{P}$ and $\mathcal{B}$ in notation, we denote a point $P \in \mathcal{P}$ by $(a_0 : \cdots : a_t)$ if $(a_0, \ldots, a_t)$ lies in the equivalence class P, and we denote a block $B \in \mathcal{B}$ by $[x_0 : \cdots : x_t]$ if $(x_0, \ldots, x_t)$ lies in the equivalence class B. The incidence relation I in $\mathbf{P}^t(R)$ is defined as follows. Let $P = (a_0 : \cdots : a_t) \in \mathcal{P}$ be a point and $B = [x_0 : \cdots : x_t] \in \mathcal{B}$ be a block. Then $(P, B) \in I$ if and only if

$$\sum_{i=0}^{t} a_i x_i = 0. \tag{1}$$

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

When R is a ring of stable rank 2, an equivalent formulation of a projective t-space over R is given in [12, Sec. 3]. The proof of the following proposition is found in [12]. We remark here that the parameters v and k in the general case may be found using techniques analogous to those in Section 3 C.

Proposition 3.1 ([12, Proposition 4.5]). *When R is a finite ring of stable rank 2, $\mathbf{P}^t(R)$ is a $(t; 1)$-covering.*

Now let R be an arbitrary finite PIR. By the structure theorem for PIRs, we may write such an R as the direct sum (or product) of finitely many (finite) special PIRs $R_1, \ldots, R_s$,

$$R = R_1 \times \cdots \times R_s.$$

An element x of R may equivalently be regarded as an s-tuple $(x_1, \ldots, x_s)$, where $x_i \in R_i$. Let M_i denote the maximal ideal of R_i, let r_i denote the smallest positive integer such that $M_i^{r_i} = 0$, and let $q_i = p_i^{n_i}$ be the prime power such that $R_i/M_i \simeq \mathbb{F}_{q_i}$.

For each i, the construction of $\mathbf{P}^t(R_i)$ has been described above. We take the Cartesian product $\times_{i=1}^{s} \mathbf{P}^t(R_i)$ to refer simply to the incidence structure $(\mathcal{P}, \mathcal{B}, I)$, where

- **i.** a point $P \in \mathcal{P}$ is an s-tuple $(P_1, \ldots, P_s)$ such that P_i is a point in $\mathbf{P}^t(R_i)$;
- **ii.** a block $B \in \mathcal{B}$ is an s-tuple $(B_1, \ldots, B_s)$ such that B_i is a block in $\mathbf{P}^t(R_i)$; and
- **iii.** $(P, B) \in I$ if $(P_i, B_i) \in I$ for all $i = 1, 2, \ldots, s$.

Theorem 3.1. *There is a natural bijection between $\mathbf{P}^t(R)$ and $\times_{i=1}^{s} \mathbf{P}^t(R_i)$ that preserves incidence.*

Proof. Let $P = (a_0 : \cdots : a_t)$ be a point of $\mathbf{P}^t(R)$. For each $j = 0, \ldots, t$, we think of a_j as $(a_{j1}, \ldots, a_{js}) \in R_1 \times \cdots \times R_s$. Since $\langle a_0, \ldots, a_t \rangle = R$, it follows that for each

$i = 1, \ldots, s, \langle a_{0i}, \ldots, a_{ti} \rangle = R_i$. Let P_i be the point $(a_{0i} : \cdots : a_{ti})$ in $\mathbf{P}^t(R_i)$. For a block $B = [x_0 : \cdots : x_t]$ of $\mathbf{P}^t(R)$, we may similarly define a block B_i of $\mathbf{P}^t(R_i)$ for each $i = 1, \ldots, s$. We claim that the map

$$\begin{aligned} \Xi : \mathbf{P}^t(R) &\to \times_{i=1}^s \mathbf{P}^t(R_i), \\ P &\mapsto (P_1, \ldots, P_s), \\ B &\mapsto (B_1, \ldots, B_s), \end{aligned}$$

is the desired bijection that preserves the incidence relation.

The map Ξ is well defined in the sense that the image of a point (respectively, a block) of $\mathbf{P}^t(R)$ under Ξ exists, and is uniquely defined. For instance, write P as $(\lambda a_0 : \cdots : \lambda a_t)$, where $\lambda \in R^\times$. Taking λ as $(\lambda_1, \ldots, \lambda_s) \in R_1 \times \cdots \times R_s$, it is clear that $\lambda_i \in R_i^\times$ for each $i = 1, \ldots, s$. Then $(\lambda_i a_{0i}, \ldots, \lambda_i a_{ti})$ defines the same point in $\mathbf{P}^t(R_i)$ as $(a_{0i}, \ldots, a_{ti})$, namely P_i.

To see the surjectivity of Ξ, we start with a point $(P_1, \ldots, P_s)$ of $\times_{i=1}^s \mathbf{P}^t(R_i)$. Write $P_i = (a_{0i} : \cdots : a_{ti})$. Define $a_0, \ldots, a_t \in R$ as follows:

$$a_j = (a_{j1}, \ldots, a_{js}) \in R_1 \times \cdots \times R_s.$$

Since for each $i, \langle a_{0i}, \ldots, a_{ti} \rangle = R_i$, it follows therefore that $\langle a_0, \ldots, a_t \rangle = R$. So $P = (a_0 : \cdots : a_t)$ is indeed a point of $\mathbf{P}^t(R)$, and clearly $\Xi(P) = (P_1, \ldots, P_s)$.

For the injectivity of Ξ, let $P = (a_0 : \cdots : a_t)$ and $P' = (a'_0 : \cdots : a'_t)$ be two points such that $\Xi(P) = \Xi(P')$. Using the same notation as above, for all $i = 1, \ldots, s$, we have

$$(a_{0i} : \cdots : a_{ti}) = (a'_{0i} : \cdots : a'_{ti}).$$

In other words, there exists a $\lambda_i \in R_i^\times$ such that $a_{ji} = \lambda_i a'_{ji}$ for all $j = 0, \ldots, t$. Taking $\lambda \in R^\times$ to be $\lambda = (\lambda_1, \ldots, \lambda_s) \in R_1 \times \cdots \times R_s$, it then follows that $a_j = \lambda a'_j$ for $j = 0, \ldots, t$, that is, $P = P'$.

Given a point $P = (a_0 : \cdots : a_t)$ and a block $B = [x_0 : \cdots : x_t]$ in $\mathbf{P}^t(R)$, recall that P is incident with B if and only if (1) holds. In view of the identification $R = R_1 \times \cdots \times R_s$, (1) holds if and only if

$$\sum_{j=0}^{t} a_{ji} x_{ji} = 0 \qquad \text{in } R_i, \tag{2}$$

for $i = 1, \ldots, s$. Now (2) is equivalent to saying that P_i is incident with B_i for every $i = 1, \ldots, s$, that is, the point $(P_1, \ldots, P_s)$ of $\times_{i=1}^s \mathbf{P}^t(R_i)$ is incident with the block $(B_1, \ldots, B_s)$.

This completes the proof of Theorem 3.1. □

B. Blowing Up Coverings

In this section, we describe a construction for blowing up coverings.

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ be a t-(v, k, a) covering, and λ, μ be positive integers. Let $\mathcal{P}' = \{P^{(i)} | 1 \le i \le \mu, P \in \mathcal{P}\}, \mathcal{B}' = \{B^{(j)} | 1 \le j \le \lambda, B \in \mathcal{B}\}$, and $I' = \{(P^{(i)}, B^{(j)}) | 1 \le i \le \mu, 1 \le j \le \lambda$, and $(P, B) \in I\}$. We call $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', I')$ the (μ, λ)-*blowup* of $\mathcal{S}$. For simplicity, we abbreviate (λ, λ)-blowup to λ-blowup. Let $P \in \mathcal{P}$ and $B \in \mathcal{B}$. The set $\{P^{(i)} | 1 \le i \le \mu\}$ is called the *fiber* of P, and the set $\{B^{(j)} | 1 \le j \le \lambda\}$ is the *fiber* of B. We define $\vartheta_{\lambda,\mu} : \mathcal{S}' \to \mathcal{S}$ to be the map such that $\vartheta_{\lambda,\mu}(P^{(i)}) = P$ for any $P^{(i)} \in \mathcal{P}'$, and $\vartheta_{\lambda,\mu}(B^{(j)}) = B$ for any $B^{(j)} \in \mathcal{B}'$. When $\lambda = \mu$, we abbreviate $\vartheta_{\lambda,\mu}$ to ϑ_λ.

Lemma 3.1. *The (μ, λ)-blowup of a t-(v, k, a) covering is a t-$(\mu v, \mu k, \lambda a)$ covering.*

We omit the proof of Lemma 3.1, which is straightforward.

Let R be a finite PIR. Since $\mathbf{P}^t(R)$ is a t-$(v, k, 1)$ covering, Lemma 3.1 applies, so we denote by $\mathbf{P}^t_\lambda(R)$ the t-$(\lambda v, \lambda k, \lambda)$ covering which is the λ-blowup of $\mathbf{P}^t(R)$.

C. Counting Points and Blocks

We now compute $|\mathcal{P}|$ and $|B|, B \in \mathcal{B}$, for any $\mathbf{P}^t_\lambda(R) = (\mathcal{P}, \mathcal{B}, I)$, where R is a finite PIR. We continue to write $R = R_1 \times \cdots \times R_s$, where $R_1, \ldots, R_s$ are finite special PIRs.

Proposition 3.2. *Let R be a finite PIR. The number of points (and hence the number of blocks) in $\mathbf{P}^t_\lambda(R)$ is*

$$\lambda |R|^t \prod_i \left(1 - \frac{1}{|R_i/M_i|^{t+1}}\right) \Big/ \left(1 - \frac{1}{|R_i/M_i|}\right) = \lambda \prod_i q_i^{(r_i-1)t} \left(\frac{q_i^{t+1} - 1}{q_i - 1}\right).$$

Proof. By Theorem 3.1, it suffices to prove the Proposition in the case when R is a finite special PIR, with maximal ideal M, $M^r = 0$, $M^{r-1} \neq 0$ and $R/M \simeq \mathbb{F}_q$, and when $\lambda = 1$. We need to show that the number of points in this case is then $(|R|^{t+1} - |M|^{t+1})/(|R| - |M|)$.

A $(t+1)$-tuple $(a_0, \ldots, a_t)$ gives rise to a point in $\mathbf{P}^t(R)$ if and only if not all of $a_0, \ldots, a_t$ belong to M. Two such $(t+1)$-tuples $(a_0, \ldots, a_t)$ and $(b_0, \ldots, b_t)$ give rise to the same point in $\mathbf{P}^t(R)$ if and only if there exists $u \in R^\times$ such that $a_i = ub_i$ for $0 \leq i \leq t$. □

Proposition 3.3. *The number of points incident with a block in $\mathbf{P}^t_\lambda(R)$ is*

$$\lambda |R|^{t-1} \prod_i \left(1 - \frac{1}{|R_i/M_i|^t}\right) \Big/ \left(1 - \frac{1}{|R_i/M_i|}\right) = \lambda \prod_i (q_i^{r_i-1})^{t-1} \left(\frac{q_i^t - 1}{q_i - 1}\right).$$

By the principle of duality, this is also the number of blocks incident with a point.

Proof. Using the same argument as in the proof of Proposition 3.2, it suffices to prove this Proposition when R is a finite special PIR with $\lambda = 1$.

Given a fixed block $[x_0 : \cdots : x_t]$ in $\mathbf{P}^t(R)$, we may suppose without loss of generality that $x_0 \notin M$. A point $(a_0 : \cdots : a_t)$ is incident with $[x_0 : \cdots : x_t]$ if and only if $\sum_{i=0}^t a_i x_i = 0$. Given $a_1, \ldots, a_t$, then a_0 is uniquely determined since x_0 is a unit. For $(a_0 : \cdots : a_t)$ to be a point in $\mathbf{P}^t(R)$, not all of $a_1, \ldots, a_t$ can belong to M simultaneously. The same argument as in Proposition 3.2 then completes the proof. □

D. (2; λ)-Coverings

In the case when $t = 2$, given a set of two distinct points, we can determine precisely the number of blocks that are incident with this set. We state this as:

Theorem 3.2. *Let P_1 and P_2 be two points of $\mathbf{P}^2_\lambda(R)$ such that $\vartheta_\lambda(P_1) = (a : b : c)$ and $\vartheta_\lambda(P_2) = (d : e : f)$ in $\mathbf{P}^2(R)$. Let $(a_i : b_i : c_i)$ and $(d_i : e_i : f_i)$ be the points in $\mathbf{P}^2(R_i)$ $(1 \leq i \leq s)$ corresponding to $\vartheta_\lambda(P_1)$ and $\vartheta_\lambda(P_2)$. If $\langle a_i e_i - b_i d_i, a_i f_i - c_i d_i, b_i f_i - c_i e_i \rangle =$*

$M_i^{\alpha_i}, 0 \le \alpha_i \le r_i$, *for each* $1 \le i \le s$, *then the number of blocks in* $\mathbf{P}^2_\lambda(R)$ *incident with both* P_1 *and* P_2 *is*

$$\lambda \left(\prod_{i:\alpha_i < r_i} q_i^{\alpha_i} \right) \left(\prod_{i:\alpha_i = r_i} q_i^{r_i - 1}(q_i + 1) \right).$$

Proof. A block $B = (B_1, \ldots, B_s)$ is incident with $(a : b : c)$ and $(d : e : f)$ in $\mathbf{P}^2(R)$ if and only if B_i is incident with $(a_i : b_i : c_i)$ and $(d_i : e_i : f_i)$ for all $i = 1, \ldots, s$. By definition of $\mathbf{P}^t_\lambda(R)$ and Theorem 3.1, to prove Theorem 3.2, it suffices to prove it when $\lambda = 1$ and when R is a finite special PIR, which we assume for the rest of this proof.

If there is a block in $\mathbf{P}^2(R)$ incident with $(a : b : c)$ and $(d : e : f)$, then let it be $[x : y : z]$. Without loss of generality, we may assume that $a \in R^\times$. By the definition of $\mathbf{P}^2(R)$, we have

$$ax + by + cz = 0, \tag{3}$$

$$dx + ey + fz = 0. \tag{4}$$

Eliminating x, we obtain

$$(ae - bd)y + (af - cd)z = 0. \tag{5}$$

Suppose $\langle ae - bd, af - cd \rangle = M^\beta, \alpha \le \beta \le r$. We have $-c(ae - bd) + b(af - cd) \in M^\beta$, that is, $a(bf - ce) \in M^\beta$. Since $a \in R^\times$, we have that $(bf - ce) \in M^\beta$. Therefore, $\langle ae - bd, af - cd \rangle = M^\alpha = \langle ae - bd, af - cd, bf - ce \rangle$.

Case (I): If $\alpha = r$, then any y, z will satisfy (5). Note that if $y \in M$ and $z \in M$, then (3) implies that $x \in M$. Hence, in order to find triples (x, y, z) such that $\langle x, y, z \rangle = R$, we need to have $y \notin M$ or $z \notin M$ (or both). The number of (y, z) (and hence (x, y, z), since x is uniquely determined by y, z) satisfying this condition is $|R|^2 - |M|^2$. Hence the number of blocks $[x : y : z]$ incident with both points is

$$\frac{|R|^2 - |M|^2}{|R| - |M|} = q^{r-1}(q + 1).$$

Case (II): If $\alpha < r$, we may assume that $ae - bd = u\pi^\alpha$, where $u \in R^\times$. Writing $af - cd = v\pi^\alpha$, (5) becomes

$$uy + vz \in M^{r-\alpha}. \tag{6}$$

Note that if $z \in M$ then $y \in M$, and by (3), $x \in M$. Therefore we need $z \notin M$ in order to find triples (x, y, z) such that $\langle x, y, z \rangle = R$. The number of such (x, y, z) is given as follows. For a given z, the number of y satisfying (6) [and hence (5)] is easily seen to be $|M^{r-\alpha}| = q^\alpha$. For $z \notin M$, there are $|R| - |M|$ choices for z. The value of x is uniquely determined by (y, z). Therefore the number of blocks $[x : y : z]$ incident with both points is

$$\frac{(|R| - |M|)|M^{r-\alpha}|}{|R| - |M|} = q^\alpha.$$

□

Unfortunately, for $t > 2$, the situation becomes more complicated and we have not been able to obtain a ‘‘nice’’ corresponding formula.

4. APPLICATIONS

In this section, we give applications of the projective spaces over PIRs constructed above to some design-theoretic problems in combinatorics.

A. An Infinite Family of Minimum $(t;1)$-Coverings

The determination of the function $C_\lambda(v,k,t)$ has a rich history and involved many researchers (see bibliography in [8]). Let

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

Schönheim [9] established $L_\lambda(v,k,t)$ as a lower bound for $C_\lambda(v,k,t)$ for all $v > k > t > 0$. In this subsection, we determine the values of $C(\frac{q(q^{t+1}-1)}{q-1}, \frac{q(q^t-1)}{q-1}, t)$ for all positive integers t and prime powers q by showing that the derived incidence structure of $\mathbf{P}^t(\mathbb{F}_q)$ are in fact minimum coverings. Our strategy is to evaluate Schönheim's bound and then show that the number of blocks in these coverings meets the bound. Previously, Todorov [11] had shown that $\mathbf{P}^t(\mathbb{F}_q)$ are minimum $(t;1)$-coverings, but their derived incidence structures seem not to have been studied.

Definition 4.1. *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ be an incidence structure. The derived incidence structure of $\mathcal{S}$ at the point $P \in \mathcal{P}$ is the induced incidence structure $\mathcal{S}_P = (\mathcal{P}_P, \mathcal{B}_P, I_P)$, where $\mathcal{P}_P = \mathcal{P} \setminus \{P\}, \mathcal{B}_P = \{B \in \mathcal{B} | (P,B) \in I\} = (P)$, and $I_P = \{(P', B) | P' \neq P, B \in \mathcal{B}_P$, and $(P', B) \in I\}$.*

Proposition 4.1. *The derived incidence structure of a t-(v,k,λ) covering at any point is a $(t-1)$-$(v-1,k-1,\lambda)$ covering.*

The proof of Proposition 4.1 is omitted. We note that the idea of the proof is the same as in [2, Lemma 1.7(ii)].

Corollary 4.1. *The derived incidence structure of $\mathbf{P}^{t+1}(\mathbb{F}_q)$ at any point is a t-$(\frac{q(q^{t+1}-1)}{q-1}, \frac{q(q^t-1)}{q-1}, 1)$ covering with $\frac{q^{t+1}-1}{q-1}$ blocks.*

Proof. That the derived incidence structure of $\mathbf{P}^{t+1}(\mathbb{F}_q)$ at any point is a t-$(\frac{q(q^{t+1}-1)}{q-1}, \frac{q(q^t-1)}{q-1}, 1)$ covering follows immediately from Proposition 3.1 and Proposition 4.1. The number of blocks in the derived incidence structure of $\mathbf{P}^t(\mathbb{F}_q)$ is obtained from the fact that the number of blocks incident with a point in $\mathbf{P}^{t+1}(\mathbb{F}_q)$ is $\frac{q^{t+1}-1}{q-1}$ (Proposition 3.3). □

Proposition 4.2. *Let $q \geq 2$. Then for any positive integer t and any integer $k, 0 \leq k \leq t-1$, we have*

$$\left\lceil \frac{\sum_{i=0}^{t} q^i - k}{\sum_{i=0}^{t-1} q^i - k} \cdot \sum_{i=0}^{t-k-1} q^i \right\rceil = \sum_{i=0}^{t-k} q^i.$$

Proof. It suffices to show that

$$\sum_{i=1}^{t-k} q^i < \frac{\sum_{i=0}^{t} q^i - k}{\sum_{i=0}^{t-1} q^i - k} \cdot \sum_{i=0}^{t-k-1} q^i \leq \sum_{i=0}^{t-k} q^i.$$

To show that $\sum_{i=1}^{t-k} q^i < \frac{\sum_{i=0}^{t} q^i - k}{\sum_{i=0}^{t-1} q^i - k} \cdot \sum_{i=0}^{t-k-1} q^i$, consider

$$\begin{aligned}
&\left(\sum_{i=0}^{t} q^i - k\right)\left(\sum_{i=0}^{t-k-1} q^i\right) - \left(\sum_{i=0}^{t-1} q^i - k\right)\left(\sum_{i=1}^{t-k} q^i\right) \\
&\quad = \left(\frac{q^{t+1}-1}{q-1} - k\right)\left(\frac{q^{t-k}-1}{q-1}\right) - \left(\frac{q^t-1}{q-1} - k\right)\left(\frac{q^{t-k+1}-1}{q-1} - 1\right) \\
&\quad = \frac{(q^{t+1}-1-k(q-1))(q^{t-k}-1) - (q^t-1-k(q-1))(q^{t-k+1}-1-(q-1))}{(q-1)^2} \\
&\quad = \frac{(q^{t-k}-1)(k(q-1)+1)}{q-1} > 0.
\end{aligned}$$

We now show that $\frac{\sum_{i=0}^{t} q^i - k}{\sum_{i=0}^{t-1} q^i - k} \cdot \sum_{i=0}^{t-k-1} q^i \leq \sum_{i=0}^{t-k} q^i$.

$$\begin{aligned}
&\left(\sum_{i=0}^{t-1} q^i - k\right)\left(\sum_{i=0}^{t-k} q^i\right) - \left(\sum_{i=0}^{t} q^i - k\right)\left(\sum_{i=0}^{t-k-1} q^i\right) \\
&\quad = \left(\frac{q^t-1}{q-1} - k\right)\left(\frac{q^{t-k+1}-1}{q-1}\right) - \left(\frac{q^{t+1}-1}{q-1} - k\right)\left(\frac{q^{t-k}-1}{q-1}\right) \\
&\quad = \frac{(q^t-1-k(q-1))(q^{t-k+1}-1) - (q^{t+1}-1-k(q-1))(q^{t-k}-1)}{(q-1)^2} \\
&\quad = \frac{q^{t-k}}{q-1}(q^k - kq + k - 1).
\end{aligned}$$

It is not hard to show that $q^k - kq + k - 1 \geq 0$ for $k \geq 0$; so the quantity on the right is non-negative. This completes the proof. □

Theorem 4.1. *Let*

$$\mathcal{L}(m) = \left\lceil \frac{\sum_{i=0}^{t} q^i - t + m}{\sum_{i=0}^{t-1} q^i - t + m} \left\lceil \frac{\sum_{i=0}^{t} q^i - t + m - 1}{\sum_{i=0}^{t-1} q^i - t + m - 1} \times \left\lceil \cdots \left\lceil \frac{\sum_{i=0}^{t} q^i - t + 1}{\sum_{i=0}^{t-1} q^i - t + 1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil, \quad (7)$$

where $1 \leq m \leq t$. *Then* $\mathcal{L}(m) = \sum_{i=0}^{m} q^i$.

Proof. For $m = 1$, this result is Proposition 4.2 by letting $k = t - 1$. For general $m \geq 2$, we carry out an induction on m. Observe that

$$\mathcal{L}(m) = \left\lceil \frac{\sum_{i=0}^{t} q^i - t + m}{\sum_{i=0}^{t-1} q^i - t + m} \cdot \mathcal{L}(m-1) \right\rceil.$$

By the induction hypothesis,

$$\mathcal{L}(m) = \left\lceil \frac{\sum_{i=0}^{t} q^i - t + m}{\sum_{i=0}^{t-1} q^i - t + m} \cdot \sum_{i=0}^{m-1} q^i \right\rceil.$$

By Proposition 4.2 (letting $k = t - m$) we have $\mathcal{L}(m) = \sum_{i=0}^{m} q^i$. □

Corollary 4.2. *The derived incidence structure of* $\mathbf{P}^{t+1}(\mathbb{F}_q)$ *at any point is a minimum* t-$(\frac{q(q^{t+1}-1)}{q-1}, \frac{q(q^t-1)}{q-1}, 1)$ *covering. Hence,* $C(\frac{q(q^{t+1}-1)}{q-1}, \frac{q(q^t-1)}{q-1}, t) = \frac{q^{t+1}-1}{q-1}$ *for all* $t > 0$ *and prime powers* q.

Proof. Corollary 4.1 gives

$$C\left(\sum_{i=1}^{t+1} q^i, \sum_{i=1}^{t} q^i, t\right) \leq \sum_{i=0}^{t} q^i,$$

and Schönheim's bound gives

$$C\left(\sum_{i=1}^{t+1} q^i, \sum_{i=1}^{t} q^i, t\right) \geq L_1\left(\sum_{i=1}^{t+1} q^i, \sum_{i=1}^{t} q^i, t\right) = \mathcal{L}(t),$$

where $\mathcal{L}$ is the function defined by (7). But $\mathcal{L}(t) = \sum_{i=0}^{t} q^i$ by Theorem 4.1. □

B. An Infinite Family of Symmetric Minimum (2; 2)-Coverings

In [4], using $\mathbf{P}^2(\mathbb{Z}/4\mathbb{Z})$, the authors determined the functions $C(2, 6, 6^n \cdot 28)$ for all $n \geq 0$ and $C(2, 6, 6^n \cdot 28 - 5)$ for all $n \geq 1$. Here, we construct an infinite family of minimum 2-$(2(q^2+q+1), 2(q+1), 2)$ coverings, for q a prime power, thereby completely determining the values of $C_2(2(q^2 + q + 1), 2(q + 1), 2)$. These minimum coverings are symmetric.

We compute the Schönheim bound $L_\lambda(v, k, t)$ when $v = \lambda(q^2 + q + 1), k = \lambda(q + 1)$ and $t = 2$.

Proposition 4.3. *We have*

$$L_\lambda(\lambda(q^2 + q + 1), \lambda(q + 1), 2) = \lambda(q^2 + q + 1) - q(\lambda - 2)$$

if $\lambda - 2 \leq q$ *and* $\lambda \geq 2$.

Proof.

$$\begin{aligned} L_\lambda(\lambda(q^2 + q + 1), \lambda(q + 1), 2) &= \left\lceil \frac{\lambda(q^2 + q + 1)}{\lambda(q + 1)} \left\lceil \frac{(\lambda(q^2 + q + 1) - 1)\lambda}{\lambda(q + 1) - 1} \right\rceil \right\rceil \\ &= \left\lceil \frac{q^2 + q + 1}{q + 1} \left\lceil \lambda q + 1 + \frac{(\lambda - 1)^2}{\lambda q + (\lambda - 1)} \right\rceil \right\rceil \end{aligned}$$

$$
\begin{aligned}
&= \left\lceil \frac{q^2+q+1}{q+1}(\lambda q+2) \right\rceil \text{ (since } (\lambda-1)(\lambda-2) \le \lambda q) \\
&= \left\lceil \lambda(q^2+q+1) - q(\lambda-2) - \frac{\lambda-2}{q+1} \right\rceil \\
&= \lambda(q^2+q+1) - q(\lambda-2).
\end{aligned}
$$

□

Corollary 4.3. *$\mathbf{P}_2^2(\mathbb{F}_q)$ is a symmetric minimum 2-$(2(q^2+q+1), 2(q+1), 2)$ covering. Hence, $C_2(2(q^2+q+1), 2(q+1), 2) = 2(q^2+q+1)$ for all prime powers q.*

Proof. When $\lambda = 2$, $L_2(2(q^2+q+1), 2(q+1), 2) = 2(q^2+q+1)$. From Proposition 3.2, $\mathbf{P}_2^2(\mathbb{F}_q)$ gives the appropriate covering realizing the number of blocks. □

Remark. Starting from the Steiner system of a projective geometry giving $C(q^2+q+1, q+1, 2) = q^2+q+1$, we obtain from the blowup construction the bound $C_\lambda(2(q^2+q+1), 2(q+1), 2) \le \lambda(q^2+q+1)$. By computing the Schönheim bound as above, we show that this last inequality is in fact an equality for $\lambda = 2$ (and so for $\lambda = 1$).

C. Imbrical Designs

From Proposition 4.3, we see easily that the number of blocks in the $(2;\lambda)$-covering $\mathbf{P}_\lambda^2(\mathbb{F}_q)$ is $q(\lambda-2)$ more than the lower bound of Schönheim. It is therefore natural to ask whether in the case of $\lambda > 2$, one can delete blocks from $\mathbf{P}_\lambda^2(\mathbb{F}_q)$ and still end up with a $(2;\lambda)$-covering. The results in this section show that this is not possible.

Definition 4.2. *A $(t;\lambda)$-imbrical design, or more specifically a t-(v,k,λ) imbrical design, is a t-(v,k,λ) covering $(\mathcal{P},\mathcal{B},I)$ such that for any $B \in \mathcal{B}$, there exists a set of t distinct points incident with B that is also incident with exactly λ blocks (including B).*

In an imbrical design, every block is essential; deleting a block results in an incidence structure in which some set of t distinct points is incident with fewer than λ blocks. It is obvious that minimum t-(v,k,λ) coverings are all t-(v,k,λ) imbrical designs. However, the converse is not necessarily true. The 2-(v,k,λ) imbrical designs were introduced by Mendelsohn and Assaf [7]. In [4], the authors showed that $\mathbf{P}^2(\mathbb{Z}/n\mathbb{Z})$ are 2-$(v,k,1)$ imbrical designs. Here, we show that $\mathbf{P}_\lambda^t(R)$ are t-(v,k,λ) imbrical designs when R is a finite PIR.

Theorem 4.2. *If $\mathcal{S}$ is a t-(v,k,a) imbrical design, then the λ-blowup of $\mathcal{S}$, denoted $\mathcal{S}'$ is a t-$(\lambda v, \lambda k, \lambda a)$ imbrical design.*

Proof. Given a block B in $\mathcal{S}'$, to show the existence of a set of t distinct points $\mathcal{Q} = \{P_1,\ldots,P_t\}$ incident with B such that there are exactly λa blocks incident with $\mathcal{Q}$, it suffices to show that $\{\vartheta_\lambda(P_1),\ldots,\vartheta_\lambda(P_t)\}$ [incident with the block $\vartheta_\lambda(B)$] have exactly a blocks incident with it. Since $\mathcal{S}$ is a t-(v,k,a) imbrical design, the existence of such a set of points is guaranteed. □

Theorem 4.3. *If R is a finite PIR, then $\mathbf{P}^t(R)$ is a $(t;1)$-imbrical design for every $t \ge 2$.*

Proof. Given a block B, where $B = [x_0 : \cdots : x_t]$ in $\mathbf{P}^t(R)$, it suffices to find a set of t distinct points $\{P_1, \ldots, P_t\}$ in $\mathbf{P}^t(R)$ such that B is the unique block incident with it.

First, we prove this fact in the case R is a finite special PIR (cf. [6, Theorem 2.6]).

Without loss of generality, we may assume that $x_0 \in R^\times$ and hence assume that the block B is of the form $[1 : x_1 : \cdots : x_t]$. The following set of t points in $\mathbf{P}^t(R)$,

$$\mathcal{Q} = \{(-x_1 : 1 : 0 : \cdots : 0), (-x_2 : 0 : 1 : 0 : \cdots : 0), \ldots, (-x_t : 0 : \cdots : 0 : 1)\},$$

is incident with B. Furthermore, any block incident with $\mathcal{Q}$ is of the form $[a : ax_1 : \cdots : ax_t]$, for some $a \in R$. In particular, we have $a \in R^\times$ and $[a : ax_1 : \cdots : ax_t] = [1 : x_1 : \cdots : x_t] = B$ is the unique block incident with $\mathcal{Q}$.

When $R = R_1 \times \cdots R_s$, where R_i are finite special PIRs, the block B may be regarded as $(B_1, \ldots, B_s)$ in $\times_{i=1}^s \mathbf{P}^t(R_i)$. From the above, for each B_i, we can find a set of t points $\{P_{i1}, \ldots, P_{it}\}$ in $\mathbf{P}^t(R_i)$ such that B_i is the unique block in $\mathbf{P}^t(R_i)$ incident with it. For each j between 1 and t, set $P_j = (P_{1j}, \ldots, P_{sj})$. By Theorem 3.1, B is the unique block in $\mathbf{P}^t(R)$ incident with $\{P_1, \ldots, P_t\}$. Therefore $\mathbf{P}^t(R)$ is an imbrical design for every $t \geq 2$. □

Combining Theorems 4.2 and 4.3, we obtain:

Corollary 4.4. *For every integer $t \geq 2$, if R is a finite PIR, then $\mathbf{P}^t_\lambda(R)$ is a $(t; \lambda)$-imbrical design.*

D. Regular Covering Designs

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ be a 2-(v, k, λ) covering design. An undirected multigraph $G = (V, E)$ is an *excess of* $\mathcal{S}$ if $V = \mathcal{P}$, and the edge $\{P_1, P_2\}$ appears precisely s times in G whenever $|\{B \in \mathcal{B} : (P_1, B) \in I, (P_2, B) \in I\}| = \lambda + s$. If the excess of $\mathcal{S}$ is regular of degree Δ, then $\mathcal{S}$ is called a *regular* 2-(v, k, λ) covering and Δ is called the degree of $\mathcal{S}$ as a 2-(v, k, λ) covering. (Note that if $\mathcal{S}$ is a 2-(v, k, λ) covering with an excess that is regular of degree Δ, then $\mathcal{S}$ is also a 2-$(v, k, \lambda - \epsilon)$ covering with an excess that is regular of degree $\Delta + (v - 1)\epsilon$. Therefore the degree is only well-defined relative to λ.) For a fixed λ, if Δ is as small as possible, then $\mathcal{S}$ is called a *degree-minimum* regular 2-(v, k, λ) covering. When $\Delta = 0$, $\mathcal{S}$ is a BIBD. Degree-minimum regular coverings were first studied by Bermond, Bond, and Sotteau [1]. These incidence structures have applications in the design of bus interconnections for computer networks. In [4], it was shown that $\mathbf{P}^2(\mathbb{Z}/4\mathbb{Z})$ is a degree-minimum regular 2-$(v, k, 1)$ covering and based on this, an infinite family of degree-minimum regular 2-$(v, k, 1)$ coverings was constructed. Here, we show that there is no peculiarity with the ring $\mathbb{Z}/4\mathbb{Z}$; more general results hold.

Theorem 4.4. *If $\mathcal{S}$ is a regular 2-(v, k, a) covering, then the λ-blowup of $\mathcal{S}$, denoted $\mathcal{S}'$, is a regular 2-$(\lambda v, \lambda k, \lambda a)$ covering.*

Proof. Let P be a point of $\mathcal{S}'$.

For a point $P' \neq P$ in the same fiber as P (under ϑ_λ), the number of blocks incident with $\{P, P'\}$ is λ times the number of blocks incident with $\vartheta_\lambda(P)$, i.e., λk. The number of P' in the same fiber as P (and $P' \neq P$) is $\lambda - 1$.

For a point $Q \neq \vartheta_\lambda(P)$ in $\mathcal{S}$, let k_Q be the number of blocks incident with $\{\vartheta_\lambda(P), Q\}$. Since $\mathcal{S}$ is regular, the number $\sum_{Q \neq \vartheta_\lambda(P)}(k_Q - a)$ is constant. In fact, this sum is the degree of the excess of $\mathcal{D}$ as a 2-(v, k, a) covering. Let it be denoted by Δ.

If P' is not in the same fiber as P, then $\vartheta_\lambda(P') \neq \vartheta_\lambda(P)$. The number of blocks incident with $\{P, P'\}$ is $\lambda k_{\vartheta_\lambda(P')}$. Moreover, for each $Q \neq \vartheta_\lambda(P)$ in $\mathcal{S}$, there exist exactly λ points P' in $\mathcal{S}'$ such that $\vartheta_\lambda(P') = Q$.

It follows then that, in the excess G of $\mathcal{S}'$ as a 2-$(v, k, \lambda a)$ covering, the degree of the vertex P is given by

$$\begin{aligned}
&\sum_{P' \neq P : \vartheta_\lambda(P) = \vartheta_\lambda(P')} (\lambda k - \lambda a) + \sum_{P' : \vartheta_\lambda(P) \neq \vartheta_\lambda(P')} (\lambda k_{\vartheta_\lambda(P')} - \lambda a) \\
&\quad = \lambda(\lambda - 1)(k - a) + \lambda \sum_{Q \neq \vartheta_\lambda(P)} \lambda(k_Q - a) \\
&\quad = \lambda(\lambda - 1)(k - 1) + \lambda^2 \Delta.
\end{aligned}$$

Since this degree is independent of the vertex chosen, every vertex of G has the same degree $\lambda(\lambda - 1)(k - a) + \lambda^2\Delta$, and G is hence regular. □

Theorem 4.5. *Let R be a finite PIR. Then the excess of $\mathbf{P}^2(R)$ (as a (2; 1)-covering) is regular of degree*

$$\begin{aligned}
&\left(\prod_i q_i^{r_i - 1}(q_i + 1)\right)\left(\prod_i q_i^{r_i - 1}(q_i + 1) - 1\right) \\
&\qquad - \left(\prod_i q_i^{2(r_i - 1)}(q_i^2 + q_i + 1)\right) + 1 = k(k - 1) - v + 1, \quad (8)
\end{aligned}$$

where v is the number of points in $\mathbf{P}^2(R)$ and k is the cardinality of block traces in $\mathbf{P}^2(R)$. Consequently, $\mathbf{P}^2_\lambda(R)$ is a regular 2-(v, k, λ) covering of degree $\lambda(\lambda-1)(k-1)+\lambda^2(k(k-1) - v + 1)$.

Proof. The second statement follows immediately from the first by applying Theorem 4.4. We now prove the first statement.

Let $P = (a : b : c)$ be a given point $\mathbf{P}^2(R)$. For every $i = 1, 2, \ldots, s$, consider the projection

$$\begin{aligned}
\Psi_i : \mathbf{P}^2(R) &\to \mathbf{P}^2(R_i), \\
(a : b : c) &\mapsto (a_i : b_i : c_i).
\end{aligned}$$

It has been shown that the map Ψ_i is well defined (see proof of Theorem 3.1).

For a point $P' = (d : e : f)$ of $\mathbf{P}^2(R)$, suppose we have

$$\langle a_i e_i - b_i d_i, a_i f_i - c_i d_i, b_i f_i - c_i e_i \rangle = M_i^{\alpha_i}, \quad \alpha_i \leq r_i. \quad (9)$$

If $\alpha_i = r_i$, then it is clear from (9) that $\Psi_i(P) = \Psi_i(P')$. Hence, there exists a unit μ_i of R_i such that

$$\begin{aligned}
d_i &\equiv \mu_i a_i (\text{mod } M_i^{r_i}), \\
e_i &\equiv \mu_i b_i (\text{mod } M_i^{r_i}), \\
f_i &\equiv \mu_i c_i (\text{mod } M_i^{r_i}).
\end{aligned}$$

If $\alpha_i < r_i$, then by considering $\Psi_i(P)$ and $\Psi_i(P')$, and assuming without loss of generality that a_i is a unit in R_i, we obtain the congruences

$$\begin{aligned} a_i e_i &\equiv b_i d_i (\text{mod } M_i^{\alpha_i}), \\ a_i f_i &\equiv c_i d_i (\text{mod } M_i^{\alpha_i}), \end{aligned} \tag{10}$$

and at least one of the congruences in (10) fails when α_i is replaced by $\alpha_i + 1$.

Now we count the number of triples (d, e, f) such that d, e, f generate R and (9) is satisfied for each $i = 1, \ldots, s$ [that is, those (d, e, f) which will define a point in $\mathbf{P}^2(R)$]. We do so by counting the number of such triples "locally" at each i.

For $\alpha_i = 0$, the number of such triples in $R_i \times R_i \times R_i$ is

$$(q_i^{3r_i} - q_i^{3(r_i-1)}) - (q_i^{r_i} - q_i^{r_i-1}) q_i^{2(r_i-1)} = (q_i^{r_i} - q_i^{r_i-1}) q_i^{2(r_i-1)} q_i (q_i + 1).$$

For $0 < \alpha_i < r_i$, the number is

$$(q_i^{r_i} - q_i^{r_i-1}) q_i^{2(r_i-\alpha_i)} - (q_i^{r_i} - q_i^{r_i-1}) q_i^{2(r_i-\alpha_i-1)} = (q_i^{r_i} - q_i^{r_i-1}) q_i^{2(r_i-\alpha_i-1)} (q_i^2 - 1).$$

For $\alpha_i = r_i$, this number is $(q_i^{r_i} - q_i^{r_i-1})$.

Therefore, for $P = (a : b : c)$, the number of points $P' = (d : e : f)$ such that (9) is true for each $i = 1, \ldots, s$, is given by

$$\begin{aligned} &\prod_{i:\alpha_i = r_i} (q_i^{r_i} - q_i^{r_i-1}) \prod_{i:\alpha_i = 0} (q_i^{r_i} - q_i^{r_i-1}) q_i^{2(r_i-1)} q_i (q_i + 1) \\ &\qquad \times \prod_{i:0<\alpha_i<r_i} (q_i^{r_i} - q_i^{r_i-1}) q_i^{2(r_i-\alpha_i-1)} (q_i^2 - 1) \Big/ \prod_i (q_i^{r_i} - q_i^{r_i-1}) \\ &= \prod_{i:\alpha_i = 0} q_i^{2(r_i-1)} q_i (q_i + 1) \prod_{i:0<\alpha_i<r_i} q_i^{2(r_i-\alpha_i-1)} (q_i^2 - 1) \\ &= \prod_{i:\alpha_i<r_i} (q_i + 1) q_i^{2(r_i-\alpha_i-1)} \prod_{i:\alpha_i=0} q_i \prod_{i:0<\alpha_i<r_i} (q_i - 1). \end{aligned}$$

(The product is interpreted as 1 when $\alpha_i = r_i$ for all i. This means that $\langle a_i e_i - b_i d_i, a_i f_i - c_i d_i, b_i f_i - c_i e_i \rangle = 0$ for all i if and only if $P' = P$.) For such points P', the number of blocks incident on $\{P, P'\}$ is (cf. Theorem 3.2)

$$\prod_{i:\alpha_i<r_i} q_i^{\alpha_i} \prod_{i:\alpha_i=r_i} q_i^{r_i-1} (q_i + 1).$$

Therefore, in the excess G of $\mathbf{P}^2(R)$, the degree of the vertex P is given by (writing $D = \{\prod_i q_i^{\alpha_i} | 0 \le \alpha_i \le r_i \text{ for all } i\}$ and $n = \prod_i q_i^{r_i}$)

$$\begin{aligned} &\sum_{d \in D : d \ne n} \left(\prod_{i:\alpha_i<r_i} (q_i + 1) q_i^{2(r_i-\alpha_i-1)} \prod_{i:\alpha_i=0} q_i \prod_{i:0<\alpha_i<r_i} (q_i - 1) \right) \\ &\qquad \times \left(\prod_{i:\alpha_i<r_i} q_i^{\alpha_i} \prod_{i:\alpha_i=r_i} q_i^{r_i-1} (q_i + 1) - 1 \right) \\ &= \left(\prod_i q_i^{r_i-1} (q_i + 1) \right) \sum_{d \in D : d \ne n} f_n(d) - \sum_{d \in D : d \ne n} g_n(d), \end{aligned} \tag{11}$$

where, for $d = \prod_i q_i^{\alpha_i} \in D$,

$$f_n(d) = \prod_{i:\alpha_i<r_i} q_i^{r_i-\alpha_i-1} \prod_{i:\alpha_i=0} q_i \prod_{i:0<\alpha_i<r_i} (q_i - 1),$$

$$g_n(d) = \prod_{i:\alpha_i<r_i} q_i^{2(r_i-1)-2\alpha_i}(q_i + 1) \prod_{i:\alpha_i=0} q_i \prod_{i:0<\alpha_i<r_i} (q_i - 1).$$

Note that empty products in the definition of $f_n(d)$ and $g_n(d)$ are taken to be 1.

For a fixed n, the functions $f_n(d)$ and $g_n(d)$ can be regarded as multiplicative functions of $d \in D$, so

$$\sum_{d\in D} f_n(d) = \prod_i \left(\sum_{j=0}^{r_i} f_n(q_i^j) \right)$$

and

$$\sum_{d\in D} g_n(d) = \prod_i \left(\sum_{j=0}^{r_i} g_n(q_i^j) \right).$$

It follows then that

$$\sum_{d\in D:d\neq n} f_n(d) = \prod_i q_i^{r_i-1}(q_i + 1) - 1. \tag{12}$$

and

$$\sum_{d\in D:\neq n} g_n(d) = \prod_i q_i^{2(r_i-1)}(q_i^2 + q_i + 1) - 1. \tag{13}$$

The degree of the vertex P is then obtained by substituting (12) and (13) in (11). Since the degree is independent of the vertex chosen, G is regular of the degree stated in (8). □

Proposition 4.4. *If a* 2-(v, k, λ) *covering has an excess that is regular of degree* Δ, *then* v, k, λ, *and* Δ *must satisfy the following congruences*:

$$\lambda(v - 1) + \Delta \equiv 0 \pmod{k - 1},$$

$$v(\lambda(v - 1) + \Delta) \equiv 0 \pmod{k(k - 1)}.$$

Proof. To prove the first congruence, let P be any fixed point of a regular 2-(v, k, λ) covering $\mathcal{S}$, and count in two ways the number of pairs of points, exactly one of which is P, that are contained in the blocks of $\mathcal{S}$.

To prove the second congruence, count in two ways the total number of pairs of distinct points that are contained in the blocks of $\mathcal{S}$. □

Proposition 4.5. *The smallest non-negative integer* Δ *that satisfies*

$$v - 1 + \Delta \equiv 0 \pmod{k - 1},$$

$$v(v - 1 + \Delta) \equiv 0 \pmod{k(k - 1)}, \tag{14}$$

where $v = q^2(q^2 + q + 1)$ (q *prime power*) *and* $k = q(q + 1)$, *is* $(q - 1)(q^2 - 1)$.

Proof. For $\Delta = (q-1)(q^2-1)$, we have

$$\begin{aligned} v - 1 + \Delta &= q^4 + q^3 + q^2 - 1 + (q^3 - q^2 - q + 1) \\ &= q^4 + 2q^3 - q \\ &= (q(q+1) - 1)(q^2 + q) \\ &\equiv 0 \pmod{k(k-1)}. \end{aligned}$$

So $\Delta = (q-1)(q^2-1)$ satisfies the congruences (14).

Any Δ that satisfies the congruences (14) must satisfy

$$\Delta \equiv -q^2(q^2+q+1) + 1 \equiv 2q - 1 \pmod{q^2+q-1}$$

and

$$q^2(q^2+q+1)(q^2(q^2+q+1) - 1 + \Delta) \equiv 0 \pmod{q(q+1)},$$

that is,

$$q(q^2+q+1)(q^2(q^2+q+1) - 1 + \Delta) \equiv 0 \pmod{q+1},$$

that is,

$$\Delta \equiv 0 \pmod{q+1}.$$

Since $q^2 + q - 1 > (q-1)^2$, it follows that

$$(q+1)(q^2+q-1) > (q-1)(q^2-1),$$

implying that $(q-1)(q^2-1)$ is the smallest non-negative integer Δ that satisfies the congruences (14). □

Corollary 4.5. *If R is a finite special PIR such that $M^2 = 0, M \neq 0$, then $\mathbf{P}^2(R)$ is a degree-minimum regular 2-$(q^2(q^2+q+1), q(q+1), 1)$ covering.*

Proof. This follows immediately from Theorem 4.5 and Propositions 4.4, 4.5. □

Corollary 4.6. *For every prime power q, there is a degree-minimum regular 2-$(q^2(q^2+q+1), q(q+1), 1)$ covering.*

Proof. This follows immediately from Corollary 4.5 and the remark in Sec. 2 B. □

Proposition 4.6. $\mathbf{P}^2(\mathbb{Z}/8\mathbb{Z})$ *is a degree-minimum regular* 2-(112, 12, 1) *covering. Its degree is* 21.

Proof. Mimic the proof for Proposition 4.5. □

For a finite special PIR R with $M^r = 0, M^{r-1} \neq 0$ and $R/M \simeq \mathbb{F}_q$, when $r \geq 3$, except for the case $q = 2$ and $r = 3$, the degree of $\mathbf{P}^2(R)$ is greater than $(q+1)(q^{r-1}(q+1)-1)$, and so the argument in Proposition 4.5 fails to show that these are degree-minimum regular coverings. It would be interesting to know if they still yield degree-minimum regular coverings.

Corollary 4.7. $\mathbf{P}^2_2(\mathbb{Z}/4\mathbb{Z})$ *is a degree-minimum regular* 2-(56, 12, 2) *covering of degree* 22. $\mathbf{P}^2_2(\mathbb{Z}/9\mathbb{Z})$ *is a degree-minimum regular* 2-(234, 24, 2) *covering of degree* 86.

Proof. Mimic the proof for Proposition 4.5. □

Now let us investigate the case when $R = \mathbb{F}_q$.

Proposition 4.7. *$\mathbf{P}^2_\lambda(\mathbb{F}_q)$ is a regular 2-$(\lambda(q^2+q+1), \lambda(q+1), \lambda)$ covering. Moreover, the excess of $\mathbf{P}^2_\lambda(\mathbb{F}_q)$ is regular of degree $\lambda(\lambda-1)q$.*

Proof. Follows immediately from Theorems 4.5 and 4.4. □

Proposition 4.8. *If $\mathcal{S}$ is a minimum $(2;\lambda)$-covering that is regular, then $\mathcal{S}$ is a degree-minimum regular $(2;\lambda)$-covering.*

Proof. Follows easily from the observation that fewer lines in the covering results in fewer edges in the corresponding excess. □

Corollary 4.8. *$\mathbf{P}^2_2(\mathbb{F}_q)$ is a degree-minimum regular 2-$(2(q^2+q+1), 2(q+1), 2)$ covering.*

Proof. Corollary 4.3, Propositions 4.7, and 4.8 yield the result. □

We now show that even though we cannot conclude from Propositions 4.7 and 4.8 that $\mathbf{P}^2_\lambda(\mathbb{F}_q)$ is a degree-minimum regular covering for $\lambda \neq 2$ (because in this case $\mathbf{P}^2_\lambda(\mathbb{F}_q)$ is not known to be a minimum covering), it is nevertheless a degree-minimum regular covering for any $\lambda \leq q+3$.

Proposition 4.9. *The smallest non-negative integer Δ that satisfies*

$$\lambda(v-1)+\Delta \equiv 0 \pmod{k-1},$$

$$v(\lambda(v-1)+\Delta) \equiv 0 \pmod{k(k-1)},$$

where $v = \lambda(q^2+q+1), k = \lambda(q+1)$, and $\lambda \leq q+3$, is $\lambda(\lambda-1)q$.

Proof. First we check that $\Delta = \lambda(\lambda-1)q$ satisfies both the given congruences. This follows from

$$\begin{aligned} \lambda(\lambda(q^2+q+1)-1)+\lambda(\lambda-1)q &= \lambda^2q^2+2\lambda^2q+\lambda^2-\lambda-\lambda q \\ &= (\lambda q+\lambda-1)\lambda(q+1) \\ &\equiv 0 \pmod{k(k-1)}. \end{aligned}$$

Now we prove that this above value for Δ is indeed the least non-negative value of Δ that satisfies the congruences.

Any Δ that satisfies the given congruences must satisfy

$$\Delta - \lambda(\lambda-1)q \equiv 0 \pmod{k-1}, \tag{15}$$

and

$$v(\Delta-\lambda(\lambda-1)q) \equiv 0 \pmod{k(k-1)}. \tag{16}$$

Note that (16) is true if and only if

$$\lambda(q^2+q+1)(\Delta-\lambda(\lambda-1)q) \equiv 0 \pmod{\lambda(q+1)(\lambda q+\lambda-1)},$$

which is equivalent to

$$(q^2+q+1)(\Delta-\lambda(\lambda-1)q) \equiv 0 \pmod{(q+1)(\lambda q+\lambda-1)}. \tag{17}$$

Congruence (17) implies

$$(q^2+q+1)(\Delta-\lambda(\lambda-1)q) \equiv 0 \pmod{q+1}. \tag{18}$$

Since it is clear that $q+1$ and $q^2+q+1 = q(q+1)+1$ are relatively prime, we have from (18)

$$\Delta \equiv \lambda(\lambda-1)q \pmod{q+1}. \tag{19}$$

From (15), we get

$$\Delta \equiv \lambda(\lambda-1)q \pmod{\lambda q+\lambda-1}. \tag{20}$$

Since $q+1$ and $\lambda q+\lambda-1 = \lambda(q+1)-1$ are relatively prime, the Chinese Remainder Theorem implies that

$$\Delta \equiv \lambda(\lambda-1)q \pmod{(q+1)(\lambda q+\lambda-1)}. \tag{21}$$

When $\lambda = 1, \lambda(\lambda-1)q = 0$ is clearly the smallest non-negative Δ that satisfies the congruences given in the statement of the proposition.

When $q-1 \geq \lambda \geq 2$, then $q \geq 3$, so $q^2-q > q+1$. This implies

$$\begin{aligned} \lambda(\lambda-1)q &\leq (\lambda-1)q(q-1) \\ &= \lambda q(q-1)-(q^2-q) \\ &< \lambda(q+1)^2-(q+1) \\ &= (q+1)(\lambda q+\lambda-1). \end{aligned} \tag{22}$$

When $q \leq \lambda \leq q+3$, it is straightforward to verify case by case that

$$\lambda(\lambda-1)q \leq (q+1)(\lambda q+\lambda-1). \tag{23}$$

Together with (21), the inequalities (22) and (23) show that $\lambda(\lambda-1)q$ is the smallest non-negative value of Δ that satisfies the congruences given in the statement of the proposition. □

Remark. For $\lambda \geq q+4$, an easy argument shows that $\lambda(\lambda-1)q > (q+1)(\lambda q+\lambda-1)$.

Corollary 4.9. *$\mathbf{P}^2_\lambda(\mathbb{F}_q)$ is a degree-minimum regular 2-$(\lambda(q^2+q+1), \lambda(q+1), \lambda)$ covering for all $\lambda \leq q+3$.*

Proof. Follows immediately from Propositions 4.7, 4.4, and 4.9. □

The method used here does not yield any conclusive result for $\lambda \geq q+4$. It would be interesting to determine if the condition $\lambda \leq q+3$ can be removed in Corollary 4.9.

We now discuss the case when R is a finite PIR (i.e., not necessarily special).

Proposition 4.10. *Let $R = R_1 \times \cdots \times R_s$ be a finite PIR, so $\mathbf{P}^2(R)$ is a 2-$(v,k,1)$ covering, and let $l = \gcd(k,v)$. If*

$$l < \frac{k(k-1)}{k(k-1)-v+1}, \tag{24}$$

then $\mathbf{P}^2(R)$ is a degree-minimum regular 2-$(v,k,1)$ covering.

Proof. From Theorem 4.5, the degree of the excess of the regular 2-(v,k,λ) covering $\mathbf{P}^2(R)$ is $\Delta = k(k-1)-v+1$. It is quite clear from the congruences (14) that the degree

of the excess of a regular 2-$(v, k, 1)$ covering is unique modulo $k(k-1)/l$. Therefore, if (24) is true, then $l < k(k-1)/\Delta$, implying $0 \leq \Delta < k(k-1)/l$, which means $\mathbf{P}^2(R)$ is degree-minimum. □

Corollary 4.10. *If $R = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$ (s times), then $\mathbf{P}^2(R)$ is a degree-minimum regular 2-$(v, k, 1)$ covering, where $v = (q^2+q+1)^s$ and $k = (q+1)^s$.*

Proof. This follows from Proposition 4.10 since $l = \gcd(k, v) = 1$ in this case. □

Corollary 4.11. *Let q_1 be a fixed prime power. Let $q_2 > q_1^2 + q_1$ be another prime power such that $\gcd(q_1^2+q_1+1, q_2+1) = 1$. Then for $R = \mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, \mathbf{P}^2(R)$ is a degree-minimum regular 2-$(v, k, 1)$ covering, with $v = (q_1^2+q_1+1)(q_2^2+q_2+1)$ and $k = (q_1+1)(q_2+1)$.*

Proof. Since $\gcd(q_1^2+q_1+1, q_2+1) = 1$, we have that $l = \gcd(q_2^2+q_2+1, q_1+1) \leq q_1+1$. If $q_2 > q_1^2+q_1$, then $q_1q_2 + q_1^2 + 2q_1 \leq q_1q_2 + q_1 + q_2$. Therefore, $q_1(q_1+q_2+2) \leq (q_1q_2+q_1+q_2)$. So,

$$l \leq q_1 + 1 < \frac{(q_1+1)(q_2+1)(q_1q_2+q_1+q_2)}{q_1q_2(q_1+q_2+2)} = \frac{k(k-1)}{k(k-1)-v+1}.$$

We then complete the proof by invoking Proposition 4.10. □

Corollary 4.12. *For a fixed prime power q_1, there exist infinitely many prime powers q_2 such that $\mathbf{P}^2(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2})$ is a degree-minimum regular 2-$(v, k, 1)$ covering, where $v = (q_1^2+q_1+1)(q_2^2+q_2+1)$ and $k = (q_1+1)(q_2+1)$.*

Proof. Dirichlet's Theorem on the distribution of primes in an arithmetic progression guarantees that there are infinitely many primes, and hence prime powers q_2, satisfying the conditions of Corollary 4.11. □

Lemma 4.1. *If $q_2 > q_1$ are prime powers, and*

$$l \leq \frac{q_1+1}{q_1} \cdot \frac{q_2+1}{q_2} \cdot \frac{q_1+1}{2},$$

then $\mathbf{P}^2(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2})$ is a degree-minimum regular 2-$(v, k, 1)$ covering with $v = (q_1^2+q_1+1)(q_2^2+q_2+1)$ and $k = (q_1+1)(q_2+1)$.

Proof. From $q_2 > q_1$, we have $q_2 \geq q_1 + 1$, so $q_1 + q_2 + 1 \leq 2q_2$, that is, $q_1 + q_2 + 2 \leq 2q_2 + 1$. Therefore,

$$\begin{aligned} l &\leq \frac{q_1+1}{q_1} \cdot \frac{q_2+1}{q_2} \cdot \frac{q_1+1}{2} \\ &= \frac{q_1+1}{q_1} \cdot \frac{q_2+1}{q_2} \cdot \frac{(q_1+1)\left(q_2+\frac{1}{2}\right)}{2\left(q_2+\frac{1}{2}\right)} \\ &< \frac{q_1+1}{q_1} \cdot \frac{q_2+1}{q_2} \cdot \frac{q_1q_2+q_1+q_2}{q_1+q_2+2} \\ &= \frac{k(k-1)}{k(k-1)-v+1}. \end{aligned}$$

□

Example 4.1. *For any prime power $q \geq 2$ such that $q \not\equiv -1 \bmod 7$, $\mathbf{P}^2(\mathbb{F}_2 \times \mathbb{F}_q)$ is a degree-minimum regular 2-$(7(q^2+q+1), 3(q+1), 1)$ covering.*

Proof. This is assured for $q > 6$ such that $\gcd(q+1, 7) = 1$ (Corollary 4.11 of Proposition 4.10). For $q = 2, 3, 4, 5$, it is easy to check that (24) is satisfied. □

Example 4.2. *For any prime power $q \geq 3$ such that $q \not\equiv -1 \bmod 13$, $\mathbf{P}^2(\mathbb{F}_3 \times \mathbb{F}_q)$ is a degree-minimum regular 2-$(13(q^2+q+1), 4(q+1), 1)$ covering.*

Proof. Whenever $\gcd(q+1, 13) = 1$, it is easy to see that $l = \gcd(4(q+1), 13(q^2+q+1)) = 1$, so (24) is satisfied. □

Example 4.3. *For any prime power $q \geq 5$ such that $q \not\equiv -1 \bmod 31$, $\mathbf{P}^2(\mathbb{F}_5 \times \mathbb{F}_q)$ is a degree-minimum regular 2-$(31(q^2+q+1), 6(q+1), 1)$ covering.*

Proof. For $q > 5$ such that $q \not\equiv -1 \bmod 31$, we have $l = \gcd(6(q+1), 31(q^2+q+1)) = \gcd(6, q^2+q+1) = 1$ or 3. In any case, the condition in Lemma 4.1 is satisfied, so $\mathbf{P}^2(\mathbb{F}_5 \times \mathbb{F}_q)$ is a degree-minimum covering. For $q = 5$, it is just a special case of Corollary 4.10 of Proposition 4.10. □

Example 4.4. *For any prime power $q \geq 7$ such that $q \not\equiv -1 \bmod 19$, $\mathbf{P}^2(\mathbb{F}_7 \times \mathbb{F}_q)$ is a degree-minimum regular 2-$(57(q^2+q+1), 8(q+1), 1)$ covering.*

Proof. For $q > 7$ such that $q \not\equiv -1 \bmod 19$, we have $l = \gcd(8(q+1), 57(q^2+q+1)) = \gcd(q+1, 57) = 1$ or 3. In either case, the condition in Lemma 4.1 is satisfied, so $\mathbf{P}^2(\mathbb{F}_7 \times \mathbb{F}_q)$ is a degree-minimum covering. For $q = 7$, this is again a special case of Corollary 4.10 of Proposition 4.10. □

Example 4.5. *For any prime power $q \geq 4$ such that $q \not\equiv -1 \bmod 7$, $\mathbf{P}^2(\mathbb{F}_4 \times \mathbb{F}_q)$ is a degree-minimum regular 2-$(21(q^2+q+1), 5(q+1), 1)$ covering.*

Proof. For $q > 4$ such that $q \not\equiv -1 \bmod 7$, we have $l = \gcd(5(q+1), 21(q^2+q+1)) = \gcd(q+1, 21) = 1$ or 3. In either case, the condition in Lemma 4.1 is satisfied (since $\frac{4+1}{4} \cdot \frac{4+1}{2} > 3$), so $\mathbf{P}^2(\mathbb{F}_4 \times \mathbb{F}_q)$ is a degree-minimum covering. For $q = 4$, this is just a special case of Corollary 4.10 of Proposition 4.10. □

Example 4.6. *For any prime power $q \geq 9$ such that $\gcd(q+1, 91) = 1$, $\mathbf{P}^2(\mathbb{F}_9 \times \mathbb{F}_q)$ is a degree-minimum regular 2-$(91(q^2+q+1), 10(q+1), 1)$ covering.*

Proof. Since $l = \gcd(10(q+1), 91(q^2+q+1)) = \gcd(q+1, 91) = 1$, (24) is satisfied. □

Example 4.7. *For any prime power $q \geq 8$ such that $q \not\equiv -1 \bmod 73$, $\mathbf{P}^2(\mathbb{F}_8 \times \mathbb{F}_q)$ is a degree-minimum regular 2-$(73(q^2+q+1), 9(q+1), 1)$ covering.*

Proof. For $q > 8$ such that $q \not\equiv -1 \bmod 73$, $l = \gcd(9(q+1), 73(q^2+q+1)) = \gcd(9, q^2+q+1) = 1$ or 3, so the condition in Lemma 4.1 is satisfied (since $\frac{8+1}{8} \cdot \frac{8+1}{2} > 3$). Therefore, $\mathbf{P}^2(\mathbb{F}_8 \times \mathbb{F}_q)$ is a degree-minimum covering. For $q = 8$, this follows from Corollary 4.10 of Proposition 4.10. □

Further families of regular coverings can be constructed using combinatorial structures called *orthogonal arrays*.

Definition 4.3. *Let S be a set of cardinality v. A (v, k, λ)* orthogonal array, *denoted OA(v, k, λ), is a $k \times v^2\lambda$ matrix with entries from S such that each $2 \times v^2\lambda$ submatrix contains every possible 2×1 column vector precisely λ times.*

We note that the existence of an OA(v, k, λ) implies the existence of an OA(v, k', λ) for all $k' < k$ (simply by deleting rows of the orthogonal array).

In [5], Gardner generalized a quadrupling construction of Stanton, Kalbfleish, and Mullin [10] to a k-tupling construction for 2-$(v, k, 1)$ coverings. We extend Gardner's k-tupling construction to 2-(v, k, λ) coverings for any λ.

Proposition 4.11 (k-Tupling Construction). *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ be a 2-(v, k, λ) covering and let $0 \leq a \leq v$. If there exists an OA$(v - a, k, \lambda)$, then there exists a 2-$(kv - (k - 1)a, k, \lambda)$ covering with $k|\mathcal{B}| + (v - a)^2\lambda$ blocks.*

Proof. Let $\mathcal{S}_i = (\mathcal{P}_i, \mathcal{B}_i, I_i)$ be a 2-(v, k, λ) covering, isomorphic to $\mathcal{S}$, with $\mathcal{P}_i = \{P_j | 1 \leq j \leq a\} \cup \{P_{i,a+j} | 1 \leq j \leq v - a\}$, for $1 \leq i \leq k$. Now take an OA$(v-a, k, \lambda)M$ with entries from the set $S = \{a + 1, a + 2, \ldots, v\}$. In this orthogonal array M, we replace the entry $M(i, j)$ by $P_{i,M(i,j)}$ for all rows i and columns j. Let $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', I')$ be an incidence structure such that $\mathcal{P}' = \{P_{i,j} | 1 \leq i \leq k, a + 1 \leq j \leq v\}, \mathcal{B}' = \{\{M(1, i), M(2, i), \ldots, M(k, i)\} | 1 \leq i \leq (v - a)^2\lambda\}$, and for $P \in \mathcal{P}', B \in \mathcal{B}'$, we have $(P, B) \in I'$ if and only if $P \in B$. It is straightforward to verify that $(\cup_{i=1}^{k} \mathcal{P}_i, \mathcal{B}' \cup (\cup_{i=1}^{k} \mathcal{B}_i), I' \cup (\cup_{i=1}^{k} I_i))$ is a 2-$(kv - (k - 1)a, k, \lambda)$ covering with $k|\mathcal{B}| + (v - a)^2\lambda$ blocks. □

Proposition 4.12. *If there exists an OA(v, k, λ) and there exists a 2-(v, k, λ) covering $\mathcal{S}$ with regular excess of degree Δ, then the k-tupling construction (with $a = 0$) produces a regular 2-(kv, k, λ) covering with regular excess of degree Δ.*

Proof. Each of the pairs of points $\{P_{i,j}, P_{i',j'}\}, 1 \leq i, i' \leq k, i \neq i', 1 \leq j, j' \leq v$, is incident with exactly λ blocks of the constructed 2-(kv, k, λ) covering, and hence contributes no edge to the excess. Consequently, the excess of this 2-(kv, k, λ) covering is a disjoint union of k copies of the excess of $\mathcal{S}$. □

The following theorem on the existence of orthogonal arrays was obtained by Bose and Bush [3].

Theorem 4.6. *If v and λ are both powers of the same prime, then an OA$(v, \lambda v + 1, \lambda)$ always exists.*

Most of the work on orthogonal arrays focused on the case $\lambda = 1$. When $\lambda = 1$, Theorem 4.6 yields the well-known result that there exists an OA$(v, v + 1, 1)$ whenever v is a prime power.

Corollary 4.13. *Let q be a prime power such that $q^2 + q + 1$ is also a prime power. Then there exists a 2-$((q + 1)(q^2 + q + 1), q + 1, 1)$ design.*

Proof. The existence of an OA$(q^2 + q + 1, q + 1, 1)$ guarantees that Propositions 4.7 and 4.12 give a 2-$((q + 1)(q^2 + q + 1), q + 1, 1)$ design. □

Potentially, an infinite number of 2-$((q + 1)(q^2 + q + 1), q + 1, 1)$ designs could be obtained from Corollary 4.13. This would depend on whether there are infinitely many

prime powers of the form $q^2 + q + 1$, where q is a prime power. However, this is at present an unsolved problem in number theory.

The existence of orthogonal arrays is also far from settled. We regret that we could not find any orthogonal arrays with $\lambda > 1$ that would enable us to construct more regular coverings from those presented in this section via Proposition 4.12. We present these results, however, in the hope that the appropriate orthogonal arrays would be discovered in the future.

5. CONCLUSION

We have shown in this article that certain incidence structures over principal ideal rings possess many interesting combinatorial properties. These incidence structures are all shown to be imbrical designs. These incidence structures allow us to determine the values of $C(\frac{q(q^{t+1}-1)}{q-1}, \frac{q(q^t-1)}{q-1}, t)$, and $C_2(2(q^2+q+1), 2(q+1), 2)$ for all positive integers t and prime powers q. We also exhibit many infinite families of regular covering designs that are degree-minimum. We note that the PIRs used to obtain the best results (e.g., to determine the two covering numbers mentioned above) are often found to be finite fields.

REFERENCES

[1] J.-C. Bermond, J. Bond, and D. Sotteau, On regular packings and coverings, Ann Discrete Math, 34 (1987), 81–99.

[2] T. Beth, D. Jungnickel, and H. Lenz, Design theory, Cambridge University Press, Cambridge, 1993.

[3] R. C. Bose and K. A. Bush, Orthogonal arrays of strength two and three, Ann Math Statist 23 (1952), 508–524.

[4] Y. M. Chee and S. Ling, Projective covering designs, Bull London Math Soc 25 (1993), 231–239.

[5] B. I. Gardner, On coverings and (r, λ)-systems. Ph.D. Thesis, Department of Combinatorics & Optimization, University of Waterloo, Ontario, Canada, 1972.

[6] K. W. Lee, Projective spaces over finite principal ideal rings, Honours Year Thesis, Department of Mathematics, National University of Singapore, 1995/1996.

[7] E. Mendelsohn and A. Assaf, On the spectrum of imbrical designs, Ann Discrete Math 34 (1987), 363–370.

[8] W. H. Mills and R. C. Mullin, ‘‘Coverings and packings,’’ Contemporary design theory: A collection of surveys, Chap. 9, J. H. Dinitz and D. R. Stinson (Editors), Wiley, New York, 1992, pp. 371–399.

[9] J. Schönheim, On coverings, Pacific J Math 14 (1964), 1405–1411.

[10] 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, pp. 428–450.

[11] D. T. Todorov, Coverings of finite sets, Godishnik Vissh Uchebn Zaved Prilozhna Mat 16 (1980), 179–190.

[12] F. D. Veldkamp, Geometry over rings, Handbook of incidence geometry, Chap. 19, F. Buekenhout (Editor), Elsevier Science B. V., Amsterdam, 1995, pp. 1033–1084.

[13] O. Zariski and P. Samuel, Commutative algebra (Volume 1), Springer-Verlag, Berlin, 1958.