AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **76(1)** (2020), Pages 41–54

Toroidal boards and code covering

João Paulo Costalonga*

Universidade Federal do Espírito Santo
Av. Fernando Ferrari, 514
UFES – Campus de Goiabeiras, CCE – Depto. de Matemática
29075-910 – Vitória – ES
Brazil
joaocostalonga@gmail.com

Abstract

We denote by $\mathbb{F}_q$ the field with q elements. A radius-r extended ball with center in a 1-dimensional vector subspace V of $\mathbb{F}_q^3$ is the set of elements of $\mathbb{F}_q^3$ with Hamming distance to V at most r. We define $c(q)$ to be the size of a minimum covering of $\mathbb{F}_q^3$ by radius-1 extended balls. We define a semiqueen to be a piece of a toroidal chessboard that extends the covering range of a rook by the southwest-northeast diagonal containing it. Let $\xi_D(n)$ be the minimum number of semiqueens of the $n \times n$ toroidal board necessary to cover the entire board except possibly for the southwest-northeast diagonal. We prove that, for $q \geq 7$, $c(q) = \xi_D(q-1) + 2$. Moreover, our proof exhibits a method to build such covers of $\mathbb{F}_q^3$ from the semiqueen coverings of the board. With this new method, we determine $c(q)$ for the odd values of q and improve both existing bounds for the even case.

1 Introduction

The problem of finding minimum coverings of $\mathbb{F}_q^n$ with radius-r balls in the Hamming distance is classic in code theory. There is a book on the subject [4] and an updated table with the known bounds for the sizes of such coverings [10]. In [17], a variation of this problem was introduced: a radius-r **extended ball** with center in a 1-dimensional vector subspace V of $\mathbb{F}_q^n$ is the set of elements of $\mathbb{F}_q^n$ with Hamming distance to V at most r. We define $c_q(n, r)$ as the size of a minimum covering of $\mathbb{F}_q^n$ by radius-r extended balls; such a minimum covering is called a **short covering**.

In [14] some interesting reasons to study short coverings are listed. One is that short coverings were used to construct record breaking classical coverings (in [14] it is proved using short coverings that the minimum number of radius-7 hamming balls necessary to cover $\mathcal{F}_5^{10}$ is 9). Another is that they respond well to some heuristic

* The author was partially supported by CNPq, grant 478053/2013-4

ISSN: 2202-3518

methods and give an economical way in terms of memory to store codes. A third one is that they seem to have more interesting mathematical properties than the classic coverings, like more compatibility with the algebraic structure of the vector space $\mathbb{F}_q^n$ and connection with other structures (see [13, 15, 16] for examples).

Few values of $c_q(n, r)$ are known. Here, our concern is the values of $c(q) := c_q(3, 1)$. Some work [13, 16, 15] proved bounds for $c(q)$. In Corollary 1.4, we establish $c(q)$ for odd values of q and improve both existing bounds for the even values. In order to do this, we introduce a relation between short coverings, projective spaces and toroidal (chess)boards. The number of rooks needed to cover an $n \times n$ toroidal board is well known, clearly n. Some studies on covering and packing of queens in toroidal boards were made by [2] and [1]. We introduce a piece with range between a rook and a queen, as described next.

We will use $1, \ldots, n$ as standard representatives for the classes of $\mathbb{Z}_n$. The toroidal $n \times n$ board will be modeled by $\mathbb{Z}_n^2$, with the first coordinate indexing the column and the second the row, in such a way that $(1, 1)$ corresponds to the southwestern square and (n, n) to the northeastern square (the orientation is similar to a cartesian plane). The **diagonal** of $(a, b) \in \mathbb{Z}_n^2$ is the set $D(a, b) := \{(a+t, b+t) : t \in \mathbb{Z}_n\}$. The **vertical** and **horizontal** lines of $(a, b) \in \mathbb{Z}_n^2$ are respectively defined by $V(a, b) := \{(a, t) : t \in \mathbb{Z}_n\}$ and $H(a, b) := \{(t, b) : t \in \mathbb{Z}_n\}$. The **semiqueen** of $(a, b) \in \mathbb{Z}_n^2$ is the set $\mathrm{SQ}(a, b) := D(a, b) \cup V(a, b) \cup H(a, b)$.

We denote by $\mathbb{D}_n$ the toroidal $n \times n$ board without the southwest-northeast diagonal: $\mathbb{D}_n := \mathbb{Z}_n^2 - D(1, 1)$. We also denote by $\xi(n)$ and $\xi_D(n)$ the respective sizes of minimum coverings of $\mathbb{Z}_n^2$ and $\mathbb{D}_n$ by semiqueens of $\mathbb{Z}_n^2$. Next we state our main results. The next theorem establishes a relation between the values of $c(q)$ and $\xi_D(q - 1)$.

Theorem 1.1 *For a prime power $q \geq 5$, $c(q) = \xi_D(q - 1) + 2$. Moreover, for $q \geq 7$, there is an algorithm for building minimum coverings of $\mathbb{F}_q^3$ by radius-1 extended balls from coverings of $\mathbb{D}_{q-1}$ by semiqueens and vice-versa.*

The proof of the first part of Theorem 1.1 is a construction that gives the algorithm for the second part. The proof for Theorem 1.1 is concluded in Section 3. There are certain difficulties in using this technique for higher dimensions than 3. One is to make a more general version of Lemma 3.5 and another is to study the coverings of higher-dimensional boards. The next theorem establishes values and bounds for $\xi(n)$:

Theorem 1.2 *Let n be a positive integer.*

(a) If $n \equiv 2 \bmod 4$, then $\xi(n) = n/2$.

(b) If $n \equiv 0 \bmod 4$, then $\xi(n) = 1 + n/2$.

(c) If n is odd, then $\frac{n+1}{2} \leq \xi(n) \leq \frac{2n+1}{3}$.

For values of $\xi_D(n)$, we have:

Theorem 1.3 *Let n be a positive integer.*

(a) If n is even, then $\xi_D(n) = n/2$.

(b) If n is odd, then $\frac{n+1}{2} \leq \xi_D(n) \leq \frac{2n+1}{3}$.

From Theorems 1.1 and 1.3 and the known values of $c(3)$ and $c(4)$ of [17](see also Section 4), we have:

Corollary 1.4 *Let $q \geq 3$ be a prime power.*

(a) If q is odd, then $c(q) = \frac{q+3}{2}$.

(b) If q is even, then $\frac{q+4}{2} \leq c(q) \leq \frac{2q+5}{3}$.

The upper bound $c(q) \leq \frac{q+3}{2}$ in Corollary 1.4 was proved by Martinhão and Carmelo in [13] for $q \equiv 3 \bmod 4$. The same result for $q \equiv 1 \bmod 4$ was recently proved independently of this work by Martinhão [12]. The upper bound in item (b) of Corollary 1.4 improves the previous one $c(q) \leq 6\lceil \frac{q-1}{9} \rceil + 6\lceil \log_4(\frac{q-1}{3}) \rceil + 3$, set in [15]. The lower bounds of Corollary 1.4 improve the bound $c(q) \geq (q+1)/2$ set in [16]. The next theorem gives us better upper bounds for some even values of q:

Theorem 1.5 *For positive odd integers m and n:*

(a) $\xi(mn) \leq m\xi(n)$.

(b) If q is a power of 2 and $q = mn + 1 \geq 7$, then $c(q) \leq m\xi(n) + 2$.

Theorems 1.2, 1.3 and 1.5 are proved in Section 2. In Section 4, we use an integer linear programming (ILP) formulation to compute $\xi(n)$, $\xi_D(n)$ and $c(q)$ for small values of q and n not covered by our results. There are still few known values for $\xi(n)$ with n odd. Next, we state some conjectures:

Conjecture 1.6 *If p is a prime number, then $\xi(p) = \left\lfloor \frac{2p+1}{3} \right\rfloor$.*

Conjecture 1.7 *If n is an odd positive integer, then*
$$\xi(n) = \min\{(n/m)\xi(m) : m \text{ divides } n\}.$$

Conjecture 1.8 *If n is an odd positive integer, then*
$$\xi(n) = \min\{(n/p)\xi(p) : p \text{ is a prime divisor of } n\}.$$

Conjecture 1.9 *For n assuming positive integer values, $\lim\limits_{n\to\infty} \frac{\xi(2n+1)}{2n+1} = \frac{2}{3}$.*

2 Proofs of Theorems 1.2, 1.3 and 1.5

In this section, we prove Theorems 1.2, 1.3 and 1.5. We will prove some lemmas and establish some concepts first.

Next, we extend our definitions for more general groups than $\mathbb{Z}_n$. Let G be a finite abelian group and $(a,b) \in G^2$. We define the respective **diagonal**, **vertical** and **horizontal** lines and **semiqueen** of $(a,b) \in G^2$ as follows:

- $D(a,b) := D_G(a,b) := \{(ta,tb) : t \in G\}$,
- $H(a,b) := H_G(a,b) := \{(t,b) : t \in G\}$,
- $V(a,b) := V_G(a,b) := \{(a,t) : t \in G\}$ and
- $\mathrm{SQ}(a,b) := \mathrm{SQ}_G(a,b) := D(a,b) \cup H(a,b) \cup V(a,b)$.

For $X \subseteq G^2$, we define $\mathrm{SQ}(X)$ as the union of all semiqueens of the form $\mathrm{SQ}(x)$ with $x \in X$. In an analogous way we define $D(X)$, $H(X)$ and $V(X)$.

We define $\mathbb{D}(G) := G^2 - D(1_G, 1_G)$ and denote by $\xi(G)$ and $\xi_D(G)$ the respective sizes of a minimum covering G^2 and $\mathbb{D}(G)$ by semiqueens of G^2. Suppose that $\varphi : G \to H$ is a group isomorphism and define $\Phi(a,b) = (\varphi(a), \varphi(b))$ for $(a,b) \in G^2$. It is clear that for $x \in G^2$, $\mathrm{SQ}_H(\Phi(x)) = \Phi(\mathrm{SQ}_G(x))$. Therefore:

Lemma 2.1 *If G and H are isomorphic finite abelian groups, then $\xi(G) = \xi(H)$ and $\xi_D(G) = \xi_D(H)$.*

Lemma 2.2 *For each finite abelian group G, $\xi_D(G) \geq (|G|-1)/2$ and $\xi(G) \geq |G|/2$.*

Proof: Write $n := |G|$. Let $\{\mathrm{SQ}(x_1), \ldots, \mathrm{SQ}(x_k)\}$ be a minimum covering of $\mathbb{D}(G)$ by semiqueens. It is clear that $k = \xi_D(G) \leq \xi(G) < n$. So, we may choose a vertical line L of G^2 avoiding $V(x_1), \ldots, V(x_k)$. Note that $C := (L \cap \mathbb{D}(G)) - (H(x_1) \cup \cdots \cup H(x_k))$ has at least $n-k-1$ elements, which must be covered by $D(x_1), \ldots, D(x_k)$. Since each diagonal intersects C in one element, $k \geq n-k-1$ and $\xi_D(G) = k \geq (n-1)/2$. Analogously, we can prove that $\xi(G) \geq n/2$. $\square$

For $k \in \mathbb{Z}_+$, we define a function $\delta_k : \mathbb{Z}_k^2 \to \mathbb{Z}_k$ by $\delta_k(a,b) = b - a$ for each $(a,b) \in \mathbb{Z}_k^2$. We will use this funtion in the proofs that follow in this section. The proof of the next lemma is elementary.

Lemma 2.3 *Le $k \in \mathbb{Z}_+$. If $(a,b), (c,d) \in \mathbb{Z}_k^2$, then $(c,d) \in D(a,b)$ if and only if $\delta_k(c,d) = \delta_k(a,b)$.*

Lemma 2.4 *If n is a positive integer and $n \equiv 2 \bmod 4$, then $\xi_D(n) = \xi(n) = n/2$.*

Proof: By Lemma 2.2, it is enough to find a covering of $\mathbb{Z}_n^2$ with $n/2$ semiqueens. Define $X := \{(2,n), (4,n-2), \ldots, (n,2)\}$. Let us check that $\{\mathrm{SQ}(x) : x \in X\}$ covers the board. This covering is illustrated for $n = 6$ in Figure 1. Note that $\delta_n(X) = \{n-2, n-6, \ldots, 2-n\}$. Since $n \equiv 2 \bmod 4$, it follows that $\delta_n(X)$ is the set of the even elements of $\mathbb{Z}_n$.

Now let $(a,b) \in \mathbb{Z}_n^2$. If both b and a are odd, then $\delta_n(a,b)$ is even and, therefore, $\delta_n(a,b) \in \delta_n(X)$ and $(a,b) \in D(X) \subseteq \mathrm{SQ}(X)$. Otherwise, if one of a or b is even, it is clear that (a,b) is in the vertical or horizontal line of an element of X. Therefore, $\{\mathrm{SQ}(x) : x \in X\}$ covers the board and the lemma is true. $\square$

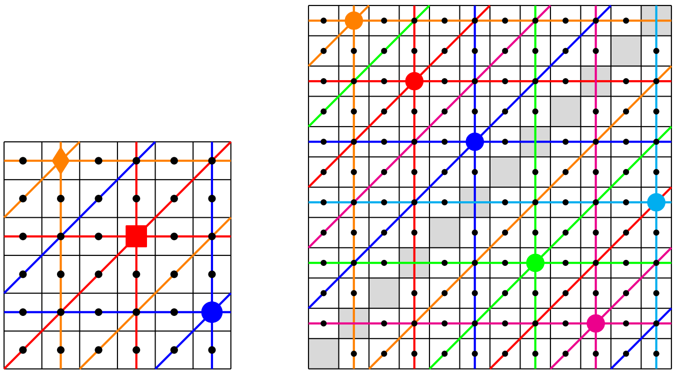

Figure 1: A covering of $\mathbb{Z}_6^2$ as in Lemma 2.4 and a covering of $\mathbb{D}_{12}$ as in Lemma 2.5

Lemma 2.5 *If n is a positive integer multiple of 4, then $\xi_D(n) = n/2$.*

Proof: Let $4m := n$. By Lemma 2.2, it is enough to find a covering of $\mathbb{D}_{4m}$ with $2m$ elements. Such covering is illustrated for $4m = 12$ in Figure 1. Define:

- $A = \{(2,4m),(4,4m-2),\dots(2m,2m+2)\}$,
- $B := \{(2m+2,2m-2),(2m+4,2m-4),\dots,(4m-2,2)\}$ and
- $C := \{(4m,2m)\}$

We claim that $\{\mathrm{SQ}(x) : x \in A\cup B\cup C\}$ covers $\mathbb{D}_{4m}$. Let $(a,b) \in \mathbb{D}_{4m}$. If a or b is even, then it is clear that (a,b) is in the horizontal or vertical line of a member of $A\cup B\cup C$. Suppose that both a and b are odd. We will use the function δ_k for $k = 4m$. Now, $\delta_{4m}(a,b)$ is even. Moreover, $\delta_{4m}(a,b) \neq 0$, since $(a,b) \notin \mathbb{D}_{4m}$ if $a = b$. Note that $\delta_{4m}(A) = \{4m-2,4m-6,\dots,6,2\}$ and $\delta_{4m}(B) = \{-4,-8,\dots,4-4m\}$. So, $\delta_{4m}(A\cup B)$ contains all non-zero even elements of $\mathbb{Z}_{4m}$. In particular it contains $\delta_{4m}(a,b) = b-a$. Therefore, $(a,b) \in D(x) \subseteq \mathrm{SQ}(x)$ for some $x \in A\cup B$ and the lemma holds. $\square$

The next lemma is elementary and its proof is omitted.

Lemma 2.6 *If $\emptyset \subsetneq S \subsetneq \mathbb{Z}_n$ then $S \neq \{x+1 : x \in S\}$.*

Lemma 2.7 *Let V_0 and V_1 be consecutive vertical lines of $\mathbb{Z}_n^2$ with $n \geq 2$. Suppose that $X, Y \subseteq \mathbb{Z}_n^2$ satisfy $|Y|, |X| \leq n-1$ and $V_0 \cup V_1 \subseteq D(X) \cup H(Y)$. Then $|X| + |Y| \geq n+1$.*

Proof: Suppose the contrary. Say that $V_1 = \{(a+1,b) : (a,b) \in V_0\}$. For $i = 0,1$, V_i is the union of $A_i := V_i \cap D(X)$ and $B_i := V_i \cap H(Y)$. Note that $|A_0| = |A_1| \leq |X|$ and $|B_0| = |B_1| \leq |Y|$. For $i = 0,1$, $|V_i| \leq |A_i| + |B_i| = |X| + |Y| \leq n = |V_i|$. So, $A_i \cap B_i = \emptyset$. Define a function $\pi : \mathbb{Z}_n^2 \to \mathbb{Z}_n$ by $\pi(a,b) = b$. Since the restriction of π to each vertical line is bijective, $\pi(A_0) = \mathbb{Z}_n - \pi(B_0) = \mathbb{Z}_n - \pi(B_1) = \pi(A_1)$. But $\pi(A_1) := \{t+1 : t \in \pi(A_0)\}$, a contradiction to Lemma 2.6. $\square$

Lemma 2.8 *For each odd integer $n \geq 3$, $\xi_D(n) \geq (n+1)/2$.*

Proof: Let $2m+1 := n$ with $m \geq 1$. By Lemma 2.2, $\xi_D(2m+1) \geq m$. Suppose for a contradiction that $\xi_D(2m+1) = m$ and let $X := \{x_1, \dots, x_m\}$ be an m-subset of $\mathbb{D}(2m+1)$ such that $\{\mathrm{SQ}(x) : x \in X\}$ covers $\mathbb{D}(2m+1)$. Thus, there are two consecutive vertical lines V_0 and V_1 in $\mathbb{Z}_{2m+1}^2$ avoiding $V(X)$. As $\mathbb{D}(2m+1) \subseteq \mathrm{SQ}(X)$, it follows that $V_0 \cup V_1 \subseteq H(X) \cup D(X \cup \{(1,1)\})$. By Lemma 2.7, $2m+1 = 2|X|+1 \geq (2m+1)+1$, a contradiction. $\square$

The next lemma was proved by L. Euler [5]. An alternative proof may be found in [6, Corollary 1]. The reader also may see a more general result in Wanless's survey [18, Theorem 2], proved by Maillet [11].

Lemma 2.9 *(Euler, 1779) Let $Q = [q_{ij}]$ be a Latin square with even order $n \geq 2$. Suppose that $q_{ij} = q_{kl}$ if and only if $i - j \equiv k - l \bmod n$. Then, Q admits no set X of n entries such that each pair of entries of X are in different rows, different columns and has different symbols. (Such a set is called a **Latin transversal**.)*

In Lemma 2.9, supposing that $q_{ij} = q_{kl}$ if and only if $i + j \equiv k + l \bmod n$ has the same effect; usually this is the way it is usually stated.

Lemma 2.10 *If n is a positive integer multiple of four, then $\xi(n) = 1 + n/2$.*

Proof: Let $4m := n$. By Lemma 2.5, $2m = \xi_D(4m) \leq \xi(4m) \leq \xi_D(4m)+1 = 2m+1$. So, all we have to prove is that $\xi(4m) \neq 2m$. Suppose for a contradiction that $\xi(4m) = 2m$. Let $X := \{(a_t, b_t) : t = 1, \dots, 2m\}$ be a subset of $\mathbb{Z}_{4m}^2$ such that $\{\mathrm{SQ}(x) : x \in X\}$ covers $\mathbb{Z}_{4m}^2$.

First we will prove that:

$$\{a_1, \dots, a_{2m}\}, \{b_1, \dots, b_{2m}\} \in \big\{\{1,3,\dots,4m-1\}, \{2,4,\dots,4m\}\big\}. \tag{1}$$

Suppose the contrary. Then, there are two consecutive horizontal lines avoiding $H(X)$ or two consecutive vertical lines avoiding $V(X)$. We may assume the later case. Let V_0 and V_1 be such lines. So, $V_0 \cup V_1 \subseteq H(X) \cup D(X)$. By Lemma 2.7, $2|X| = 4m \geq 4m+1$, a contradiction. So, (1) holds.

By (1), we may assume, without loss of generality, that $E := \{2,4,\dots,4m\} = \{a_1, \dots, a_{2m}\} = \{b_1, \dots, b_{2m}\}$. So $X \subseteq E \times E$. Let $F := \mathbb{Z}_{4m} - E$. The fact that $V(X) \cup H(X)$ does not intersect $F \times F$ implies that $F \times F \subseteq D(X)$. We will use the function δ_k for $k = 4m$. Note that, in each row or column of $F \times F$, δ_{4m} assumes

$2m$ distinct values. By Lemma 2.3, δ_{4m} also assumes $2m$ distinct values on X. Now, construct a Latin square having F as set of rows and columns such that the symbol in (a, b) is $\delta_{4m}(a, b)$. The existence of this Latin square contradicts Lemma 2.9. $\square$

Next we prove Theorem 1.5.

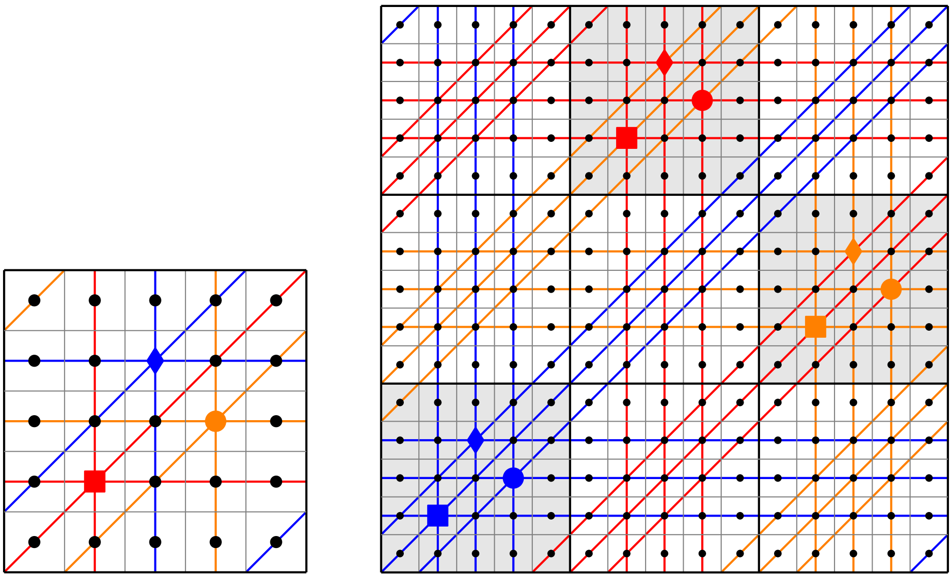

Figure 2: A covering of $\mathbb{Z}_{15}^2$ by semiqueens constructed from a covering of $\mathbb{Z}_5^2$ with the method of the proof of Theorem 1.5

Proof of Theorem 1.5: As we will deal with both rings $\mathbb{Z}_n$ and $\mathbb{Z}_{mn}$, for distinction purposes, we will denote by $z + k\mathbb{Z}$ the residue class modulo k of z for each $z \in \mathbb{Z}$ and $k \in \{n, mn\}$. Let $\{\mathrm{SQ}_{\mathbb{Z}_n}(x_i + n\mathbb{Z}, y_i + n\mathbb{Z}) : i = 1, \ldots, \xi(\mathbb{Z}_n)\}$ be a covering for $\mathbb{Z}_n^2$. Define

$$X := \big\{\big((x_i + \lambda n) + mn\mathbb{Z}, (y_i - \lambda n) + mn\mathbb{Z}\big) : i = 1, \ldots, \xi(\mathbb{Z}_n) \text{ and } \lambda \in \mathbb{Z}\big\}.$$

Note that $|X| \leq m\xi(\mathbb{Z}_n)$. To prove item (a), it suffices to check that each element $(a + mn\mathbb{Z}, b + mn\mathbb{Z}) \in \mathbb{Z}_{mn}^2$ is in the semiqueen of some element of X. Let i be the index such that, for $v_i := (x_i + n\mathbb{Z}, y_i + n\mathbb{Z})$, $u := (a + n\mathbb{Z}, b + n\mathbb{Z}) \in \mathrm{SQ}_{Z_n}(v_i)$. If $u \in V_{Z_n}(v_i)$, then there is an integer λ such that $a = x_i + \lambda n$ and $(a+mn\mathbb{Z}, b+mn\mathbb{Z})$ is in the semiqueen of $\big((x_i + \lambda n) + mn\mathbb{Z}, (y_i - \lambda n) + mn\mathbb{Z}\big) \in X$. If $u \in H_{Z_n}(v_i)$, we proceed analogously. So, we may assume that $u \in D_{Z_n}(v_i)$. We will use the function δ_k for $k = n$ on $\mathbb{Z}_n^2$ and for $k = mn$ on $\mathbb{Z}_{mn}$. As $u \in D_{Z_n}(v_i)$, it follows that $\delta_n(u) = \delta_n(v_i)$ and, therefore, there is an integer α such that $b - a = y_i - x_i - \alpha n$. Since mn is odd, $2 + mn\mathbb{Z}$ is invertible in $\mathbb{Z}_{mn}$ and there is an integer λ such that $2\lambda + mn\mathbb{Z} = \alpha + mn\mathbb{Z}$. Now

$$\begin{aligned}\delta_{mn}\big((x_i + \lambda n) + mn\mathbb{Z}, (y_i - \lambda n) + mn\mathbb{Z}\big) &= (y_i - x_i) - 2\lambda n + mn\mathbb{Z} \\ &= b - a + mn\mathbb{Z} \\ &= \delta_{mn}(a + mn\mathbb{Z}, b + mn\mathbb{Z}).\end{aligned}$$

By Lemma 2.3, $(a + mn\mathbb{Z}, b + mn\mathbb{Z})$ is in the semiqueen of $\big((x_i + \lambda n) + mn\mathbb{Z}, (y_i - \lambda n) + mn\mathbb{Z}\big) \in X$. This completes the proof for item (a). Item (b) follows from item (a) and Theorem 1.1. $\square$

Lemma 2.11 *If n is odd, then $\xi(n) \leq \lfloor (2n+1)/3 \rfloor$.*

Proof: Write $n = 3m + r$ with $r \in \{0, 1, 2\}$. If $r = 0$, then, as $\xi(3) = 2$, by Theorem 1.5, $\xi(n) \leq 2m = \lfloor (2n+1)/3 \rfloor$ and the lemma holds. So, assume that $r \in \{1, 2\}$. We shall prove that $\xi(n) \leq 2m + 1$. Consider a subdivision of the board as below:

$Q_{1,3}$	$Q_{2,3}$	$Q_{3,3}$
$Q_{1,2}$	$Q_{2,2}$	$Q_{3,2}$
$Q_{1,1}$	$Q_{2,1}$	$Q_{3,1}$

,

where $Q_{1,1}$, $Q_{2,2}$ and $Q_{3,3}$ are square blocks with respective orders $m + 1$, m and $m + r - 1$. Let X_i be the set of the pairs of $\mathbb{Z}_n^2$ in the southeast-northwest diagonal of $Q_{i,i}$. Define $X = X_1 \cup X_2$. We will prove that $\{\mathrm{SQ}(x) : x \in X\}$ covers the board. If $Q_{i,j} \neq Q_{3,3}$ it is clear that $Q_{i,j} \subseteq \bigcup_{x \in X} \big(H(x) \cup V(x)\big)$. So, let $y \in Q_{3,3}$. We shall prove that $y \in D(x)$ for some $x \in X$. If c is a coordinate of y, then $2m + 2 \leq c \leq 3m + r$. Therefore, $-m \leq -m - r + 2 \leq \delta_n(y) \leq m + r - 2 \leq m$. Note that $\delta_n(X_1) = \{m, m-2, m-4, \ldots, 4-m, 2-m, -m\}$ and $\delta_n(X_2) = \{m-1, m-3, \ldots, 3-m, 1-m\}$. So, $\delta_n(X_1 \cup X_2) = \{m, m-1, \ldots, 1-m, -m\}$ and $\delta_n(y) \in \delta_n(X)$. By Lemma 2.3, y is in $D(x)$ for some $x \in X$ and the lemma holds. $\square$

Proof of Theorem 1.2: Items (a) and (b) follow from Lemmas 2.4 and 2.10, respectively. Item (c) follows from Lemmas 2.8 and 2.11. $\square$

Proof of Theorem 1.3: Item (a) follows from Lemmas 2.4 and 2.5. Item (b) follows from Lemmas 2.8 and 2.11. $\square$

3 From $\mathbb{F}_q^3$ to the projective plane

In this section, we establish relations between short coverings and coverings by semiqueens using the projective plane as a link between them. We prove Theorem 1.1 at the end of this section.

We define the **projective plane** $PG(2, q)$ as the set of the 1-dimensional vector subspaces of $\mathbb{F}_q^3$; we call its elements **points**. We say that $L \subseteq PG(2, q)$ is a **line** if the union of the elements of L is a 2-dimensional vector subspace of $\mathbb{F}_q^3$. We denote the subspace spanned by $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3 - \{0\}$ by homogeneous coordinates $(\alpha : \beta : \gamma) \in PG(2, q)$.

We say that the points of $PG(2, q)$ are **cardinal**, **coast** or **midland** when they have exactly one, two or three non-zero coordinates respectively. We denote the cardinal points by $c_1 := (1 : 0 : 0)$, $c_2 := (0 : 1 : 0)$ and $c_3 := (0 : 0 : 1)$. We also denote the line containing the points u and v by $\overleftrightarrow{u, v}$, provided $u \neq v$, and, for convenience, $\overleftrightarrow{u, u} := \{u\}$. We say that a line of $PG(2, q)$ is a **midland line** if it contains a midland point and a **coast line** otherwise. Note that the unique coast lines are $\overleftrightarrow{c_1, c_2}$, $\overleftrightarrow{c_1, c_3}$ and $\overleftrightarrow{c_2, c_3}$. Moreover, we denote by e_i the i-th vector in the canonical basis of $\mathbb{F}_q^3$, and by $[v_1, \ldots, v_n]$ the subspace of $\mathbb{F}_q^3$ spanned by $v_1, \ldots, v_n$. We denote by $EB[v, r]$ the extended ball with radius r and center v. The next lemma is easy to check:

Lemma 3.1 *If $v \in \mathbb{F}_q^3 - \{0\}$, then $EB[v, 1]$ is the union of the members of $\overleftrightarrow{[v], c_1} \cup \overleftrightarrow{[v], c_2} \cup \overleftrightarrow{[v], c_3}$.*

Motivated by Lemma 3.1, we define the **compass rose** of $p \in PG(2, q)$ as

$$W(p) := \overleftrightarrow{p, c_1} \cup \overleftrightarrow{p, c_2} \cup \overleftrightarrow{p, c_3}.$$

From Lemma 3.1, we may conclude:

Corollary 3.2 *Let $p_1, \ldots, p_n \in PG(2, q)$ and for $i = 1, \ldots, n$, let $v_i \in p_i - \{0\}$. Then, $\{W(p_1), \ldots, W(p_n)\}$ covers $PG(2, q)$ if and only if $\{EB[v_1, 1], \ldots, EB[v_n, 1]\}$ covers $\mathbb{F}_q^3$. Moreover, $c(q)$ is the size of a minimum covering of $PG(2, q)$ by compass roses.*

We say that a compass rose $W(p)$ is **cardinal**, **coast** or **midland** according to which of these adjectives applies to p. It is clear that $W(p_1) = W(p_2)$ implies $p_1 = p_2$. So, exactly one of these adjectives applies to a particular compass rose. The following properties of compass roses are elementary and easy to check:

Lemma 3.3 *Each midland compass rose is the union of three distinct midland lines, each coast compass rose is the union of a coast and a midland line and each cardinal compass rose is the union of two distinct coast lines.*

Lemma 3.4 *Let q be a prime power and suppose that $c(q) \leq q - 2$. Then, every minimum covering $\mathcal{C}$ of $PG(2, q)$ by compass roses contains at least two non-midland compass roses. In particular, each coast line is contained in a member of $\mathcal{C}$.*

Proof: Since $PG(2, q)$ has three distinct coast lines, the first part of the lemma follows from the second part and from Lemma 3.3. So, let us prove the second part. Suppose that it fails. Let $\mathcal{C}$ be a minimum covering of $PG(2, q)$ by compass roses such that no member contains a fixed coast line L. Let K be the set of coast points in L. Since no member of $\mathcal{C}$ contains L, each compass rose in $\mathcal{C}$ meets K in at most one point. So, $q - 1 = |K| \leq |\mathcal{C}| = c(q) \leq q - 2$, a contradiction. □

Lemma 3.5 *Let q be a prime power and suppose that $c(q) \leq q - 2$. Then, there is a minimum covering of $PG(2, q)$ by compass roses containing precisely one cardinal compass rose and one coast compass rose.*

Proof: Choose a minimum covering $\mathcal{C}$ of $PG(2, q)$ by compass roses maximizing the number of midland compass roses primarily and coast compass roses secondarily. There are three coast lines in $PG(2, q)$: the members of $\mathcal{L} := \{\overleftrightarrow{c_1, c_2}, \overleftrightarrow{c_1, c_3}, \overleftrightarrow{c_2, c_3}\}$. By Lemmas 3.4 and 3.3, the members of $\mathcal{L}$ are covered by:

(i) One cardinal and one coast compass rose of $\mathcal{C}$,

(ii) Two cardinal compass roses of $\mathcal{C}$, or

(iii) Three coast compass roses of $\mathcal{C}$.

We shall prove that (i) occurs. Indeed, first suppose for a contradiction that (ii) holds. Say that the members of $\mathcal{L}$ are covered by $W(c_1)$ and $W(c_2)$. If p is a coast point of $\overleftrightarrow{c_2, c_3}$, then $W(c_1)$ and $W(p)$ are enough to cover the coast lines of $PG(2, q)$. Hence $(\mathcal{C} - \{W(c_2)\}) \cup \{W(p)\}$ contradicts the secondary maximality of $\mathcal{C}$. Thus, (ii) does not hold.

Now, suppose that (iii) holds. The coast lines of $PG(2, q)$ are covered by three coast compass roses $W(p_1), W(p_2), W(p_3) \in \mathcal{C}$. It is clear that p_1, p_2 and p_3 are in different coast lines. For $\{i, j, k\} = \{1, 2, 3\}$, say that $p_k \in \overleftrightarrow{c_i, c_j}$. Let x be the intersection point of $\overleftrightarrow{c_2, p_2}$ and $\overleftrightarrow{c_3, p_3}$. Note that x is a midland point. We claim that

$$\mathcal{C}' := (\mathcal{C} - \{W(p_2), W(p_3)\}) \cup \{W(c_1), W(x)\}$$

contradicts the primary maximality of $\mathcal{C}$. Note that $\mathcal{C}'$ has more midland compass roses than $\mathcal{C}$ and $|\mathcal{C}'| \leq |\mathcal{C}|$. It is left to to show that $\mathcal{C}'$ covers $PG(2, q)$. For this purpose, it is enough to prove that $W(p_2) \cup W(p_3) \subseteq W(c_1) \cup W(x)$. Indeed, as $p_2 \in \overleftrightarrow{c_1, c_3}$, it follows that $W(p_2) = \overleftrightarrow{c_1, c_3} \cup \overleftrightarrow{c_2, p_2}$, but $\overleftrightarrow{c_2, p_2} = \overleftrightarrow{c_2, x} \subseteq W(x)$ and $\overleftrightarrow{c_1, c_3} \subseteq W(c_1)$. Moreover, $W(p_3) = \overleftrightarrow{c_1, c_2} \cup \overleftrightarrow{c_3, p_3}$, but $\overleftrightarrow{c_3, p_3} = \overleftrightarrow{c_3, x} \subseteq W(x)$ and $\overleftrightarrow{c_1, c_2} \subseteq W(c_1)$. So, $\mathcal{C}'$ covers $PG(2, q)$ and (iii) does not occur. Therefore, (i) holds.

Now, let W_1 and W_2 be the respective compass roses described in (i). It is left to prove that W is midland if $W \in \mathcal{C} - \{W_1, W_2\}$. As all cardinal compass roses are contained in $W_1 \cup W_2$, by the minimality of $\mathcal{C}$, it follows that W is not cardinal. If W is coast, then W is the union of a coast line C and a midland line M. But, $C \subseteq W_1 \cup W_2$ and, if $x \in M - C$ is a midland point, then $M \subseteq W(x)$. Thus $(\mathcal{C} - \{W\}) \cup \{W(x)\}$ violates the primary maximality of $\mathcal{C}$. Therefore, W is midland and the lemma holds. □

We define a bijection $f : PG(2, q) \to PG(2, q)$ to be a **projective automorphism** if $f(\overleftrightarrow{x, y}) = \overleftrightarrow{f(x), f(y)}$ for all $x, y \in PG(2, q)$.

Lemma 3.6 *If f is a projective automorphism of $PG(2, q)$ carrying cardinal points into cardinal points, then $f(W(x)) = W(f(x))$ for each $x \in PG(2, q)$. Moreover, x is midland (resp. coast, cardinal) if and only if $f(x)$ is midland (resp. coast, cardinal).*

Proof: For $x \in PG(2, q)$:

$$\begin{aligned}
f(W(x)) &= f\left(\overleftrightarrow{x, c_1} \cup \overleftrightarrow{x, c_2} \cup \overleftrightarrow{x, c_3}\right) \\
&= f\left(\overleftrightarrow{x, c_1}\right) \cup f\left(\overleftrightarrow{x, c_2}\right) \cup f\left(\overleftrightarrow{x, c_3}\right) \\
&= \overleftrightarrow{f(x), f(c_1)} \cup \overleftrightarrow{f(x), f(c_2)} \cup \overleftrightarrow{f(x), f(c_3)} \\
&= \overleftrightarrow{f(x), c_1} \cup \overleftrightarrow{f(x), c_2} \cup \overleftrightarrow{f(x), c_3} \\
&= W(f(x)).
\end{aligned}$$

This proves the first part of the lemma. For the second part, by hypothesis, x is cardinal if and only if $f(x)$ is cardinal. Also, x is coast if and only if x is not cardinal but is in the line containing two cardinal points, thus $f(x)$ is also coast. Therefore, x is coast if and only $f(x)$ is coast. By elimination, this implies that x is midland if and only if $f(x)$ is midland. □

The next lemma has a straightforward proof.

Lemma 3.7 *Let x be a cardinal point and y a coast point of $PG(2, q)$ such that $W(x) \cup W(y)$ contains all coast points of $PG(2, q)$. Then, for some $\{i, j, k\} = \{1, 2, 3\}$, $x = c_i$ and $y \in \overleftrightarrow{c_j, c_k}$.*

Lemma 3.8 *Let q be a prime power and suppose that $c(q) \leq q - 2$. There is a minimum covering of $PG(2, q)$ by compass roses containing $W(0 : 0 : 1)$ and $W(1 : 1 : 0)$ and such that all other members are midland.*

Proof: By Lemma 3.5, there is a minimum covering $\mathcal{C}$ of $PG(2, q)$ by compass roses, all of which are midland, except for two, namely $W(x)$ and $W(y)$, where x is a cardinal point and y a coast point. We may define a projective automorphism $f : PG(2, q) \to PG(2, q)$ by permutations of homogeneous coordinates and multiplying fixed coordinates by non-zero factors such that $f(x) = (0 : 0 : 1)$. By Lemma 3.7, $f(y)$ is in the form $(a : b : 0)$ with $a \neq 0 \neq b$. So, in addition, we may pick f in such a way that $f(y) = (1 : 1 : 0)$. By Lemma 3.6, $\{f(W) : W \in \mathcal{C}\}$ is the covering we are looking for. □

Consider the multiplicative group $\mathbb{F}_q^*$. We will use the terminologies $\mathbb{D}(\mathbb{F}_q^*)$, $\xi_D(\mathbb{F}_q^*)$, etc. as defined in the beginning of Section 2 for $G = \mathbb{F}_q^*$.

Consider the set M of midland points in $PG(2, q)$ and the bijection ψ between $(\mathbb{F}_q^*)^2$ and M defined by $\psi(a, b) = (a : b : 1)$. For $x = (a, b) \in (\mathbb{F}_q^*)^2$, we clearly have $\psi\big(H_{\mathbb{F}_q^*}(x)\big) = M \cap \big(\overleftrightarrow{\psi(x), c_1}\big)$ and $\psi\big(V_{\mathbb{F}_q^*}(x)\big) = M \cap \big(\overleftrightarrow{\psi(x), c_2}\big)$. Moreover, as $D_{\mathbb{F}_q^*}(x) = \big\{(ta, tb) : t \in \mathbb{F}_q^*\big\}$, hence:

$$\psi\big(D_{\mathbb{F}_q^*}(x)\big) = \{(ta : tb : 1) : t \in \mathbb{F}_q^*\} = \{(a : b : t^{-1}) : t \in \mathbb{F}_q^*\} = M \cap \big(\overleftrightarrow{\psi(x), c_3}\big).$$

As a consequence, $\psi\big(\mathrm{SQ}_{\mathbb{F}_q^*}(x)\big) = M \cap W(\psi(x))$. Note that $\psi\big(D_{\mathbb{F}_q^*}(1, 1)\big) = M \cap \big(\overleftrightarrow{c_3, (1 : 1 : 0)}\big)$. Therefore, the following lemma holds:

Lemma 3.9 *Consider the function ψ as defined above and let $X \subseteq (\mathbb{F}_q^*)^2$. Then $\mathrm{SQ}_{\mathbb{F}_q^*}(X)$ is a covering by semiqueens of $\mathbb{D}(\mathbb{F}_q^*)$ if and only if $\{W(\psi(x)) : x \in X\} \cup \{W(0 : 0 : 1), W(1 : 1 : 0)\}$ is a covering of $PG(2, q)$ by compass roses.*

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1: It is well known that the multiplicative group of a finite field is cyclic. Thus, $\mathbb{F}_q^* \cong \mathbb{Z}_{q-1}$ and, by Lemma 2.1, $\xi_D(\mathbb{F}_q^*) = \xi_D(q - 1)$.

Let $\mathcal{Q}$ be a minimum covering of $\mathbb{D}(\mathbb{F}_q^*)$ by semiqueens of $(\mathbb{F}_q^*)^2$ and $\mathcal{R}$ the covering of $PG(2, q)$ by compass roses obtained from $\mathcal{Q}$ as in Lemma 3.9. So, $|\mathcal{R}| - 2 = |\mathcal{Q}| = \xi_D(\mathbb{F}_q^*) = \xi_D(q - 1)$. By Corollary 3.2, $c(q) \leq |\mathcal{R}| = \xi_D(q - 1) + 2$.

Now we have to prove that $\xi_D(q-1) \leq c(q) - 2$ to finish the proof. When $q = 5$ the values are known and match the theorem (see Section 4). Assume that $q \geq 7$.

We shall prove next that $c(q) \leq q-2$ in order to satisfy the hypothesis of Lemma 3.8. First suppose that q is odd. By Theorem 1.3, $\xi_D(q-1) \leq (q-1)/2$. By the inequality that we already proved, $c(q) \leq \xi_D(q-1)+2 \leq (q-1)/2+2$. Since $q \geq 7$, this implies $c(q) \leq q-2$. Now suppose that q is even. It is known that $c(8) = 6$ (see Section 4). So, we may assume that $q \geq 16$. By Theorem 1.3, $\xi_D(q-1) \leq (2q-1)/3$. Hence $c(q) \leq \xi_D(q-1) + 2 \leq (2q+5)/3$. This implies that $c(q) \leq q-2$ because $q \geq 16$. Therefore, $c(q) \leq q-2$ for each prime power $q \geq 7$.

By Corollary 3.2, $c(q)$ is the size of a minimum covering $\{W(p) : p \in A\}$ of $PG(2,q)$ by compass roses. By Lemma 3.8, we may choose A in such a way that $(0:0:1)$ and $(1:1:0)$ are in A and all points of $B := A - \{(0:0:1),(1:1:0)\}$ are midland. Consider the injective function $\psi : (\mathbb{F}_q^*)^2 \to PG(2,q)$ defined by $\psi(a,b) = (a:b:1)$, the same one of Lemma 3.9. By Lemma 3.9, $\mathcal{Q} := \{W(x) : x \in \psi^{-1}(B)\}$ is a covering of $\mathbb{D}(\mathbb{F}_q^*)$ by semiqueens of $(\mathbb{F}_q^*)^2$. So, $\xi_D(q-1) = \xi_D(\mathbb{F}_q^*) \leq |\mathcal{Q}| = |B| = |A| - 2 = c(q) - 2$. $\square$

4 Particular instances and ILP formulation

For $X \in \{\mathbb{Z}_n^2, \mathbb{D}_n\}$, the following integer 0-1 linear program may be used to find minimum coverings of X by semiqueens of $\mathbb{Z}_n^2$. In this formulation, $x_p = 1$ if and only if $\mathrm{SQ}(p)$ is used in the covering.

$$\begin{array}{rl} \text{Minimize :} & \sum\limits_{p\in\mathbb{Z}_n^2} x_p \\ \text{Subject to :} & \forall q \in X : \sum\limits_{p\in\mathbb{Z}_n^2 : q\in \mathrm{SQ}(p)} x_p \geq 1. \end{array}$$

For finding short coverings of $\mathbb{F}_q^3$, a formulation in terms of compass roses in $PG(2,q)$ works similarly (see Corollary 3.2):

$$\begin{array}{rl} \text{Minimize :} & \sum\limits_{p\in PG(2,q)} x_p \\ \text{Subject to :} & \forall q \in PG(2,q) : \sum\limits_{p\in PG(2,q) : q\in W(p)} x_p \geq 1. \end{array}$$

Some instances not covered by our theorems were solved using GLPK [7], Cplex [9] and Gurobi [8]. They are displayed in the tables below. The values $c(2)$, $c(3)$ and $c(4)$ are already known from [16].

n	3	5	7	9	11	13	15	17
$\xi(n)$	2	3	5	6	7	9	9	11
$\xi_D(n)$	2	3	4	6	7	8	9	11

q	2	3	4	5	8	16
$c(q)$	1	3	3	4	6	11

References

[1] A. P. Burger, C. M. Mynhardt and W. D. Weakley, The domination number of the toroidal queens graph of size $3k \times 3k$, *Australas. J. Combin.* **28** (2003), 137–148.

[2] A. P. Burger, E. J. Cockayne and C. M. Mynhardt, Queens graphs for chessboards on the torus, *Australas. J. Combin.* **24** (2001), 231–246.

[3] E. J. Cockayne, Chessboard domination problems, *Discrete Math.* **86** (1990), 13–20.

[4] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Amsterdam, 1997.

[5] L. Euler, Recherche sur une nouvelle espèce de quarrès magiques, *Leonardi Euleri Opera Omnia* **7** (1923), 291–392.

[6] A. B. Evans, Latin squares without orthogonal mates, *Des. Codes Cryptogr.* **40** (2006), 121–130.

[7] GNU Linear Programming Kit, Version 4.52, `http://www.gnu.org/software/glpk/glpk.html`.

[8] Gurobi Optimization Inc., Gurobi Optimizer Reference Manual, 2015, `http://www.gurobi.com`.

[9] IBM ILOG CPLEX Optimizer, 2010, `http://www-01.ibm.com/software/integration/optimization/cplex-optimizer/`.

[10] G. Kéri, *Tables for bound on covering codes*, (accessed 2017), `http://archive.is/8LCxi`.

[11] E. Maillet, Sur les carrés Latins d'Euler, *Assoc. Franc. Caen.* **23** (1894), 244–252.

[12] A. N. Martinhão, *Problemas combinatórios envolvendo estruturas em espaços de Hamming*, Universidade Estadual de Maringá, Ph.D. Thesis, 2016.

[13] A. N. Martinhão and E. L. Monte Carmelo, Short covering codes arising from matchings in weighted graphs, *Math. Comp.* **82** (2012), 605–616.

[14] C. Mendes, E. L. Monte Carmelo and M. V. Poggi, Bounds for short covering codes and reactive tabu search, *Discrete Appl. Math.* **158** (2010), 522–533.

[15] E. L. Monte Carmelo and C. F. X. De Mendonça Neto, Extremal problems on sum-free sets and coverings in tridimensional spaces, *Aequat. Math.* **78** (2009), 101–112.

[16] E. L. Monte Carmelo and I. N. Nakaoka, Short coverings in tridimensional spaces arising from sum-free sets, *European J. Combin.* **29** (2008), 227–233.

[17] E. L. Monte Carmelo, I. N. Nakaoka and J. R. Geronimo, A covering problem on finite spaces and rook domains, *Int. J. Appl. Math.* **20** (2007), 875–886.

[18] I. M. Wanless, "Transversals in Latin squares: A survey", in: Chapman (ed.), *Surveys in Combinatorics 2011*, London Math. Soc. Lec. Note Series 392, Cambridge University Press, 2011, 403–437.

(Received 6 Aug 2018; revised 30 Jan 2019, 23 July 2019)