JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Bhawesh MISHRA et Paolo SANTONASTASO

Prime Power Residues and Blocking Sets

Tome 37, nº 3 (2025), p. 775-793.

https://doi.org/10.5802/jtnb.1342

Journal de Théorie des Nombres
de Bordeaux **37** (2025), 775–793

Prime Power Residues and Blocking Sets

par Bhawesh MISHRA et Paolo SANTONASTASO

Résumé. Soit q un nombre premier impair et soit B une partie finie de l'ensemble des entiers qui ne contient aucune puissance q-ième parfaite. Nous prouvons que B contient une puissance q-ième modulo presque tout nombre premier si et seulement si B correspond à un ensemble bloquant (par rapport aux hyperplans) dans $\mathrm{PG}(\mathbb{F}_q^k)$. Ici k désigne le nombre de diviseurs premiers des parties q-libres des éléments de B. Par conséquent, la propriété de contenir une puissance q-ième modulo presque tout nombre premier est invariante sous la q-équivalence géométrique définie par un élément du groupe projectif linéaire $\mathrm{PGL}(\mathbb{F}_q^k)$. En utilisant ce lien entre la géométrie de Galois et la théorie des nombres, deux branches différentes des mathématiques, nous classifions les ensembles minimaux vérifiant cette propriété et donnons des majorations de leur taille.

Abstract. Let q be a fixed odd prime. We show that a finite subset B of integers, not containing any perfect q^{th} power, contains a q^{th} power modulo almost every prime if and only if B corresponds to a blocking set (with respect to hyperplanes) in $\mathrm{PG}(\mathbb{F}_q^k)$. Here, k is the number of distinct prime divisors of q-free parts of elements of B. As a consequence, the property of a subset B to contain q^{th} power modulo almost every prime p is invariant under geometric q-equivalence defined by an element of the projective general linear group $\mathrm{PGL}(\mathbb{F}_q^k)$. Employing this connection between two disparate branches of mathematics, Galois geometry and number theory, we classify, and provide bounds on the sizes of, minimal such sets B.

1. Introduction

In this article, we are primarily concerned with finite subsets B of integers that contain a q^{th} power modulo almost every prime p. Here, the phrase *almost every prime* will denote all but finitely many primes and *perfect q^{th} power* will mean q^{th} power of an integer. Any B that already contains a perfect q^{th} power is trivially such a set. The more interesting case is when

Manuscrit reçu le 4 décembre 2023, révisé le 5 juin 2025, accepté le 4 juillet 2025.

2020 *Mathematics Subject Classification.* 51E21, 05B25, 11A15.

Mots-clefs. Power-Residue, Blocking Sets, Local-Global Principle.

The second author research was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM) and by the INdAM - GNSAGA Project *Tensors over finite fields and their applications*, number E53C23001670001 and by Bando Galileo 2024 - G24-216.

B does not contain any perfect q^{th} power but still contains a q^{th} power modulo almost every prime. We will call such sets *locally q^{th} power sets.*

Our starting point is the following classical result on locally 2^{nd} power sets, which was first obtained by Fried in [8], and later rediscovered by Filaseta and Richman in [7].

Proposition 1.1. *Let $a_1, a_2, \ldots, a_l$ be finitely many nonzero integers. Then the following three conditions are equivalent:*

1. *The set $\{a_1, a_2, \ldots, a_l\}$ contains a square modulo almost every prime.*
2. *For every odd prime $p \nmid \prod_{j=1}^{l} a_j$, the set $\{a_1, a_2, \ldots, a_l\}$ contains a square modulo p.*
3. *There exists $T \subseteq \{1, 2, \ldots, l\}$ of odd cardinality such that $\prod_{j\in T} a_j$ is a perfect square.*

The analogous result for general powers was obtained by A. Schinzel and M. Skałba in [13] and is combinatorially quite complex in nature. The main result in [13] deals with a more general problem and considers subsets of rings of integers. We refer the readers to [13, Theorems 1, 2] for the results obtained by Schinzel and Skałba. For prime powers, M. Skałba further simplified the result to obtain the following [14].

Proposition 1.2. *Let q be a prime and $B = \{b_1, b_2, \ldots, b_l\}$ be a set of finitely many distinct non-zero integers. Then the following conditions are equivalent:*

1. *The set B contains a q^{th} power modulo almost every prime.*
2. *For every prime $p \neq q$ and $p \nmid \prod_{j=1}^{l} b_j$, the set B contains a q^{th} power modulo p.*
3. *For each sequence of integers $\{c_j\}_{j=1}^{l}$, there exists a sequence of integers $\{f_j\}_{j=1}^{l}$ such that*

$$\sum_{j=1}^{l} f_j \not\equiv 0 \pmod{q} \text{ and } \prod_{j=1}^{l} b_j^{c_j f_j} = d^q \text{ for some integer } d. \tag{1.1}$$

This article focuses on extremal sizes and multiplicative structure of locally q^{th} power sets. We bridge number theory and finite geometry by providing a geometric characterization of locally q^{th} power sets. Specifically, we show that locally q^{th} power sets B correspond to blocking sets (with respect to hyperplanes) in projective space $\mathrm{PG}(\mathbb{F}_q^k)$. Here, k is equal to the number of distinct primes dividing the q-free parts of elements of B (see Section 3). This geometric characterization allows us to introduce the notion of *geometric q-equivalence*, which, we will establish, is an equivalence relation between locally q^{th} power sets. This allows us to construct and recognize locally q^{th} power sets from existing ones (see Section 4). Moreover, our methods enable us to study subtler details of locally q^{th} power sets such as their dimensions and lower and upper bounds on their cardinalities. In some cases, classifications of minimum size locally q^{th} power sets are also provided (see Sections 5, 6 and 7).

Acknowledgments. The authors are very grateful to the reviewer for their invaluable comments and suggestions, which have significantly improved the exposition of this article.

2. Preliminaries

Given a prime p, an integer $\nu \geq 1$ and $a \in \mathbb{Z}$, we write $p^{\nu} \mid\mid a$, if p^{ν} is the highest power of p dividing a. In this article, q will always denote a fixed odd prime.

2.1. Reduction to the positive q-free equivalence class. Let $B = \{b_1, b_2, \ldots, b_\ell\}$ be a finite subset of integers. For any prime p, an integer b is a q^{th} power modulo p if and only if $|b|$ is a q^{th} power modulo p. This is because -1 is always a perfect q^{th} power. Therefore, we can replace the set B by the set $\{|b_j|\}_{j=1}^{\ell}$.

Given a positive integer b with unique prime factorization $\prod_{j=1}^{k} p_j^{a_j}$ ($a_j \geq 1$), its *q-free part* is denoted by $\mathrm{rad}_q(b)$, and can be defined as

$$\mathrm{rad}_q(b) := \prod_{j=1}^{k} p_j^{a_j \pmod q}.$$

For a prime $p \neq q$ and $p \nmid b$, b is a q^{th} power modulo p if and only if $\mathrm{rad}_q(b)$ is a q^{th} power modulo p. Since there are only finitely many primes dividing p that divide $\prod_{b \in B} b$, we can see that a set $B = \{b_j\}_{j=1}^{\ell} \subset \mathbb{Z}$ contains a q^{th} power modulo almost every prime if and only if the set $\{\mathrm{rad}_q(|b_j|)\}_{j=1}^{\ell}$ contains a q^{th} power modulo almost every prime. Therefore, we introduce an equivalence relation $\sim_q$ on the set $\mathbb{Z} \setminus \{0\}$ defined as follows:

Let b_1, b_2 be two non-zero integers and $p_1, p_2, \ldots, p_k$ be all the primes dividing $b_1 b_2$. Let $b_1 = \pm \prod_{i=1}^{k} p_i^{\mu_i}$ ($\mu_i \geq 0$) and $b_2 = \pm \prod_{i=1}^{k} p_i^{\nu_i}$ ($\nu_i \geq 0$). We will say that

$$b_1 \sim_q b_2 \text{ if and only if } \mu_i \equiv \nu_i \pmod q \text{ for every } 1 \leq i \leq k.$$

$\sim_q$ is clearly an equivalence relation, where the equivalence class containing an integer b will be denoted by $[b]_q$. Let $\mathscr{Z}$ be the set of equivalence classes and

$$\pi_q : \mathbb{Z} \setminus \{0\} \to \mathscr{Z}$$

be the canonical map that takes an integer b to its equivalence class $[b]_q$. Note that $b \sim_q \mathrm{rad}_q(|b|)$ for every integer b, and therefore we will often identify $[b]_q$ with $\mathrm{rad}_q(|b|)$.

Therefore, to study whether a given finite subset $B = \{b_j\}_{j=1}^{\ell} \subset \mathbb{Z} \setminus \{0\}$ is a locally q^{th} power set, it suffices to investigate whether $\pi_q(B) = \{\mathrm{rad}_q(|b_j|)\}_{j=1}^{\ell} \subset \mathcal{Z}$ is a locally q^{th} power set. Moreover, if B is a locally q^{th} power set, then every set A, with $A \supset B$, is also a locally q^{th} power set. Keeping this in mind, we introduce the following definition:

Definition 2.1. An element b of a locally q^{th} power set B is said to be *essential* if the set $B \setminus \{b\}$ is no longer a locally q^{th} power set. We will say that a locally q^{th} power set B is minimal if every element of B is essential.

Clearly, if B has two distinct elements c and d such that $c \sim_q d$, then B cannot be minimal. Therefore, we have the following immediate assertion.

Lemma 2.2. *If a finite subset B of non-zero integers is a minimal locally q^{th} power set, then $|B| = |\pi_q(B)|$.*

Following is an example of a minimal locally 3^{rd} power set.

Example 2.3. Let $q = 3$, p_1, p_2 be two distinct primes and consider the set

$$B = \{p_1, p_2, p_1p_2, p_1p_2^2\}.$$

One can easily see that the set B is a locally 3^{rd} power set. If neither p_1 nor p_2 is cube modulo p then, two cases arise in $G = \mathbb{F}_p^{\times}/\mathbb{F}_p^{\times 3}$:

(1) Both p_1 and p_2 are the same non-identity element in G. In this case, $p_1p_2^2$ is a cube modulo p.
(2) If not, p_1 and p_2 are distinct in G, in which case, p_1p_2 is a cube modulo p.

In either case, B is a locally 3^{rd} power set since it contains a cube modulo p for every prime $p \notin \{3, p_1, p_2\}$. Since every locally 3^{rd} power set has at least four elements (for instance, see [11, Corollary 1, pp. 10]), it also follows that B is minimal locally 3^{rd} power set. In fact, we will establish in this article that all minimal locally q^{th} power sets are of the form

$$C := \{p_1, p_2, p_1p_2, p_1p_2^2, \ldots, p_1p_2^{q-1}\}$$

up to a suitable equivalence. The equivalence is needed since, for instance, any element in C could be modified by a perfect q^{th} power multiple and the resulting set would still remain a locally q^{th} power set.

2.2. Blocking sets. Let $\mathbb{K}$ be a field and V be a vector space over $\mathbb{K}$. Let $\mathrm{PG}(V, \mathbb{K})$ be the projective space defined over $\mathbb{K}$ by V. In this article, $\mathbb{K}$ will always be the Galois field $\mathbb{F}_q$ of order q. Therefore, we will abbreviate $\mathrm{PG}(V, \mathbb{F}_q)$ as $\mathrm{PG}(V)$.

Definition 2.4. Let $k \geq 2$. A *blocking set* $\mathcal{S}$ (with respect to hyperplanes) of $\mathrm{PG}(\mathbb{F}_q^k)$ is a collection of points that meets every hyperplane in at least one point.

Any line in $\mathrm{PG}(\mathbb{F}_q^k)$ is a blocking set, and any blocking set that contains a line will be called a *trivial* blocking set. Similar to the case of locally q^{th} power set, we define minimal blocking sets as follows.

Definition 2.5. A point $\mathcal{P}$ of a blocking set $\mathcal{S}$ of $\mathrm{PG}(\mathbb{F}_q^k)$ is said to be *essential* if $\mathcal{S} \setminus \{\mathcal{P}\}$ is no longer a blocking set, i.e. there is a hyperplane of $\mathrm{PG}(\mathbb{F}_q^k)$ meeting $\mathcal{S}$ in $\mathcal{P}$ only. Hence a blocking set is *minimal* if and only if every point is essential. Equivalently a blocking set is minimal if it does not properly contain a blocking set.

Readers can also consult [3] for an excellent survey on the topic. We will say that a blocking set $\mathcal{S}$ of $\mathrm{PG}(\mathbb{F}_q^k)$ is r-dimensional if the projective subspace of $\mathrm{PG}(\mathbb{F}_q^k)$ generated by $\mathcal{S}$ has dimension r, In the case $r = 2$, we say that $\mathcal{S}$ is planar, i.e., if the projective subspace generated by $\mathcal{S}$ is a plane of $\mathrm{PG}(\mathbb{F}_q^k)$. We note that if W is a subspace of $\mathbb{F}_q^k$, then any blocking set of $\mathrm{PG}(W)$ is also a blocking set of $\mathrm{PG}(\mathbb{F}_q^k)$.

3. Blocking Sets and Locally q^{th}-Power Sets

Before we can characterize locally q^{th} power sets in terms of blocking sets, we will need a few notation.

3.1. Point set associated to a finite subset of integers. Let $B = \{b_j\}_{j=1}^{\ell}$ be a finite subset of non-zero integers not containing any perfect q^{th} power. Let $p_1 < p_2 < \ldots < p_k$ be all the distinct primes that divide any element of $\pi_q(B)$. For every $1 \leq i \leq k$ and for every $1 \leq j \leq \ell$, let $\nu_{ij} \geq 0$ be such that $p_i^{\nu_{ij}} \mid\mid \mathrm{rad}_q(|b_j|)$. For every $1 \leq j \leq \ell$, let $\mathcal{P}_j = \langle(\nu_{1j}, \nu_{2j}, \ldots, \nu_{kj})\rangle \in \mathrm{PG}(\mathbb{F}_q^k)$. The set $\{\mathcal{P}_j\}_{j=1}^{\ell} \subset \mathrm{PG}(\mathbb{F}_q^k)$ will be called the point set (in $\mathrm{PG}(\mathbb{F}_q^k)$) associated to $B \subset \mathbb{Z} \setminus \{0\}$. Our first result is the following:

Theorem 3.1. *Let B be a finite subset of non-zero integers not containing a perfect q^{th} power and let k be the total number of primes dividing $\prod_{b \in B} \mathrm{rad}_q(|b_j|)$. Then, the following two statements are equivalent:*

(1) *The set B is a locally q^{th} power set.*
(2) *The point set $\{\mathcal{P}_j\}_{j=1}^{\ell}$, associated to B, forms a blocking set in $\mathrm{PG}(\mathbb{F}_q^k)$.*

In order to prove Theorem 3.1, we will use a characterization of locally q^{th} power sets in terms of linear hyperplane coverings of vector spaces, obtained by the first author in [11].

Let V be a vector space of dimension ≥ 2 over a field $\mathbb{K}$. A collection $\{W_i\}_{i \in I}$ of proper $\mathbb{K}$-subspaces is said to be a *linear covering* if $V = \bigcup_{i \in I} W_i$.

3.2. Hyperplanes Associated with a Finite Subset. Let $B = \{b_j\}_{j=1}^{\ell}$ be a finite subset of non-zero integers. Let $p_1, p_2, \ldots, p_k$ be all the primes that divide any element of $\pi_q(B)$. For every $1 \leq i \leq k$ and for every $1 \leq j \leq \ell$, let $\nu_{ij} \geq 0$ be such that $p_i^{\nu_{ij}} \mid\mid \operatorname{rad}_q(b_j)$. For every $1 \leq j \leq \ell$, define the $\mathcal{H}_j$ as,

$$\mathcal{H}_j := \left\{ (x_i)_{i=1}^{k} \in \mathbb{F}_q^k : \sum_{i=1}^{k} \nu_{ij} x_i = 0 \right\}.$$

We will say that $\{\mathcal{H}_j\}_{j=1}^{\ell}$ is the set of hyperplanes (in $\mathbb{F}_q^k$) associated with the set B. Proposition 1.2 was further simplified in terms of linear covering in [11].

Proposition 3.2. *Let q be an odd prime, $B = \{b_j\}_{j=1}^{\ell}$ be a finite subset of non-zero integers that does not contain a perfect q^{th} power. Then, the following two statements are equivalent.*

(1) *B is a locally q^{th} power set.*
(2) *$\bigcup_{j=1}^{\ell} \mathrm{PG}(\mathcal{H}_j) = \mathrm{PG}(\mathbb{F}_q^k)$ $\left(\text{or equivalently } \bigcup_{j=1}^{\ell} \mathcal{H}_j = \mathbb{F}_q^k\right)$, where $\{\mathcal{H}_j\}_{j=1}^{\ell}$ is the set of hyperplanes associated with B.*

3.3. Proof of Theorem 3.1. From now on, we consider the projective space $\mathrm{PG}(\mathbb{F}_q^k)$ together with a coordinatization $(x_1, \ldots, x_k)$. We also consider the following duality $\perp$ on $\mathrm{PG}(\mathbb{F}_q^k)$. To any projective subspace $\Omega = \mathrm{PG}(W)$, we associate $\Omega^{\perp} = \mathrm{PG}(W^{\perp})$, where

$$W^{\perp} = \left\{ (u_1, \ldots, u_k) \in \mathbb{F}_q^k \colon \sum_{i=1}^{k} u_i w_i = 0, \text{for each } (w_1, \ldots, w_k) \in W \right\}.$$

In particular, to a hyperplane $\mathcal{H}$ of $\mathrm{PG}(\mathbb{F}_q^k)$ defined by the equation $v_1 X_1 + \cdots + v_k X_k = 0$ corresponds the point $\mathcal{H}^{\perp} = \langle (v_1, \ldots, v_k) \rangle_{\mathbb{F}_q}$, and conversely. The duality $\perp$ gives is a 1-to-1 correspondence between points and hyperplanes of $\mathrm{PG}(\mathbb{F}_q^k)$ and preserves the incidence, i.e. if $\mathcal{P}$ is a point and $\mathcal{H}$ is a hyperplane of $\mathrm{PG}(\mathbb{F}_q^k)$ then $\mathcal{P} \in \mathcal{H}$ if and only if $\mathcal{H}^{\perp} \in \mathcal{P}^{\perp}$. The dual of a linear covering, with hyperplanes, is a blocking set. We include a statement and its proof for the sake of completeness.

Lemma 3.3. *Let $\ell \in \mathbb{N}$ and for every $1 \leq j \leq \ell$, let $\mathcal{H}_j$ be the hyperplane of $\mathrm{PG}(\mathbb{F}_q^k)$ defined as*

$$\left\{ (x_i)_{i=1}^{k} : \sum_{i=1}^{k} \nu_{ij} x_i = 0 \right\}.$$

Then, the following two statements are equivalent:

(1) $\bigcup_{j=1}^{\ell} \mathcal{H}_j = \mathrm{PG}(\mathbb{F}_q^k)$.

(2) *The set* $\mathcal{S} = \{\mathcal{H}_j^{\perp}\}_{j=1}^{\ell}$ *forms a blocking set in* $\mathrm{PG}(\mathbb{F}_q^k)$.

Proof. Let $\mathcal{H}$ be a hyperplane of $\mathrm{PG}(\mathbb{F}_q^k)$. We need to show that $\mathcal{H}$ intersects the set $\mathcal{S}$. Since $\mathcal{P} = \mathcal{H}^{\perp} \in \mathrm{PG}(\mathbb{F}_q^k) = \bigcup_{j=1}^{\ell} \mathcal{H}_j$, we have that $\mathcal{P} \in \mathcal{H}_{j_0}$ for some $1 \leq j_0 \leq \ell$. Since $\perp$ preserves the incidences between points and hyperplanes, $\mathcal{P} \in \mathcal{H}_{j_0}$ implies $\mathcal{H}_{j_0}^{\perp} \in \mathcal{P}^{\perp} = \mathcal{H}$, i.e., $\mathcal{H}_{j_0} \in (\mathcal{H} \cap \mathcal{S})$.

For the proof of the other direction, let $\mathcal{P}$ be a point in $\mathrm{PG}(\mathbb{F}_q^k)$. We want to show that $\mathcal{P} \in \mathcal{H}_{j_0}$ for some $1 \leq j_0 \leq \ell$. Since $\mathcal{S}$ is a blocking set, the hyperplane $\mathcal{H} = P^{\perp}$ in $\mathrm{PG}(\mathbb{F}_q^k)$ must intersect $\mathcal{S}$. In other words, there exists $1 \leq j_0 \leq \ell$ such that $H_{j_0}^{\perp} \in \mathcal{H} = \mathcal{P}^{\perp}$, which gives us $\mathcal{P} \in \mathcal{H}_{j_0}$. □

Since every locally q^{th} power set is associated to a linear covering of $\mathrm{PG}(\mathbb{F}_q^k)$, Theorem 3.1 is a consequence of Proposition 3.2 and Lemma 3.3.

Theorem 3.1 enables us to employ various tools and results from the field of Galois geometry to extract number-theoretic information regarding locally q^{th} power sets. To wrap up this section, we will present few corollaries of Theorem 3.1. The first corollary below demonstrates that the concept of (i) minimal locally q^{th} power set and (ii) minimal blocking set, correspond to one another as expected.

Corollary 3.4. *Using the notations in Theorem 3.1, we have that B is a minimal locally q^{th} power set if and only if the set $\mathcal{S}$ of points in* $\mathrm{PG}(\mathbb{F}_q^k)$ *forms a minimal blocking set of* $\mathrm{PG}(\mathbb{F}_q^k)$ *and* $|\mathcal{S}| = |B|$.

Proof. Note that every element $\mathcal{H}_j^{\perp}$ of $\mathcal{S}$ is associated to an element of B. This corollary is a straightforward consequence of Lemma 2.2 and the fact that the following two statements are equivalent, as a consequence of Theorem 3.1:

- The set $\mathcal{S} \setminus \{\mathcal{H}_{j_0}^{\perp}\}$ is a blocking set of $\mathrm{PG}(\mathbb{F}_q^k)$.
- The set $B \setminus \{b_{j_0}\}$ is a locally q^{th} power set,

see Proposition 3.2. □

Another consequence of Theorem 3.1 is the following lower bound on non-trivial locally q^{th} power sets.

Proposition 3.5 (see [3, Theorem 2.1] and [4])**.** *Let $k \geq 2$. Any blocking set B of* $\mathrm{PG}(\mathbb{F}_q^k)$ *has at least $q+1$ points. In case of equality the blocking set is the point set of a line.*

As a consequence, in unison with Theorem 3.1, we obtain the following corollary that was also proved in [11].

Corollary 3.6. *A subset B of integers, with cardinality at most q, contains a q^{th} power modulo almost every prime if and only if B contains a perfect q^{th} power. In particular, any locally q^{th} power set has size at least $q+1$.*

4. Geometric q-Equivalence

To start the discussion pertaining to this section, consider the following proposition that shows that the property of a finite subset of integers to be a locally q^{th} power set is invariant under exponentiation by elements of $\mathbb{F}_q \setminus \{0\}$ in the following sense.

Proposition 4.1 (see [11, Corollary 2])**.** *Let $B = \{b_j\}_{j=1}^{\ell}$ be a finite subset of integers. Given $\vec{c} = (c_j)_{j=1}^{\ell} \in \left(\mathbb{F}_q \setminus \{0\}\right)^l$, define $B^{\vec{c}} = \{b_j^{c_j}\}_{j=1}^{\ell}$. B is a locally q^{th} power set if and only if $B^{\vec{c}}$ is a locally q^{th} power set for every $\vec{c} \in \mathbb{F}_q \setminus \{0\}$.*

Element-wise exponentiation in Proposition 4.1 is a particular instance of a much more general set of transformations, that we will call *geometric q-equivalence.* In this section, we will explain geometric q-equivalence and show that the property of being a locally q^{th} power set is invariant under it. We will denote the projective general linear group of degree k over $\mathbb{F}_q$ by $\mathrm{PGL}(k, q)$.

Definition 4.2. Let $B = \{a_j\}_{j=1}^{m}$ and $B' = \{b_j\}_{j=1}^{\ell}$ be two finite subsets of non-zero integers, not containing a perfect q^{th} power. Let $p_1, p_2, \ldots, p_k$ be all the primes that divide any element of $\pi_q(B) \cup \pi_q(B')$. Let $\mathrm{rad}_q(|a_j|) = \prod_{i=1}^{k} p_i^{\nu_{ij}}$ for every $j \in \{1, 2, \ldots, m\}$ and $\mathrm{rad}_q(|b_j|) = \prod_{i=1}^{k} p_i^{\mu_{ij}}$ for every $j \in \{1, 2, \ldots, \ell\}$, where $\nu_{ij}, \mu_{ij} \geq 0$. Define

$$\mathcal{S} = \{\langle(\nu_{1j}, \nu_{2j}, \ldots, \nu_{kj})\rangle_{\mathbb{F}_q} \in \mathrm{PG}(\mathbb{F}_q^k) : j \in \{1, 2, \ldots, m\}\} \text{ and}$$
$$\mathcal{S}' = \{\langle(\mu_{1j}, \mu_{2j}, \ldots, \mu_{kj})\rangle_{\mathbb{F}_q} \in \mathrm{PG}(\mathbb{F}_q^k) : j \in \{1, 2, \ldots, \ell\}\}$$

to be the point sets in $\mathrm{PG}(\mathbb{F}_q^k)$ associated to B and B' respectively. We will say that the sets B and B' are *geometrically q-equivalent* if and only if there exists an element $\Psi \in \mathrm{PGL}(k, q)$ such that $\Psi(\mathcal{S}) = \mathcal{S}'$.

Our next result shows that property whether a given finite $B \subset \mathbb{Z} \setminus \{0\}$, is a locally q^{th} power set is preserved by geometric q-equivalence.

Theorem 4.3. *Let $B = \{b_1, b_2, \ldots, b_t\} \subset \mathbb{Z} \setminus \{0\}$ be a set of integers not containing a perfect q^{th} power. Then B is a locally q^{th} power set if and only if every set B' that is geometrically q-equivalent to B is a locally q^{th} power set, as well.*

Proof. We will show that if B is a locally q^{th} power set, then every set B' that is geometrically q-equivalent to B is also a locally q^{th} power set. The converse holds trivially.

Let $\{p_1, \dots, p_s\}$ be the set of all prime numbers dividing the elements of

$$\pi_q(B) = \{\mathrm{rad}_q(b_1), \dots, \mathrm{rad}_q(b_t)\}$$

such that $p_i^{v_{ij}} \mid\mid \mathrm{rad}_q(b_j)$, for every $1 \leq i \leq s$ and every $1 \leq j \leq t$. By Lemma 3.3, the set of points $\mathcal{S} = \{\mathcal{P}_1, \dots, \mathcal{P}_t\} \subseteq \mathrm{PG}(\mathbb{F}_q^s)$, where

$$\mathcal{P}_j = \langle (v_{1j}, \dots, v_{sj}) \rangle_{\mathbb{F}_q},$$

for each $1 \leq j \leq t$, is a blocking set of $\mathrm{PG}(\mathbb{F}_q^s)$. First, assume that B' is a geometrically q-equivalent set to B and let $\pi_q(B') = \{a_1, \dots, a_l\}$. Let $p_{s+1}, \dots, p_k$, with $k \geq s$ be some primes such that $\{p_1, \dots, p_s, p_{s+1}, \dots, p_k\}$ is the set of all the primes that divides the elements of $B \cup B'$. Suppose that $|a_j| = \prod_{i=1}^k p_i^{w_{ij}}$, for $j \in \{1, \dots, l\}$ and $|b_h| = \prod_{i=1}^k p_i^{v_{ih}}$, for $h \in \{1, \dots, t\}$ (Note that $v_{ij} = 0$, if $i \geq s+1$). Since, B' is geometrically q-equivalent to B then there exists an element $\Psi \in \mathrm{PGL}(k, q)$, such that

$$\Psi(\mathcal{S}) = \mathcal{S}',$$

where $\mathcal{S} = \{\langle (w_{1j}, \dots, w_{kj}) \rangle_{\mathbb{F}_q} : j \in \{1, \dots, l\}\}$ and $\mathcal{S}' = \{\langle (v_{1h}, \dots, v_{kh}) \rangle_{\mathbb{F}_q} : h \in \{1, \dots, t\}\}$. Since the $\mathcal{P}_j$'s form a blocking set of $\mathrm{PG}(\mathbb{F}_q^s)$, they define also a blocking set in $\mathrm{PG}(\mathbb{F}_q^k)$, because $k \geq s$, and hence $\mathcal{S}$ is a blocking set in $\mathrm{PG}(\mathbb{F}_q^k)$. The property of being a blocking set is invariant under the action of $\mathrm{PGL}(k, q)$ on $\mathrm{PG}(\mathbb{F}_q^k)$, and then we get that also $\mathcal{S}'$ is a blocking set. Again by Theorem 3.3, we have that B' is a q^{th}-power set, and then the assertion follows. □

One benefit of Theorem 4.3 is that one can systematically study locally q^{th} power sets according to the number of distinct primes that divide them. Assume that the point set of $\mathrm{PG}(\mathbb{F}_q^k)$ associated to the set $B \subset \mathbb{Z} \setminus \{0\}$ lie in a proper subspace of $\mathrm{PG}(\mathbb{F}_q^k)$. In this case, B is geometrically q-equivalent to a set B' that is divisible by fewer primes. We will demonstrate this first using an illustrative example.

Example 4.4. Choose $q = 7$. Let

$$\begin{aligned} B &= \{2, 15, 30, 60, 120, 240, 480, 960\} \\ &= \{2, 3 \cdot 5, 2 \cdot 3 \cdot 5, 2^2 \cdot 3 \cdot 5, 2^3 \cdot 3 \cdot 5, 2^4 \cdot 3 \cdot 5, 2^5 \cdot 3 \cdot 5, 2^6 \cdot 3 \cdot 5\} \end{aligned}$$

The set of all primes that divide an element of B is $\{2, 3, 5\}$. The set B defines the points

$$\begin{aligned} \mathcal{P} = \Big\{ &\langle (1,0,0) \rangle_{\mathbb{F}_q}, \langle (0,1,1) \rangle_{\mathbb{F}_q}, \langle (1,1,1) \rangle_{\mathbb{F}_q}, \langle (2,1,1) \rangle_{\mathbb{F}_q}, \\ &\qquad \langle (3,1,1) \rangle_{\mathbb{F}_q}, \langle (4,1,1) \rangle_{\mathbb{F}_q}, \langle (5,1,1) \rangle_{\mathbb{F}_q}, \langle (6,1,1) \rangle_{\mathbb{F}_q} \Big\} \end{aligned}$$

in $\mathrm{PG}(\mathbb{F}_7^3)$, which is the line of $\mathrm{PG}(\mathbb{F}_7^3)$ through the points $\langle(1,0,0)\rangle_{\mathbb{F}_q}$ and $\langle(0,1,1)\rangle_{\mathbb{F}_q}$. Consider

$$A=\begin{pmatrix}1&0&0\\0&1&0\\0&1&6\end{pmatrix}\in\mathrm{PGL}(3,7).$$

The set $\mathcal{P}$ is mapped to the set

$$\mathcal{P}'=\Big\{\langle(1,0,0)\rangle_{\mathbb{F}_q},\langle(0,1,0)\rangle_{\mathbb{F}_q},\langle(1,1,0)\rangle_{\mathbb{F}_q},\langle(2,1,0)\rangle_{\mathbb{F}_q},\\ \langle(3,1,0)\rangle_{\mathbb{F}_q},\langle(4,1,0)\rangle_{\mathbb{F}_q},\langle(5,1,0)\rangle_{\mathbb{F}_q},\langle(6,1,0)\rangle_{\mathbb{F}_q}\Big\}$$

by the element of $\mathrm{PGL}(3,7)$ induced by matrix A. Note that $\mathcal{P}'$ is associated to the set

$$B'=\{2,3,2\cdot 3,2^2\cdot 3,2^3\cdot 3,2^4\cdot 3,2^5\cdot 3,2^6\cdot 3\}=\{2,3,6,12,24,48,96,192\}.$$

that is divisible only by primes 2 and 3. To summarize, B is geometrically 7-equivalent to a set B', which is only divisible by 2 primes. This is because $\mathcal{P}$ spans a proper subspace of $\mathrm{PG}(\mathbb{F}_7^3)$.

Consider the following definition.

Definition 4.5. Let $B\subset\mathbb{Z}\setminus\{0\}$ be a finite set of integers and assume that there are exactly k distinct primes dividing any element of $\pi_q(B)$. For a positive integer $d\leq k-1$, we will say that B is d-dimensional if the point set in $\mathrm{PG}(\mathbb{F}_q^k)$ associated to B spans a d-dimensional subspace.

Since k counts the number of distinct primes dividing the elements of $\pi_q(B)$, one expects that if B is d-dimensional, B must ultimately be made up of $(d+1)$ primes. This is essentially the case, up to geometric q-equivalence, which is the content of the next proposition.

Proposition 4.6. *Consider $B=\{b_1,b_2,\ldots,b_t\}\subset\mathbb{Z}\setminus\{0\}$ be a set of integers not containing a perfect q^{th} power and assume that B is $(r-1)$-dimensional. Then, for any choice of r different primes $\overline{p}_1,\ldots,\overline{p}_r$, there exists a set B', that is geometrically q-equivalent to B, such that $\{\overline{p}_1,\ldots,\overline{p}_r\}$ is the set of all the primes numbers that divides at least one element of B'.*

Proof. Let $\{p_1,\ldots,p_k\}$ be the set of all prime numbers diving the elements of

$$\pi_q(B)=\{\mathrm{rad}_q(b_1),\ldots,\mathrm{rad}_q(b_t)\}$$

such that $p_i^{v_{ij}}\ ||\ \mathrm{rad}_q(b_j)$, for every $1\leq i\leq k$ and every $1\leq j\leq t$. And consider the set of points $\mathcal{S}=\{\mathcal{P}_1,\ldots,\mathcal{P}_t\}\subseteq\mathrm{PG}(\mathbb{F}_q^k)$, where

$$\mathcal{P}_j=\langle(v_{1j},\ldots,v_{kj})\rangle_{\mathbb{F}_q},$$

for each $1\leq j\leq t$. Since B is $(r-1)$-dimensional, the projective subspace $\langle\mathcal{S}\rangle$, generated by $\mathcal{S}$ has dimension $r-1$. Let Ψ be the element of

$\mathrm{PGL}(k,q)$ mapping $\langle\mathcal{S}\rangle$ in the $(r-1)$-dimensional subspace of $\mathrm{PG}(\mathbb{F}_q^k)$ having equation $X_{r+1} = \ldots = X_k = 0$. In other words, $\Psi(\mathcal{S}) = \mathcal{S}'$, where $\mathcal{S}' = \{\mathcal{Q}_1, \ldots, \mathcal{Q}_t\} \subseteq \mathrm{PG}(\mathbb{F}_q^k)$, where

$$\mathcal{Q}_j = \langle(w_{1j}, \ldots, w_{kj})\rangle_{\mathbb{F}_q},$$

for each $1 \le j \le t$, with the properties that $w_{ij} = 0$, if $i \ge r+1$. So the set

$$B' = \left\{\prod_{i=1}^{r} p_i^{w_{i1}}, \ldots, \prod_{i=1}^{r} p_i^{w_{it}}\right\}$$

is geometrically q-equivalent to B, having the desired property. □

In certain cases, Proposition 4.6 can be employed to show that a given set is not a locally q^{th} power set. Consider the following example:

Example 4.7. Choose $q = 7$. Let

$$B = \{2, 3, 4, 5, 6, 10, 15, 25\} = \{2, 3, 2^2, 5, 2\cdot 3, 2\cdot 5, 3\cdot 5, 5^2\},$$

which has 8 elements. The set of all primes that divide an element of B is $\{2, 3, 5\}$. The point set

$$\mathcal{S} = \Big\{\langle(1,0,0)\rangle_{\mathbb{F}_q}, \langle(0,1,0)\rangle_{\mathbb{F}_q}, \langle(2,0,0)\rangle_{\mathbb{F}_q}, \langle(0,0,1)\rangle_{\mathbb{F}_q}, \\ \langle(1,1,0)\rangle_{\mathbb{F}_q}, \langle(1,0,1)\rangle_{\mathbb{F}_q}, \langle(0,1,1)\rangle_{\mathbb{F}_q}, \langle(0,0,2)\rangle_{\mathbb{F}_q}\Big\}$$

in $\mathrm{PG}(\mathbb{F}_7^3)$ is associated to B. However, as a point set in $\mathrm{PG}(\mathbb{F}_7^3)$

$$\mathcal{S} = \Big\{\langle(1,0,0)\rangle_{\mathbb{F}_q}, \langle(0,1,0)\rangle_{\mathbb{F}_q}, \langle(0,0,1)\rangle_{\mathbb{F}_q}, \\ \langle(1,1,0)\rangle_{\mathbb{F}_q}, \langle(1,0,1)\rangle_{\mathbb{F}_q}, \langle(0,1,1)\rangle_{\mathbb{F}_q}\Big\}$$

and hence, B is geometrically q-equivalent to

$$B' = \{2, 3, 5, 2\cdot 3, 2\cdot 5, 3\cdot 5\} = \{2, 3, 5, 6, 10, 15\}.$$

Now the size of B' is $6 < 7$. Therefore, Proposition 3.6 implies that the set B' is not a locally 7^{th} power set, and hence using Theorem 4.3, B is not a locally 7^{th} power set.

5. Classification and bounds of locally q^{th} power set

In this section, we will classify the locally q^{th} power sets based on their cardinality and the shape of their elements. For instance, we describe the minimal locally q^{th} power sets of smallest cardinality $q+1$. Next, we will describe the minimal locally q^{th} power set of second smallest cardinality. Here, our starting point is the following well-known result.

Proposition 5.1 (see [2, 9])**.** *For q an odd prime, let $\mathcal{S}$ be a non-trivial blocking set of* $\mathrm{PG}(\mathbb{F}_q^k)$*, then $|\mathcal{S}| \geq \frac{3(q+1)}{2}$. In the case of equality the blocking set is planar.*

We also prove that the bound $|B| \geq 3(q+1/2)$ is sharp, for any q odd prime, completely classifying minimal locally q^{th}-power set in the case of the second smallest size $|B| = 3(q+1)/2$ for $q = 3, 5$.

Theorem 5.2. *Let $B = \{b_1, \ldots, b_\ell\}$ be a locally q^{th} power set and $\mathcal{S}$ be the point set in* $\mathrm{PG}(\mathbb{F}_q^k)$ *associated to B. Here, k is the number of distinct primes dividing $\prod_{j=1}^{\ell} \pi_q(b_j)$. Then, $|B| \geq q+1$ and the following holds:*

(i) *The cardinality of B is $q+1$ if and only if $\mathcal{S}$ is a line of* $\mathrm{PG}(\mathbb{F}_q^k)$ *and B is geometrically q-equivalent to the set*

$$\{\overline{p}_1, \overline{p}_2, \overline{p}_1\overline{p}_2, \overline{p}_1\overline{p}_2^2, \ldots, \overline{p}_1\overline{p}_2^{q-1}\}, \tag{5.1}$$

for two distinct primes $\overline{p}_1, \overline{p}_2$. In this case, B is 1-dimensional and minimal.

(ii) *Minimal locally q^{th} power sets of cardinality strictly between $q+1$ and $\frac{3(q+1)}{2}$ do not exist. In particular, $q+1 < |B| < \frac{3(q+1)}{2}$ if and only if B contains a proper subset that is geometrically q-equivalent to* (5.1)*.*

(iii) *B is minimal and $|B| = \frac{3(q+1)}{2}$ if and only if B is 2-dimensional, i.e., $\mathcal{S}$ is a blocking set of a plane* $\mathrm{PG}(\mathbb{F}_q^2)$ *of* $\mathrm{PG}(\mathbb{F}_q^k)$*.*

Proof. Since B is a q^{th} power set, Theorem 3.1 implies that $\mathcal{S}$ is a blocking set of $\mathrm{PG}(\mathbb{F}_q^k)$. In this case, $|B| \geq q+1$ follows from Proposition 3.5.

If $|B| = q+1$, then Proposition 3.5 again implies that $\mathcal{S}$ is a line of $\mathrm{PG}(\mathbb{F}_q^k)$. So $\mathcal{S} = \mathrm{PG}(1, q)$ and B is 1-dimensional.

When $|B|$ lies strictly between $q+1$ and $\frac{3(q+1)}{2}$, and when $|B| = \frac{3(q+1)}{2}$ the result follows from Proposition 5.1. □

Now we present two examples that demonstrate how Theorem 5.2 can be employed to obtain results about locally q^{th} power sets.

Example 5.3. Suppose we want to investigate whether the set $B = \{2, 3, 4, 6, 21, 41\}$ is a locally q^{th} power set for $q = 5$. Note that $B = \{2, 3, 2^2, 2 \cdot 3, 3 \cdot 7, 2 \cdot 3 \cdot 7\}$ has size 6. So by Theorem 5.2, we have that B is a q^{th} power set if and only if the point set

$$\mathcal{S} = \Big\{ \langle(1,0,0)\rangle_{\mathbb{F}_q}, \langle(0,1,0)\rangle_{\mathbb{F}_q}, \langle(2,0,0)\rangle_{\mathbb{F}_q}, \\ \langle(1,1,0)\rangle_{\mathbb{F}_q}, \langle(0,1,1)\rangle_{\mathbb{F}_q}, \langle(1,1,1)\rangle_{\mathbb{F}_q} \Big\}$$

defines a line of $\mathrm{PG}(\mathbb{F}_5^3)$. However, the subspace generated by $\mathcal{S}$ must contain $\langle(1,0,0)\rangle_{\mathbb{F}_q}$, $\langle(0,1,0)\rangle_{\mathbb{F}_q}$, $\langle(0,1,1)\rangle_{\mathbb{F}_q}$; so, $\mathcal{S}$ generates the whole space $\mathrm{PG}(\mathbb{F}_5^3)$. In other words, $\mathcal{S}$ is not a line and B is not a locally 5^{th} power set.

Example 5.4. Similarly, $B = \{6, 7, 42, 252, 1512, 18114\} = \{2 \cdot 3, 7, 2 \cdot 3 \cdot 7, 2^2 \cdot 3^2 \cdot 7, 2^3 \cdot 3^3 \cdot 7, 2^4 \cdot 3^4 \cdot 7\}$ has size 6. So by Theorem 5.2, B is a locally 5^{th} power set, because the associated point set

$$\langle(1,1,0)\rangle_{\mathbb{F}_q}, \langle(0,0,1)\rangle_{\mathbb{F}_q}, \langle(1,1,1)\rangle_{\mathbb{F}_q}, \langle(2,2,1)\rangle_{\mathbb{F}_q}, \langle(3,3,1)\rangle_{\mathbb{F}_q}, \langle(4,4,1)\rangle_{\mathbb{F}_q}$$

defines the line of $\mathrm{PG}(\mathbb{F}_q^3)$ through the points $\langle(1,1,0)\rangle_{\mathbb{F}_q}$ and $\langle(0,0,1)\rangle_{\mathbb{F}_q}$.

Note that Theorem 5.2 says that 1-dimensional locally q^{th} power set having size $q+1$ are associated to a line in the projective space. In the same spirit, in the next we investigate minimal 2-dimensional locally q^{th} power sets, which have cardinality $\frac{3(q+1)}{2}$. We provide constructions of such sets for every odd prime q. We will then show that, unlike the case of locally q^{th} power sets of size $q+1$, here it is possible to give inequivalent constructions. Therefore, this shows that the structure of such sets depends on the value of q. Finally, we classify these sets for small values of q. We will introduce some preliminary definitions and facts before doing so.

Definition 5.5. A *projective triangle* in $\mathrm{PG}(\mathbb{F}_q^3)$, is a set $\mathcal{S}$ of $\frac{3(q+1)}{2}$ points such that:

(1) there exist three non collinear points $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ such that on each side of the triangle $\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$ (i.e. $\mathcal{S} \cap \mathcal{P}_i\mathcal{P}_j$, with $i \neq j$), there are exactly $\frac{q-1}{2} + 2$ points of $\mathcal{S}$;

(2) the vertices $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ are in $\mathcal{S}$;

(3) for $\{i, j, k\} = \{1, 2, 3\}$, the line connecting a point of $\mathcal{S} \cap \mathcal{P}_i\mathcal{P}_j$, with a point of $\mathcal{S} \cap \mathcal{P}_j\mathcal{P}_k$ also contain a point of $\mathcal{S} \cap \mathcal{P}_i\mathcal{P}_k$.

A projective triangle is a minimal blocking set of $\mathrm{PG}(\mathbb{F}_q^3)$ having size reaching the equality in Proposition 5.1.

Proposition 5.6 (see [10, Lemma 13.6 (i)])**.** *Any projective triangle is a minimal non-trivial blocking set of* $\mathrm{PG}(\mathbb{F}_q^3)$ *having size* $\frac{3(q+1)}{2}$.

A construction of such a point set is the following. Denote by Q the set of non zero square elements of $\mathbb{F}_q$, i.e.

$$Q := (\mathbb{F}_q^*)^2 = \{a^2 \colon a \in \mathbb{F}_q^*\}.$$

Recall that if q is odd then $|Q| = \frac{q-1}{2}$.

Proposition 5.7 (see [10, Lemma 13.6 (i)]). *Let q be an odd prime. The point set*

$$\mathcal{S} = \{\langle(0,1,-s)\rangle_{\mathbb{F}_q}, \langle(-s,0,1)\rangle_{\mathbb{F}_q}, \langle(1,-s,0)\rangle_{\mathbb{F}_q} : s \in Q\} \\ \cup \{\langle(1,0,0)\rangle_{\mathbb{F}_q}, \langle(0,1,0)\rangle_{\mathbb{F}_q}, \langle(0,0,1)\rangle_{\mathbb{F}_q}\}$$

in $\mathrm{PG}(\mathbb{F}_q^3)$ *is a projective triangle. In particular, a projective triangle always exists.*

In the next proposition, we show that is always possible to construct a minimal locally q^{th} power set for any q as in iii) of Theorem 5.2.

Proposition 5.8. *Let Q be the set of non zero square elements of* $\mathbb{F}_q$. *Let p_1, p_2, p_3 be three distinct primes. The set*

$$B = \{p_2p_3^{q-s}, p_1^{q-s}p_3, p_1p_2^{q-s} : s \in Q\} \cup \{p_1, p_2, p_3\}$$

is a minimal q^{th} power set having size $\frac{3(q+1)}{2}$.

Proof. The point set

$$\mathcal{S} = \{\langle(0,1,-s)\rangle_{\mathbb{F}_q}, \langle(-s,0,1)\rangle_{\mathbb{F}_q}, \langle(1,-s,0)\rangle_{\mathbb{F}_q} : s \in Q\} \\ \cup \{\langle(1,0,0)\rangle_{\mathbb{F}_q}, \langle(0,1,0)\rangle_{\mathbb{F}_q}, \langle(0,0,1)\rangle_{\mathbb{F}_q}\} \subseteq \mathrm{PG}(\mathbb{F}_q^3),$$

associated to B is a projective triangle (see Proposition 5.7). Now, the assertion follows by Theorem 5.2 and Proposition 5.6. □

Example 5.9. For $q = 5$, the set of non-zero squares is $Q = \{1, 4\}$. Hence, the set

$$B = \{p_1, p_2, p_3, p_2p_3^4, p_1^4p_3, p_1p_3, p_1p_2^4, p_1p_2, p_2p_3\}$$

is a minimal locally 5^{th} power set of cardinality 9, according to Proposition 5.8. Here, p_1, p_2 and p_3 are three distinct primes.

6. 2-dimensional Locally q^{th} Power Set

Theorem 5.2 states that a minimal 2-dimensional locally q^{th} power set has cardinality at least $\frac{3(q+1)}{2}$, and in the case of equality the associated point set in $\mathrm{PG}(\mathbb{F}_q^k)$ spans a planar blocking set. In this section, we will classify minimal 2-dimensional locally q^{th} power set for $q \in \{3, 5, 7\}$.

6.1. For $q = 3$.

Proposition 6.1 (see [10, Theorem 13.21]). *A non-trivial minimal blocking set of* $\mathrm{PG}(\mathbb{F}_3^3)$ *has size* 6 *and it is a projective triangle, that is unique up to the action of* $\mathrm{PGL}(3, 3)$.

As a consequence, we get that, up to the action of $\mathrm{PGL}(3, 3)$, the only minimal blocking set of $\mathrm{PG}(2, 3)$, is that described in Proposition 5.7.

Proposition 6.2. *Let $q = 3$ and B be a minimal locally 3^{rd} power set and $\mathcal{S}$ be the point set in $\mathrm{PG}(\mathbb{F}_q^k)$ associated to B. Then, $|B| = \frac{3(q+1)}{2} = 6$ if and only if $\mathcal{S}$ is geometrically q-equivalent to the set*

$$\{\overline{p}_1, \overline{p}_2, \overline{p}_3, \overline{p}_1\overline{p}_2^2, \overline{p}_1\overline{p}_3^2, \overline{p}_2\overline{p}_3^2\},$$

for three distinct primes $\overline{p}_1, \overline{p}_2, \overline{p}_3$.

6.2. For $q = 5$. We classify all the q^{th} power set having the second minimum size $3(q+1)/2 = 9$. We start by recalling the following classification theorem for blocking sets of $\mathrm{PG}(\mathbb{F}_5^3)$.

Proposition 6.3 (see [10, Theorem 13.25] and [6, Section 3])**.** *A non-trivial minimal blocking set of $\mathrm{PG}(\mathbb{F}_5^3)$ of minimum size 9 is a projective triangle, that is unique up to the action of $\mathrm{PGL}(3,5)$.*

As a consequence, we get that, up to the action of $\mathrm{PGL}(3,5)$, the only minimal blocking set of $\mathrm{PG}(\mathbb{F}_5^3)$, is that described in Proposition 5.7.

Proposition 6.4. *Let B be a minimal locally 5^{th} power set. Then, $|B| = \frac{3(q+1)}{2}$ if and only if B is geometrically 5-equivalent to the set*

$$\{\overline{p}_1, \overline{p}_2, \overline{p}_3, \overline{p}_1\overline{p}_2, \overline{p}_1\overline{p}_3, \overline{p}_2\overline{p}_3, \overline{p}_1\overline{p}_2^4, \overline{p}_1\overline{p}_3^4, \overline{p}_2\overline{p}_3^4\},$$

for three distinct primes $\overline{p}_1, \overline{p}_2, \overline{p}_3$.

6.3. For $q = 7$. Unlike the case $q \in \{3,5\}$, when $q = 7$, it is possible to find a non-trivial minimal blocking set $\mathcal{S}$ of $\mathrm{PG}(\mathbb{F}_7^3)$, that is not $\mathrm{PGL}(3,7)$-equivalent to the projective triangle. This construction is related to the Hessian configuration of $\mathrm{PG}(\mathbb{F}_7^3)$, that is, the set $\mathcal{C}$ of nine points

$$\mathcal{C} = \left\{ \begin{array}{ccc} (1,-1,0))\rangle_{\mathbb{F}_q}, & \langle(0,1,-1)\rangle_{\mathbb{F}_q}, & \langle(-1,0,1)\rangle_{\mathbb{F}_q} \\ \langle(1,-\omega,0)\rangle_{\mathbb{F}_q}, & \langle(0,1,-\omega)\rangle_{\mathbb{F}_q}, & \langle(-\omega,0,1)\rangle_{\mathbb{F}_q} \\ \langle(1,-\omega^2,0)\rangle_{\mathbb{F}_q}, & \langle(0,1,-\omega^2)\rangle_{\mathbb{F}_q}, & \langle(-\omega^2,0,1)\rangle_{\mathbb{F}_q} \end{array} \right\},$$

where ω is a cubic root of unity in $\mathbb{F}_7$ (for instance, one can take $\omega = 2$). We can find a blocking set of cardinality $\frac{3(7+1)}{2} = 12$, related to the Hessian, in the following way:

There are 12 trisecants $\{\ell_1, \ell_2, \ldots, \ell_{12}\}$ of $\mathcal{C}$, i.e. lines of $\mathrm{PG}(\mathbb{F}_7^3)$ meeting $\mathcal{C}$ in exactly three points. The set of points $\mathcal{S} = \{\ell_1^\perp, \ell_2^\perp, \ldots, \ell_{12}^\perp\}$ forms a non-trivial minimal blocking set of $\mathrm{PG}(2,7)$ having size 12 that is not equivalent under the action of $\mathrm{PGL}(3,q)$ to a projective triangle, see [6, Theorem 4]. A representation of $\mathcal{S}$ is the following

$$\mathcal{S} = \left\{ \begin{array}{cccc} (1,0,0))\rangle_{\mathbb{F}_q}, & \langle(0,1,0)\rangle_{\mathbb{F}_q}, & \langle(0,0,1)\rangle_{\mathbb{F}_q}, & \langle(1,1,1)\rangle_{\mathbb{F}_q} \\ \langle(\omega^2,\omega,1)\rangle_{\mathbb{F}_q}, & \langle(\omega^2,1,\omega)\rangle_{\mathbb{F}_q}, & \langle(\omega,\omega,1)\rangle_{\mathbb{F}_q}, & \langle(1,\omega,1)\rangle_{\mathbb{F}_q} \\ \langle(\omega,1,1)\rangle_{\mathbb{F}_q}, & \langle(\omega,1,\omega)\rangle_{\mathbb{F}_q}, & \langle(1,\omega,\omega)\rangle_{\mathbb{F}_q}, & \langle(1,1,\omega)\rangle_{\mathbb{F}_q} \end{array} \right\}. \tag{6.1}$$

Proposition 6.5 (see [6, Theorem 4])**.** *The point set $\mathcal{S}$ as in* (6.1) *is minimal blocking set of* $\mathrm{PG}(\mathbb{F}_7^3)$ *of minimum size* 12 *that is not* $\mathrm{PGL}(3,7)$ *equivalent to a projective triangle.*

Consequently, we obtain a different behavior of minimal locally 7^{th} power set of the second smallest size $|B| = 3(q+1)/2$, in contrast to the case when $q \in \{3,5\}$ (cf. 6.2 and 6.4).

Theorem 6.6. *Let p_1, p_2, p_3 be three distinct primes and ω be a cubic root of the unity in $\mathbb{F}_7$. Then, the set*

$$B_1 = \{p_1, p_2, p_3, p_1p_2^3, p_1p_3^3, p_2p_3^3, p_1p_2^5, p_1p_3^5, p_2p_3^5, p_1p_2^6, p_1p_3^6, p_2p_3^6\},$$

and the set

$$B_2 = \{p_1, p_2, p_3, p_1p_2p_3, p_1^{\omega^2}p_2^{\omega}p_3, p_1^{\omega^2}p_2p_3^{\omega}, p_1^{\omega}p_2^{\omega}p_3,$$
$$p_1p_2^{\omega}p_3, p_1^{\omega}p_2p_3, p_1^{\omega}p_2p_3^{\omega}, p_1p_2^{\omega}p_3^{\omega}, p_1p_2p_3^{\omega}\}$$

are locally 7^{th} power sets of minimum size $3(q+1)/2 = 12$, that are not geometrically 7-equivalent.

7. 3-dimensional locally q^{th} power set

This last section is to provide insights into 3-dimensional locally q^{th} power sets for $q = 3, 5$.

Proposition 7.1. *Let $q \in \{3,5\}$ and $\mathcal{S}$ be a 3-dimensional minimal blocking set of* $\mathrm{PG}(\mathbb{F}_q^4)$*. Then, $|\mathcal{S}| \geq 2q+1$.*

The above bound is sharp. Constructions of point sets having size meeting the above bound were provided by Tallini in [16].

Definition 7.2. If $\mathcal{T}$ is a set of $q+1$ points, then a point $\mathcal{P} \notin \mathcal{T}$ is called a *nucleus* of $\mathcal{T}$ if every line through $\mathcal{P}$ contains exactly one point of $\mathcal{T}$.

Proposition 7.3 (see [16, Example 1])**.** *Let ℓ be a line in* $\mathrm{PG}(\mathbb{F}_q^4)$*, π be a plane in* $\mathrm{PG}(\mathbb{F}_q^4)$ *not containing ℓ, and T be a set of $(q+1)$ non-collinear points of π having the point $\pi \cap \ell$ as nucleus. Then, the point set*

$$\mathcal{S} = (\ell \setminus \pi) \cup \mathcal{T} \subseteq \mathrm{PG}(\mathbb{F}_q^4),$$

is a 3-dimensional minimal blocking set having size $2q+1$.

Using the above results, we can construct explicit examples of minimal 3-dimensional locally q^{th}-power set for $q \in \{3,5\}$ of size $2q+1$. Choose a coordinatization for $\mathrm{PG}(\mathbb{F}_q^4)$ and let π be the plane of $\mathrm{PG}(\mathbb{F}_q^4)$ having equation $X_3 = 0$. Consider the set

$$\mathcal{T} = \{\langle (1, t, t^2, 0)\rangle_{\mathbb{F}_q} \colon t \in \mathbb{F}_q\} \cup \{\langle 0, 0, 1\rangle\} \subseteq \pi.$$

It is easy to see that the point set $\mathcal{T}$ has as nucleus the point $\mathcal{Q} = \langle (0,1,0,0)\rangle_{\mathbb{F}_q}$ and consider ℓ be the line having equation $X_1 = X_3 = 0$.

We have that $\{\mathcal{Q}\} = \ell \cap \pi$. Then π, ℓ and $\mathcal{T}$ are as in Theorem 7.3. This means that the point set

$$\mathcal{S} = \{\langle(1,t,t^2,0)\rangle_{\mathbb{F}_q} : t \in \mathbb{F}_q\} \cup \{\langle(0,1,0,0)\rangle_{\mathbb{F}_q}, \langle(0,0,1,0)\rangle_{\mathbb{F}_q}\} \\ \cup \{\langle(0,1,0,t)\rangle_{\mathbb{F}_q} : t \in \mathbb{F}_q^*\}$$

is a 3-dimensional minimal blocking set having size $2q+1$. Considering the set of integers associated to $\mathcal{S}$, we have the following theorem.

Theorem 7.4. *Let B be a minimal 3-dimensional locally q^{th} power set. Then $|B| \geq 2q+1$. Moreover, the sets*

$$B_1 = \{p_1, p_2, p_3, p_2p_3, p_1p_2^2p_3, p_2p_4, p_2p_4^2\}$$

and

$$B_2 = \{p_1, p_2, p_3, p_2p_3, p_1p_2^2p_3^4, p_1p_2^3p_3^4, p_1p_2^4p_3, p_2p_4, p_2p_4^2, p_2p_4^3, p_2p_4^4\}$$

are minimal, 3-dimensional, locally 3^{rd} power set and minimal, 3-dimensional, locally 5^{th} power set, respectively.

7.1. Upper bound on minimal locally q^{th} power set. In contrast to the lower bounds on cardinality of minimal locally q^{th} power sets, one also has upper bounds on the same cardinality.

Proposition 7.5. *Let $\mathcal{S}$ be a minimal blocking set of* $\mathrm{PG}(\mathbb{F}_q^k)$ *and s denote the fractional part of $\sqrt{q}$. Then:*

(1) *if $k=3$, then* $|\mathcal{S}| \leq \begin{cases} q\sqrt{q}+1-\frac{s(1-s)q}{4} & \text{for } q \neq 5 \\ q\sqrt{q}+1 & \text{for } q = 5. \end{cases}$

(2) *if $k=4$, then $|\mathcal{S}| \leq q^2+1$.*

(3) *if $k \geq 5$, then $|\mathcal{S}| < \sqrt{q^k}+1$.*

The result above for $k=3$ and $q \neq 5$ has been first shown in [15] and the rest appears in [5, Theorem 1]. As a consequence we obtain the following.

Corollary 7.6. *Let B be a finite subset of integers not containing a perfect q^{th} power that is a minimal locally q^{th} power set. Let s denote the fractional part of $\sqrt{q}$. Then:*

(1) *if $k=3$, then* $|B| \leq \begin{cases} q\sqrt{q}+1-\frac{s(1-s)q}{4} & \text{for } q \neq 5 \\ q\sqrt{q}+1 & \text{for } q = 5. \end{cases}$

(2) *if $k=4$, then $|B| \leq q^2+1$.*

(3) *if $k \geq 5$, then $|B| < \sqrt{q^k}+1$.*

When $k=4$, 3-dimensional minimal blocking sets of $\mathrm{PG}(\mathbb{F}_q^4)$ having size q^2+1 are classified and they correspond to an ovoid [5], which correspond to an elliptic quadric of $\mathrm{PG}(\mathbb{F}_q^4)$ [1, 12]. These results are summarized in the following proposition.

Proposition 7.7. *A 3-dimensional minimal blocking set of* $\mathrm{PG}(\mathbb{F}_q^4)$ *having maximum size* q^2+1*, with* q *odd, is an elliptic quadric.*

Note also that the elliptic quadric of $\mathrm{PG}(\mathbb{F}_q^4)$ are classified, see e.g. [10, p. 123].

Proposition 7.8. *An elliptic quadric in* $\mathrm{PG}(\mathbb{F}_q^4)$*, up to* $\mathrm{PGL}(4,q)$*-equivalence, has equation*

$$f(X_1,X_2)+X_2X_3=0,$$

where $f(X_1,X_2)\in\mathbb{F}_q[X_1,X_2]$ *is an irreducible polynomial.*

For instance, let $f(X_1,X_2)=X_1^2-\alpha X_2^2$, with $\alpha\notin Q$. As a consequence, we have the following:

Theorem 7.9. *B be a minimal, 3-dimensional, locally q^{th} power set. Then, $|B|\leq q^2+1$. Moreover, $|B|=q^2+1$ if and only if B is geometrically q-equivalent to the set*

$$\left\{p_1^{v_{11}}p_2^{v_{21}}p_3^{v_{31}}p_4^{v_{41}},\ldots,p_1^{v_{1,q^2+1}}p_2^{v_{2,q^2+1}}p_3^{v_{3,q^2+1}}p_4^{v_{4,q^2+1}}\right\},$$

where $\{\langle(v_{1j},v_{2j},v_{3j},v_{4j})\rangle_{\mathbb{F}_q}\}_{j=1}^{q^2+1}\subset\mathrm{PG}(\mathbb{F}_q^4)$ *is the set of* q^2+1 *points on an elliptic quadric.*

References

[1] A. Barlotti, "Un'estensione del teorema di Segre-Kustaanheimo", *Boll. Unione Mat. Ital.* **10** (1955), no. 4, p. 498-506.

[2] A. Blokhuis, "On the size of a blocking set in $\mathrm{PG}(2,p)$", *Combinatorica* **14** (1994), p. 111-114.

[3] A. Blokhuis, P. Sziklai & T. Szonyi, "Blocking sets in projective spaces", in *Current research topics in Galois geometry*, Mathematics Research Developments, Nova Science Publishers/Novinka, 2011, p. 61-84.

[4] R. C. Bose & R. C. Burton, "A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes", *J. Comb. Theory* **1** (1966), no. 1, p. 96-104.

[5] A. A. Bruen & J. A. Thas, "Hyperplane coverings and blocking sets", *Math. Z.* **181** (1982), no. 3, p. 407-409.

[6] K. Coolsaet, A. Botteldoorn & V. Fack, "Classification of minimal blocking sets in small Desarguesian projective planes", *J. Comb. Des.* **30** (2022), no. 8, p. 561-580.

[7] M. A. Filaseta & D. R. Richman, "Sets which contain a quadratic residue modulo p for almost all p", *Math. J. Okayama Univ.* **39** (1989), p. 1-8.

[8] M. Fried, "Arithmetical properties of value sets of polynomials", *Acta Arith.* **15** (1969), no. 2, p. 91-115.

[9] U. Heim, "Blockierende Mengen in endlichen projektiven Räumen", PhD Thesis, Justus-Liebig-Universität Giessen, Giessen, 1996.

[10] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Oxford Mathematical Monographs, Clarendon Press; Oxford University Press, 1998.

[11] B. Mishra, "Prime power residue and linear coverings of vector space over $\mathbb{F}_q$", *Finite Fields Appl.* **89** (2023), article no. 102199 (12 pages).

[12] G. Panella, "Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito.", *Boll. Unione Mat. Ital.* **10** (1955), no. 4, p. 507-513.

[13] A. Schinzel & M. Skałba, "On power residues", *Acta Arith.* **108** (2003), no. 1, p. 77-94.

[14] M. Skałba, "On sets which contain a q^th power residue for almost all prime modules", *Colloq. Math.* **102** (2005), p. 67-71.

[15] T. Szőnyi, A. Cossidente, A. Gács, C. Mengyán, A. Siciliano & Z. Weiner, "On large minimal blocking sets in PG(2, q)", *J. Comb. Des.* **13** (2005), no. 1, p. 25-41.

[16] G. Tallini, "Blocking sets with respect to planes in $PG(3, q)$ and maximal spreads of a non-singular quadric in $PG(4, q)$", *Mitt. Math. Semin. Gießen* **201** (1991), p. 141-147.

Bhawesh Mishra
Department of Mathematical Sciences,
384 Dunn Hall, University of Memphis,
Memphis, TN 38107, USA
E-mail: `bmishra1@memphis.edu`

Paolo Santonastaso
Dipartimento di Matematica e Fisica,
Università degli Studi della Campania "Luigi Vanvitelli",
I–81100 Caserta, Italy
E-mail: `paolo.santonastaso@unicampania.it`