INTEGRAL POINT SETS OVER FINITE FIELDS

SASCHA KURZ

Abstract. We consider point sets in the affine plane $\mathbb{F}_q^2$ where each Euclidean distance of two points is an element of $\mathbb{F}_q$. These sets are called integral point sets and were originally defined in m-dimensional Euclidean spaces $\mathbb{E}^m$. We determine their maximal cardinality $\mathcal{I}(\mathbb{F}_q, 2)$. For arbitrary commutative rings $\mathcal{R}$ instead of $\mathbb{F}_q$ or for further restrictions as no three points on a line or no four points on a circle we give partial results. Additionally we study the geometric structure of the examples with maximum cardinality.

1. Introduction

Originally integral point sets were defined in m-dimensional Euclidean spaces $\mathbb{E}^m$ as a set of n points with pairwise integral distances in the Euclidean metric, see [10, 14, 16, 17] for a overview on the most recent results. Here we transfer the concept of an integral point set to modules $\mathcal{R}^m$ of a commutative ring with 1. We equip those spaces with a squared distance

$$d^2(u,v) := \sum_{i=1}^{m} (u_i - v_i)^2 \quad \in \mathcal{R}.$$

for any two points $u = (u_1, \ldots, u_m)$, $v = (v_1, \ldots, v_m)$ in $\mathcal{R}^m$ and say that they are at integral distance if $d^2(u,v)$ is contained in the set $\square_{\mathcal{R}} := \{r^2 \mid r \in \mathcal{R}\}$ consisting of the squares in $\mathcal{R}$. A set of points $\mathcal{P}$ is called an integral point set if every pair of points is at integral distance.

The concept of integral point sets over finite fields is not brand-new. There are some recent papers and preprints [29, 27, 28, 30] by L.A. Vinh dealing with Quadrance graphs. These are in the authors definition point sets in the affine plane $\mathbb{F}_q^2$ where the squared distances, there called quadrances, are elements of $\square_{\mathbb{F}_q} \backslash \{0\}$. So for $q \equiv 3 \mod 4$ quadrance graphs coincide with integral point sets over $\mathbb{F}_q^2$. For $q \equiv 1 \mod 4$ we have the small difference that $0 = 0^2$ is not considered as an integral distance. So i.e. the points $(0,0)$ and $(2,3)$ in $\mathbb{F}_{13}$ are not considered to be at an integral distance since $d^2((0,0),(2,3)) = 2^2 + 3^2 = 0$. We would like to mention that quadrance graphs and so integral point sets over finite fields are isomorphic to strongly regular graphs and that there are some connections to other branches of Combinatorics including Ramsey theory and association schemes [23, 24, 31]. The origin of quadrance graphs lies in the more general concept of rational trigonometry and universal geometry by N.J. Wildberger, see [32] for more background.

Some related results on integral point sets over commutative rings can be found in [1, 8, 13].

A somewhat older topic of the literature is also strongly connected to integral point sets over finite fields. The Paley graph $\mathcal{PG}_q$ has the elements of the finite field $\mathbb{F}_q$ as its vertices. Two vertices u and v are connected via an edge if and only if their difference is a non-zero square in $\mathbb{F}_q$. For $q = q'^2$ with $q' \equiv 3 \mod 4$ we have a coincidence between the Paley graph $\mathcal{PG}_q$ and integral point sets over $\mathcal{PG}_{q'}^2$, or quadrance graphs. It is somewhat interesting that these one-dimensional and two-dimensional geometrical objects are so strongly connected. See i.e. [2, 28] for a detailed description and proof of this connection. Actually one uses the natural embedding of $\mathbb{F}_{q^2}$ in $\mathbb{F}_q^2$.

So what are the interesting questions about integral point sets over finite fields? From the combinatorial point of view one could ask for the maximum cardinality $\mathcal{I}(\mathcal{R}, m)$ of those point

sets in $\mathcal{R}^m$. For $\mathcal{R} = \mathbb{F}_q$ with $q \equiv 3 \mod 4$ and $m = 2$ this is a classical question about maximum cliques of Paley graphs of square order, where the complete answer is given in [3]. See also [26] for some generalizations. A geometer might ask for the geometric structure of the maximal examples. Clearly the case where $\mathcal{R}$ is a finite field $\mathbb{F}_q$ is the most interesting one.

1.1. **Our contribution.** For primes p we completely classify maximal integral point sets in the affine planes $\mathbb{F}_p^2$ and for prime powers $q = p^r$ we give partial results. Since in an integral point set not all directions can occur we can apply some Rédei-type results in this context. Although these results are not at hand in general we can derive some results for arbitrary rings $\mathcal{R}$ and special cases like $\mathcal{R} = \mathbb{Z}_{p^2}$ or rings with characteristic two.

It will turn out that most maximal examples or constructions in the plane consist of only very few lines. So it is interesting to consider the case where we forbid three points to be collinear. This means that we look at 2-arcs with the additional integrality condition. Here we denote the maximal cardinality by $\overline{\mathcal{I}}(\mathcal{R}, m)$ where we in general forbid that $m+1$ points are contained in a hyperplane. We give a construction and a conjecture for the case $\mathcal{R} = \mathbb{F}_q$, $2 \nmid q$, and $m = 2$ using point sets on circles.

Being even more restrictive we also forbid $m+2$ points to be situated on a hypersphere and denote the corresponding maximal cardinality by $\dot{\mathcal{I}}(\mathcal{R}, m)$. Although in this case we have almost no theoretical insight so far, this is the most interesting situation when we look from the viewpoint of integral point sets in $\mathbb{E}^m$. As a motivation for further research the following open problem of P. Erdős and C. Noll [20] may serve:

> Are there seven points in the plane, no three on a line, no four on a circle with integral coordinates and pairwise integral distances?

If we drop the condition of integral coordinates the problem was recently solved in [14]. As a connection to our problem one may use the ring homomorphism $\mathbb{Z}^m \to \mathbb{Z}_n^m$, $x \mapsto x + (n\mathbb{Z})^m$, which preserves integral distances and coordinates. For lines and circles the situation is a bit more complicated. We give some examples for various primes p showing $\dot{\mathcal{I}}(\mathbb{Z}_p, 2) \geq 7$ and determine some exact numbers. Perhaps in the future an application of the Chinese remainder theorem helps to construct the desired example in $\mathbb{Z}^2$.

1.2. **Organization of the paper.** The paper is arranged as follows. In Section 2 we give the basic definitions and facts on integral point sets over commutative rings $\mathcal{R}$. In Section 3 we determine the automorphism group of the affine plane $\mathbb{F}_q^2$ with respect to Δ. For $q \equiv 3 \mod 4$ it is the well known automorphism group of the Paley graph $\mathcal{PG}_{q^2}$ which is isomorphic to a subgroup of $\mathrm{P\Gamma}(1, q^2)$ of index 2, see i.e. [6, 12, 25]. For $q \equiv 1 \mod 4$ the automorphism group was not known. We give a proof for both cases and prove some lemmas on integral point sets over finite fields which will be useful in the following sections. Most of the automorphisms also exist in some sense for arbitrary commutative rings $\mathcal{R}$. In Section 4 we determine the maximum cardinality $\mathcal{I}(\mathbb{F}_q, 2)$ of an integral point set over $\mathbb{F}_q^2$ and classify the maximal examples up to isomorphism in some cases. Here we use a result of Blokhuis et al. on point sets with a restricted number of directions. In Section 5 we give some results on $\mathcal{I}(\mathbb{Z}_n, 2)$ and give some constructions which reach this upper bound. In Section 6 we determine the maximum cardinality $\overline{\mathcal{I}}(\mathbb{F}_q, 2)$ of integral point sets over $\mathbb{F}_q$ where no three points are collinear for $q \equiv 3 \mod 4$. For $q \equiv 1 \mod 4$ we give lower and upper bounds which are only two apart. In Section 7 we consider the maximum cardinality $\dot{\mathcal{I}}(\mathbb{F}_q, 2)$ of integral point sets over $\mathbb{F}_q^2$ where no three points are collinear and no four points are situated on a circle. We determine some exact values via an exhaustive combinatorial search and list some maximum examples.

2. Integral point sets

If not stated otherwise we assume that $\mathcal{R}$ is a commutative ring with 1 and consider sets of elements of the $\mathcal{R}$-module $\mathcal{R}^m$. We speak of these elements as points with a geometric interpretation in mind. For our purpose we equip the module $\mathcal{R}^m$ with something similar to an Euclidean metric:

Definition 1. *For two points $u = (u_1, \ldots, u_m)$, $v = (v_1, \ldots, v_m)$ in $\mathcal{R}^m$ we define the* ***squared distance*** *as*

$$d^2(u, v) := \sum_{i=1}^{m} (u_i - v_i)^2 \quad \in \mathcal{R}.$$

We are interested in those cases where $d^2(u, v)$ is contained in the set $\square_{\mathcal{R}} := \{r^2 \mid r \in \mathcal{R}\}$ of squares of $\mathcal{R}$.

Definition 2. *Two points $u = (u_1, \ldots, u_m)$, $v = (v_1, \ldots, v_m)$ in $\mathcal{R}^m$ are at* ***integral distance*** *if there exists an element r in $\mathcal{R}$ with $d^2(u, v) = r^2$. As a shorthand we define $\Delta : \mathcal{R}^m \times \mathcal{R}^m \to \{0, 1\}$,*

$$(u, v) \mapsto \begin{cases} 1 & \text{if } u \text{ and } v \text{ are at integral distance,} \\ 0 & \text{otherwise.} \end{cases}$$

A set $\mathcal{P}$ of points in $\mathcal{R}^m$ is called an ***integral point set*** *if all pairs of points are at integral distance.*

If $\mathcal{R}$ is a finite ring it makes sense to ask for the maximum cardinality of an integral point set in $\mathcal{R}^m$.

Definition 3. *By $\mathcal{I}(\mathcal{R}, m)$ we denote the maximum cardinality of an integral point set in $\mathcal{R}^m$.*

Lemma 1.

$$|\mathcal{R}| \leq \mathcal{I}(\mathcal{R}, m) \leq |\mathcal{R}|^m.$$

Proof. For the lower bound we consider the *line* $\mathcal{P} = \{(r, 0, \ldots, 0) \mid r \in \mathcal{R}\}$. □

Lemma 2. *If $\mathcal{R}$ has characteristic 2, meaning that $1+1 = 0$ holds, then we have $\mathcal{I}(\mathcal{R}, m) = |\mathcal{R}|^m$.*

Proof. For two points $u = (u_1, \ldots, u_m)$, $v = (v_1, \ldots, v_m)$ in $\mathcal{R}^m$ we have

$$d^2(u, v) = \sum_{i=1}^{m} (u_i - v_i)^2 = \underbrace{\left(\sum_{i=1}^{r} u_i + v_i \right)^2}_{\in \mathcal{R}}.$$

□

So in the remaining part of this article we consider only rings with characteristic not equal to two. If a ring $\mathcal{R}$ is the Cartesian product of two rings $\mathcal{R}_1$, $\mathcal{R}_2$, where we define the operations componentwise, then we have the following theorem:

Theorem 1.

$$\mathcal{I}(\mathcal{R}_1 \times \mathcal{R}_2, m) = \mathcal{I}(\mathcal{R}_1, m) \cdot \mathcal{I}(\mathcal{R}_2, m).$$

Proof. If $\mathcal{P}$ is an integral point set in $\mathcal{R}_1 \times \mathcal{R}_2$ then the projections into $\mathcal{R}_1$ and $\mathcal{R}_2$ are also integral point sets. If on the other hand $\mathcal{P}_1$ and $\mathcal{P}_2$ are integral point sets over $\mathcal{R}_1$ and $\mathcal{R}_2$, respectively, then $\mathcal{P} := \mathcal{P}_1 \times \mathcal{P}_2$ is an integral point set over $\mathcal{R}_1 \times \mathcal{R}_2$. □

Lemma 3. *If N is an additive subgroup of $\{n \in \mathcal{R} \mid n^2 = 0\}$ or $\{n \in \mathcal{R} \mid 2n^2 = 0 \wedge n^2 = n^4\}$ then we have for $m \geq 2$*

$$|N|^{m-1} \cdot |\mathcal{R}| \leq \mathcal{I}(\mathcal{R}, m) \leq |\mathcal{R}|^m.$$

Proof. We can take the integral point set $\mathcal{P} = \{(r, n_1, \dots, n_{m-1}) \mid r \in \mathcal{R},\, n_i \in N\}$ and have $r^2 + \sum_{i=1}^{m-1} n_i^2 = r^2$ or $r^2 + \sum_{i=1}^{m-1} n_i^2 = \left(r + \sum_{i=1}^{m-1} n_i^2\right)^2$. □

If we specialize these general results to rings of the from $\mathcal{R} = \mathbb{Z}/\mathbb{Z}n =: \mathbb{Z}_n$ then we have the following corollaries:

Corollary 1.
$$\mathcal{I}(\mathbb{Z}_n, 1) = n \text{ and } \mathcal{I}(\mathbb{Z}_2, m) = 2^m.$$

Corollary 2. *For coprime integers a and b we have $\mathcal{I}(\mathbb{Z}_{ab}, m) = \mathcal{I}(\mathbb{Z}_a, m) \cdot \mathcal{I}(\mathbb{Z}_b, m)$.*

Corollary 3. *For a prime $p > 2$ we have*
$$\mathcal{I}(\mathbb{Z}_{p^r}, m) \geq p^r \cdot p^{m-1\left\lfloor \frac{r}{2} \right\rfloor}.$$

To be able to do some algebraic calculations later on we denote the set of invertible elements of $\mathcal{R}$ by $\mathcal{R}^*$ and derive a ring $\mathcal{R}'$ from the module $\mathcal{R}^2$.

Definition 4.
$$\mathcal{R}' := \mathcal{R}[x]/(x^2 + 1).$$

With i being a root of $x^2 + 1$ we have the following bijection
$$\varrho : \mathcal{R}^2 \to \mathcal{R}',\ (a, b) \mapsto a + bi.$$
The big advantage of the ring $\mathcal{R}'$ is that we naturally have an addition and multiplication. The construction of the ring is somewhat a reverse engineering of the connection between Paley graphs of square order and integral point sets over the affine plane $\mathbb{F}_q^2$ for $q \equiv 3 \mod 4$. With the similar construction of the complex numbers in mind we define:

Definition 5.
$$\overline{a + bi} = a - bi.$$

Lemma 4. *For $p, p_1, p_2 \in \mathcal{R}'$ we have*
(1) $d^2(p_1, p_2) = (p_1 - p_2) \cdot \overline{(p_1 - p_2)}$,
(2) $p\overline{p} \in \mathcal{R}$,
(3) $\overline{p_1 + p_2} = \overline{p_1} + \overline{p_2}$,
(4) $\overline{p_1 \cdot p_2} = \overline{p_1} \cdot \overline{p_2}$, *and*
(5) $\overline{\overline{p}} = p$.

3. Automorphism group of the plane $\mathcal{R}^2$

Since we want to classify maximal integral point sets up to isomorphism we have to define what we consider as an automorphism.

Definition 6. *An automorphism of $\mathcal{R}'$ with respect to Δ is a bijective mapping φ of $\mathcal{R}'$ with*
(1) $\Delta(a + bi, c + di) = \Delta(\varphi(a + bi), \varphi(c + di))$ *and*
(2) *there exist $a', b', c', d' \in \mathcal{R}$ such that*
$\{\varphi(a + bi + r(c + di)) \mid r \in \mathcal{R}\} = \{a' + b'i + r(c' + d'i) \mid r \in \mathcal{R}\}$
for all a, b, c, d in $\mathcal{R}$.

In words this definition says that φ has to map points to points, lines to lines, and has to preserve the integral distance property. There is a natural similar definition for $\mathcal{R}^2$ instead of $\mathcal{R}'$.

Lemma 5. *We have the following examples of automorphisms:*

(1) $\varphi_s(r) = r + s$ *for* $s \in \mathcal{R}'$,
(2) $\widetilde{\varphi}(a + bi) = b + ai$,
(3) $\widetilde{\varphi}_y(r) = ry$ *for* $y \in \mathcal{R}'^*$ *with* $\exists r' \in \mathcal{R}^* : y\overline{y} = r'^2$, *and*
(4) $\widehat{\varphi}_j(a + bi) = a^{p^j} + b^{p^j} i$ *for* $j \in \mathbb{N}$ *and* p *being the characteristic of a field* $\mathcal{R}$.

Proof. The first two cases are easy to check. For the third case we consider

$$\begin{aligned} d^2(r_1 y, r_2 y) &= (r_1 y - r_2 y) \cdot \overline{(r_1 y - r_2 y)}, \\ &= (r_1 - r_2) \cdot \overline{(r_1 - r_2)} y\overline{y}, \\ &= d^2(r_1, r_2) \cdot y\overline{y}. \end{aligned}$$

For the fourth case we have

$$\begin{aligned} d^2(\widehat{\varphi}_j(a_1 + b_1 i), \widehat{\varphi}_j(a_2 + b_2 i)) &= (a_1^{p^j} - a_2^{p^j})^2 + (b_1^{p^j} - b_2^{p^j})^2, \\ &= (a_1 - a_2)^{p^j \cdot 2} + (b_1 - b_2)^{p^j \cdot 2}, \\ &= \left((a_1 - a_2)^2 + (b_1 - b_2)^2\right)^{p^j}, \\ &= d^2(a_1 + b_1 i, a_2 + b_2 i)^{p^j} \end{aligned}$$

Thus integral point sets are mapped onto integral point sets. That lines are mapped onto lines can be checked immediately. Since we have requested that $\mathcal{R}$ is a field for the forth case the mappings are injective. □

After this general definition of automorphisms we specialize to the case $\mathcal{R} = \mathbb{F}_q$ with $2 \nmid q$. As shorthand we use $\square_q := \square_{\mathbb{F}_q}$. We remark that the case (4) is the set of Frobenius automorphisms of the field $\mathbb{F}_q$ which is a cyclic group of order r for $q = p^r$.

Theorem 2. *For* $q = p^r$, $p \neq 2$, $q \neq 5, 9$ *the automorphisms of* $\mathbb{F}'_q$ *with respect to* Δ *are completely described in Lemma 5.*

For $q \equiv 3 \mod 4$ this is a well known result on the automorphism group of Paley graphs as mentioned in the introduction. If we consider the set of automorphisms from Lemma 5 in $\mathbb{F}_q^2$ instead of $\mathbb{F}'_q$ then they form a group with its elements being compositions of the following four mappings:

(1) $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$ where $a, b \in \mathbb{F}_q$,
(2) $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$ where $a, b \in \mathbb{F}_q$, $a^2 + b^2 \in \square_q \backslash \{0\}$,
(3) $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$, and
(4) $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x^p \\ y^p \end{pmatrix}$.

In the remaining part of this section we will prove Theorem 2. For the sake of completeness we also give the proof for $q \equiv 3 \mod 4$. If we forget about respecting Δ then the automorphism group of $\mathbb{F}_q^2$ is the well known group $\mathrm{A\Gamma L}(2, \mathbb{F}_q)$. It is a semi-direct product of the translation group, the Frobenius group $\mathrm{Aut}(\mathbb{F}_q)$, and $\mathrm{GL}(2, \mathbb{F}_q)$, the group of multiplications with invertible 2×2 matrices over $\mathbb{F}_q$. So if G' is the automorphism group of $\mathbb{F}_q^2$ with respect to Δ it suffices to determine the group $G := G' \cap \mathrm{GL}(2, \mathbb{F}_q)$ because every translation and every element in $\mathrm{Aut}(\mathbb{F}_q)$

respects Δ. So all elements of G can be written as $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x & y \end{pmatrix} \cdot M$ with M being an invertible 2×2-matrix. As a shorthand we say that M is an element of the automorphism group G.

Lemma 6. *If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an element of the automorphism group G then we have $ad-bc \neq 0$ and a^2+b^2, a^2+c^2, b^2+d^2, $c^2+d^2 \in \square_q$.*

Proof. Since M is also an element of $\mathrm{GL}(2,\mathbb{F}_q)$ its determinant does not vanish. By considering the points $(0,0)$ and $(0,y)$ which are at an integral distance we obtain that b^2+d^2 must be a square in $\mathbb{F}_q$. Similarly we obtain that a^2+c^2, a^2+b^2, and c^2+d^2 must be squares in $\mathbb{F}_q$. □

To go on we need some facts about roots in $\mathbb{F}_q$ and the set of solutions of quadratic equations in $\mathbb{F}_q$.

Definition 7. *For $p^r \equiv 1 \mod 4$ we denote by ω_q an element with $\omega_q^2 = -1$.*

Lemma 7. *For a finite field $\mathbb{F}_q$ with $q = p^r$ and $p \neq 2$ we have $-1 \in \square_q$ iff $q \equiv 1 \mod 4$, $\omega_q \in \square_q$ iff $q \equiv 1 \mod 8$, and $2 \in \square_q$ iff $q \equiv \pm 1 \mod 8$.*

Proof. The multiplicative group of the units $\mathbb{F}_q^*$ is cyclic of order $q-1$. Elements of order 4 are exactly those elements x with $x^2 = -1$. A similar argument holds for the the fourth roots of -1. The last statement is the second Ergänzungssatz of the quadratic reciprocity law generalized to $\mathbb{F}_q$. For a proof we may consider the situation in $\mathbb{F}_p$ and adjungate x modulo the ideal (x^2-2). □

Lemma 8. *For a fix $c \neq 0$ and $2 \nmid q$ the equation $a^2+b^2=c^2$ in $\mathbb{F}_q$ has exactly $q+1$ different solutions if $-1 \notin \square_q$ and exactly $q-1$ different solutions if $-1 \in \square_q$.*

Proof. If $b = 0$ then we have $a = \pm c$. Otherwise

$$a^2+b^2=c^2 \quad \Leftrightarrow \quad \frac{a-c}{b} \cdot \frac{a+c}{b} = -1.$$

Here we set $t := \frac{a+c}{b} \in \mathbb{F}_q^*$ ($t=0$ corresponds to $b=0$). We obtain

$$2\frac{a}{b} = t - t^{-1}, \quad 2\frac{c}{b} = t + t^{-1} \neq 0,$$

yielding

$$t^2 \neq -1, \quad b = \frac{2c}{t+t^{-1}}, \text{ and } a = c \cdot \frac{t-t^{-1}}{t+t^{-1}}.$$

If t and t' yield an equal b then we have $t' = t^{-1}$. For $t \neq t^{-1}$ we have different values for a in these cases. Summing up the different solutions proves the stated result. □

Lemma 9. *In $\mathbb{F}_q'$ the set $C = \{z \in \mathbb{F}_q' \mid z\overline{z} = 1\}$ forms a cyclic multiplicative group.*

Proof. If $-1 \notin \square_q$ then $\mathbb{F}_q'$ is a field and thus C must be cyclic. For the case $-1 \in \square_q$ we utilize the bijection

$$\rho_q : \mathbb{F}_q^* \to G, \quad t \mapsto \frac{1+t^2}{2t} + \omega_q \frac{1-t^2}{2t} x.$$

Now we only have to check that the mapping is a group isomorphism, namely

$$\rho_q(i \cdot j) = \rho_q(i) \cdot \rho_q(j).$$

□

Our next ingredient is a classification of the subgroups of the projective special linear group $\mathrm{PSL}(2,q)$.

Theorem 3. *(Dickson [7]) The subgroups of $PSL(2,p^r)$ are isomorphic to one of the following families of groups:*

1. *elementary abelian p-groups,*
2. *cyclic group of order z, where z is a divisor of $\frac{p^r \pm 1}{k}$ and $k = \gcd(p^r - 1, 2)$,*
3. *dihedral group of order $2z$, where z is defined as in (2),*
4. *alternating group A_4 (this can occur only for $p > 2$ or when $p = 2$ and $r \equiv 0 \mod 12$),*
5. *symmetric group S_4 (this can only occur if $p^{2r} \equiv 1 \mod 16$),*
6. *alternating group A_5 (for $p = 5$ or $p^{2r} \equiv 1 \mod 5$),*
7. *a semidirect product of an elementary abelian group of order p^m with a cyclic group of order t, where t is a divisor of $p^m - 1$ and of $p^r - 1$, or*
8. *the group $PSL(2,p^m)$ for m a divisor of r, or the group $PGL(2,p^m)$ for $2m$ a divisor of r.*

By $Z := \pm E$ we denote the center of $\mathrm{SL}(2,q)$, where E is the identity matrix. Our strategy is to consider $H := (G \cap \mathrm{SL}(2,q))/Z = G \cap \mathrm{PSL}(2,q)$ and to prove $H \simeq H'$ for $q \geq 13$ where H' is the group of those automorphisms of Lemma 5 which are also elements of $\mathrm{PSL}(2,q)$. For $-1 \notin \square_q$ we set $\tilde{H} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 = 1 \right\}$ and for $-1 \in \square_q$ we set $\tilde{H} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 = 1 \right\} \cup \left\{ \begin{pmatrix} -b & a \\ a & b \end{pmatrix} \mid a^2 + b^2 = -1 \right\}$.

Lemma 10. *For $q \equiv 3 \mod 4$ we have $\tilde{H} \simeq \mathbb{Z}_{q+1}$ and for $q \equiv 1 \mod 4$ we have $\tilde{H} \simeq D_{q-1}$, where D_{q-1} is the dihedral group of order $2(q-1)$.*

Proof. Utilizing Lemma 8 and checking that both sets are groups we get

$$|\tilde{H}| = \begin{cases} q+1 & \text{if } q \equiv 3 \mod 4, \\ 2(q-1) & \text{if } q \equiv 1 \mod 4. \end{cases}$$

In the first case the group is cyclic due to Lemma 9. In the second case it contains a cyclic subgroup of order $q-1$. By checking the defining relations of a dihedral group we can conclude $\tilde{H} \simeq D_{q-1}$ for $q \equiv 1 \mod 4$. □

Now we define $H' := \tilde{H}/Z$.

Lemma 11. *For $q \geq 13$, $q \equiv 3 \mod 4$ we have $H' \simeq \mathbb{Z}_{\frac{q+1}{2}}$ and for $q \geq 13$, $q \equiv 1 \mod 4$ we have $H' \simeq D_{\frac{q-1}{2}}$.*

Proof. We have $|H'| = \frac{|\tilde{H}|}{2}$. It remains to show that H' is not abelian for $q \equiv 1 \mod 4$. Therefore we may consider the sets $\{\pm M_1\}$ and $\{\pm M_2\}$ where a, b, c, d are elements of $\mathbb{F}_q^*$ with $a^2 + b^2 = 1$, $c^2 + d^2 = -1$ and where

$$M_1 = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} -d & c \\ c & d \end{pmatrix}.$$

□

Lemma 12. *For $q \geq 13$ we have $H \simeq H'$.*

Proof. Since H is a subgroup of $\mathrm{PSL}(2,q)$ we can utilize Theorem 3. We run through the subgroups of $\mathrm{PSL}(2,q)$, identify H' and show that H is no of the subgroups of $\mathrm{PSL}(2,q)$ containing H' as a proper subgroup. With the numbering from the theorem we have the following case distinctions. We remark that for $q \equiv 1 \mod 4$ the group H' is the group of case (3) and for $q \equiv 3 \mod 4$ the group H' is the group of case (2)

(1) H is not an elementary abelian p-group since $|H'|$ is not a p-power.
(2) For $q \equiv 1 \mod 4$ the order of H' is larger than $\frac{p^r+1}{2}$ and for $q \equiv 3 \mod 4$ the characterized group must be H' itself.
(3) For $q \equiv 1 \mod 4$ the characterized group must be H' itself due to the order of the groups. For $q \equiv 3 \mod 4$ we must have a look at the elements of order 2 in $\mathrm{PSL}(2,q)$. These are elements $M \cdot Z$ where $M = \begin{pmatrix} a & b \\ c & b \end{pmatrix}$ with $ad - bc = 1$ and $M^2 = E$ or $M^2 = -E$. Solving this equation system yields $M = \pm E$ which corresponds to an element of H' and $M = \begin{pmatrix} a & b \\ -\frac{a^2+1}{b} & -a \end{pmatrix}$ where $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_q^*$. Now we choose a matrix $N = \begin{pmatrix} u & v \\ -v & u \end{pmatrix}$ with $u^2 + v^2 = 1$ and $u, v \neq 0$. So $N \cdot Z = \{\pm N\} \in H'$ and since $\langle H', N\rangle$ would be a dihedral group we have the following relation

$$MZ \cdot NZ \cdot MZ = N^{-1}Z$$

$$\Leftrightarrow \quad \{\pm M\} \cdot \{\pm N\} \cdot \{\pm M\} = \{\pm N^{-1}\} = \left\{ \pm \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \right\}$$

$$\Leftrightarrow \quad \left\{ \pm \begin{pmatrix} \frac{-ab^2v-a^3v-av-bu}{b} & -v(a^2+b^2) \\ \frac{v(a^2b^2+a^4+2a^2+1)}{b^2} & \frac{-bu+ab^2v+a^3v+av}{b} \end{pmatrix} \right\} = \left\{ \pm \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \right\}.$$

By comparing the diagonal elements we get $av(a^2+b^2+1) = 0$ and $v(b^4-a^4-2a^2-1) = 0$. Due to $v \neq 0$ this is equivalent to $a(a^2+b^2+1) = 0$ and $(a^2+b^2+1) \cdot (a^2-b^2+1) = 0$. Together with $a^2 + b^2 \in \square_q$ we conclude $a = 0$ and $b = \pm 1$. Since these solutions correspond to an element of H' we derive that case (3) is not possible for $q \equiv 3 \mod 4$.
(4) If $H' < H \leq A_4$ then H' must be contained in a maximal subgroup of A_4. Since the order of a maximal subgroup of A_4 is at most 4 and $q \geq 13$ this case can not occur.
(5) Since we have $q \geq 13$ and the maximal subgroups of the S_4 are isomorphic to A_4, D_4, and S_3, this case can not occur.
(6) The maximal subgroups of A_5 are isomorphic to D_5, S_3, and A_4. So this case can not occur for $q \geq 13$.
(7) We have that $|H|$ divides $(q-1) \cdot p^m$. Since $\gcd\left(\frac{q+1}{2}, (q-1) \cdot p^m\right) \leq 2$ and $|H'|$ divides $|H|$, only $q \equiv 1 \mod 4$, $|H'| = q-1$, $t = q-1$, and $r|m$ is possible. If $m \geq 2r$ then $|H| \geq q^2(q-1) > |\mathrm{PSL}(2,q)| = \frac{1}{2}(q^2-1)q$, which is a contradiction. So only $m = r$ is possible and H must be the semidirect product of an abelian group of order q and a cyclic group of order $q-1$. Using Zassenhaus' theorem [11, I.18.3] we can deduce that all subgroups of order $q-1$ of H are conjugates and so isomorphic. Since H' is not abelian (for $q \equiv 1 \mod 4$) it is not cyclic and so at the end case (7) of Theorem 3 is impossible.
(8) Clearly $H \not\cong \mathrm{PSL}(2,q)$. Since $|H'|$ does not divide $|\mathrm{PSL}(2,p^m)| = \frac{(p^{2m}-1)p^m}{2}$ only the second possibility is left. Since $|H'|$ divides $|\mathrm{PGL}(2,p^m)| = (p^{2m}-1)(p^{2m}-p^m)$ we have $2m = r$, $p^m = \sqrt{q}$, and $q \equiv 1 \mod 4$. But for $q \geq 13$ we have $D_{\frac{q-1}{2}} \not\leq \mathrm{PGL}(2,\sqrt{q})$, see i.e. [5], thus case (8) is also not possible.

□

To finish the proof of the characterization of the automorphisms of $\mathbb{F}_q^2$ with respect to Δ we need as a last ingredient a result on the number of solutions of an elliptic curve in $\mathbb{F}_q$.

Theorem 4. *(Hasse, i.e.* [22]*) Let f be a polynomial of degree 3 in $\mathbb{F}_q$ without repeated factors then we have for the number N of different solutions of $f(t) = s^2$ in $\mathbb{F}_q^2$ the inequality $|N-q-1| \leq 2\sqrt{q}$.*

Proof of Theorem 2. For the cases $q = 3, 7, 11$ we utilize a computer to check that there are no other automorphisms. So we can assume $q \geq 13$.

If $M \in G$ is an automorphism for $q \equiv 3 \mod 4$ then there exists an element $x \in \mathbb{F}_q^*$ so that either $x \cdot M$ or $x \cdot M \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has determinant 1. Thus with the help of Lemma 12 and Lemma 5 the theorem is proven for $q \equiv 3 \mod 4$. With the same argument we can show that for $q \equiv 1 \mod 4$ any possible further automorphism which is not contained in the list of Lemma 5 must have a determinant which is a non-square in $\mathbb{F}_q$. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of G with $\det(M) = ad - bc \notin \square_q$. So $M^2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & bc + d^2 \end{pmatrix}$ is also an element of G. Since we have $\det(M^2) = \det(M)^2 \in \square_q$ we have $a^2 + bc = bc + d^2$, $b(a+d) = -c(a+d)$ or $a^2 + bc = -(bc + d^2)$, $b(a+d) = c(a+d)$ due to Lemma 12. This leads to the four cases

(1) $a = d$, $b = -c$,
(2) $a = d = 0$,
(3) $a = -d$, and
(4) $b = c$, $a^2 + d^2 = -2b^2$.

Now we consider the derived matrix $M' := M \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$ with $\det(M') \notin \square_q$ which must be also an automorphism. So each of the matrices M and M' must be one of the four cases. From this we can conclude some equations and derive a contradiction for each possibility. Here we assume that the number of the case of M' is at least the number of the case of M.

(1) M as in (1): With the help of Lemma 6 we get $\det(M) = a^2 + b^2 \in \square_q$, which is a contradiction.
(2) M as in (2): Since $\det(M) \notin \square_q$ the only possibility for M' is case (4). Thus we have $b^2 + c^2 = 0 \Leftrightarrow b = \pm\omega_q c$, where we can assume $c = 1$ and $b = \omega_q$ without loss of generality. Since $\det(M')$ must be a non-square in $\mathbb{F}_q$ we have $q \equiv 5 \mod 8$. If we apply M' onto the points $(0, 0)$ and $(1, 1)$ then we can conclude that 2 must be a square in $\mathbb{F}_q$, which is not the case if $q \equiv 5 \mod 8$.
(3) M as in (3): Due to $\det(M) \notin \square_q$ the matrix M' must be in case (4). So we have $a = d = 0$, a situation already treated in case (2).
(4) M as in (4): Thus also M' has to be in case (4). Here we have $a = d$, $b = c$, $2a^2 = -2b^2$. Without loss of generality we can assume $a = 1$ and $b = \omega_q$. Due to $\det(M) = 2 \notin \square_q$ we have $q \equiv 5 \mod 8$. For two elements $x, y \in \mathbb{F}_q$ with $x^2 + y^2$ being a square we have that also $\tilde{M} := \begin{pmatrix} 1 & \omega_q \\ \omega_q & 1 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} x - \omega_q x & x\omega_q + y \\ x\omega_q - y & x + y\omega_q \end{pmatrix}$ is an automorphism. Thus with Lemma 6 we get that $(x\omega_q + y)^2 + (x + y\omega)^2 = 2^2 xy\omega_q$ must be a square in $\mathbb{F}_q$ for all possible values $x, y \neq 0$. So for $q \equiv 5 \mod 8$ for all possible x, y the product $xy \neq 0$ must be a non-square. We specialize to $x^2 + y^2 = 1^2$ and so can get with the help of Lemma 8 that $x = \frac{2}{t+t^{-1}}$ and $y = \frac{t-t^{-1}}{t+t^{-1}}$ with $t^2 \neq -1$, $t \neq 0$. If we require $t^4 \neq 1$ instead of $t^2 \neq -1$ we get $x, y \neq 0$. Thus $xy = \frac{2(t-t^{-1})}{(t+t^{-1})^2}$ must be a non-square for all $t \in \mathbb{F}_q^*$ with $t^4 \neq 1$. Since 2 is a non-square we have that $t - t^{-1}$ and so also $t^3 - t = t(t-1)(t+1)$ must be a square for all $t \in \mathbb{F}_q^*$ with $t^4 \neq 1$. By checking the five excluded values we see that $f(t) := t(t-1)(t+1)$ must be a square for all $t \in \mathbb{F}_q$. So $f(t) = s^2$ has exactly $N := 2q - 3$ solutions in $\mathbb{F}_q$. Since f has not repeated factors and degree 3 we can apply Theorem 4 to get a contradiction to $q \geq 13$.

□

Lemma 13. *For two points $p_1 \neq p_2 \in \mathbb{F}_q'$ at integral distance there exists an isomorphism φ with either $\varphi(p_1) = 0$, $\varphi(p_2) = 1$ or $\varphi(p_1) = 0$, $\varphi(p_2) = 1 + \omega_q i$.*

Proof. Without loss of generality we assume $p_1 = 0$. Since the points p_1 and p_2 are at integral distance there exists an element $r \in \mathbb{F}_q$ with $p_2\overline{p_2} = r^2$ and since $p_2 \neq p_1$ we have $p_2 \in {\mathbb{F}_q'}^*$. If $p_2\overline{p_2} \neq 0$ we choose $\cdot p_2^{-1}$ as the isomorphism φ. Otherwise we have $p_2 = a + bi$ with $a^2 + b^2 = 0$ where $a, b \neq 0$. Thus $\left(\frac{b}{a}\right)^2 = -1$ and $\varphi = \cdot a^{-1}$. □

We remark that Lemma 13 can be sharpened a bit. For three pairwise different non-collinear points $p_1, p_2, p_3 \in \mathbb{F}_q'$ with pairwise integral distances there exists an isomorphism φ with $\{0, 1\} \subset \{\varphi(p_1), \varphi(p_2), \varphi(p_3)\}$.

Via a computer calculation we can determine the automorphism groups of the missing cases $q = 5, 9$.

Lemma 14. *For $q = 5$ the group $G \leq GL(2, \mathbb{F}_5)$ is given by*

$$\left\{ M = \begin{pmatrix} a & b \\ \pm b & \pm a \end{pmatrix} \mid a, b \in \mathbb{F}_5,\ a^2 + b^2 \in \square_5,\ \det(M) \neq 0 \right\}$$

where the two signs can be chosen independently.

Lemma 15. *For $q = 9$ the group $G \leq GL(2, \mathbb{F}_9)$ is given by*

$$\left\langle \left\{ M = \begin{pmatrix} a & b \\ \pm b & \pm a \end{pmatrix} \mid a, b \in \mathbb{F}_9,\ a^2 + b^2 \in \square_9,\ \det(M) \neq 0 \right\}, \begin{pmatrix} 1 & 0 \\ 0 & y^2 \end{pmatrix} \right\rangle$$

where the two signs can be chosen independently and where y is a primitive root in $\mathbb{F}_9^*$.

For $q = 5$ there are exactly 32 such matrices and for $q = 9$ there are exactly 192 such matrices. For $q = 5, 9$ Lemma 13 can be sharpend. Here the automorphism group acts transitively on the pairs of points with integral distance, as for $q \equiv 3 \mod 4$.

We would like to remark that also for $q \equiv 3 \mod 4$ the automorphism group of $\mathbb{F}_q^2$ with respect to Δ is isomorphic to the automorphism group of the quadrance graph over $\mathbb{F}_q^2$. This can easily be verified be going over the proof of Theorem 2 again and by checking the small cases using a computer.

4. Maximal integral point sets in the plane $\mathbb{F}_q^2$

Very nice rings are those which are integral domains. These are in the case of finite commutative rings exactly the finite fields $\mathbb{F}_q$ where $q = p^r$ is a prime power. So far we only have the lower bound $\mathcal{I}(\mathbb{F}_q, 2) \geq q$. In this section we will prove $\mathcal{I}(\mathbb{F}_q, 2) = q$ for $q > 2$. In the case of $\mathbb{F}_p$ we will even classify the maximum integral point sets up to isomorphism. One way to prove $\mathcal{I}(\mathbb{F}_q, 2) = q$ for $2 \nmid q$ is to consider the graph $\mathcal{G}_q$ with the elements of $\mathbb{F}_q$ as its vertices and pairs of points at integral distance as edges. For $q \equiv 3 \mod 4$ the graph $\mathcal{G}_q$ is isomorphic to the Paley graph of order q^2. From [3] we know that in this case a maximum clique of $\mathcal{G}_q$ has size q and is isomorphic to a line. Also for $q \equiv 1 \mod 4$ the graph $\mathcal{G}_q$ is a strongly regular graph. So we can apply a result from [18, 19] on cliques of strongly regular graphs. It turns out that a maximum clique has size q and that every clique $\mathcal{C}$ of size q is *regular*, in the sense of [18, 19], this means in our special case that every point not in $\mathcal{C}$ is adjacent to $\frac{q+1}{2}$ points in $\mathcal{C}$. To start with our classification of maximum integral point sets over $\mathbb{F}_q$ we need the concept of directions.

Definition 8. *For a point $p = a + bi \in \mathbb{F}_q'$ the quotient $\frac{b}{a} \in \mathbb{F}_q \cup \{\infty\}$ is called the **direction** of p. For two points $p_1 = a_1 + b_1 i$, $p_2 = a_2 + b_2 i$ the direction is defined as $\frac{b_1 - b_2}{a_1 - a_2} \in \mathbb{F}_q \cup \{\infty\}$. We call an direction d **integral** if two points p_1, p_2 with direction d have an integral distance.*

Point sets of cardinality q in $\mathbb{F}_q^2$ with at most $\frac{q+3}{2}$ directions are more or less completely classified:

Theorem 5. *(Ball, Blokhuis, Brouwer, Storme, Szőnyi, [4]) Let $f : \mathbb{F}_q \to \mathbb{F}_q$, where $q = p^n$, p prime, $f(0) = 0$. Let $N = |D_f|$, where D_f is the set of directions determined by the function f. Let e (with $0 \leq e \leq n$) be the largest integer such that each line with slope in D_f meets the graph of f in a multiple of p^e points. Then we have the following:*

(1) *$e = 0$ and $\frac{q+3}{2} \leq N \leq q + 1$,*
(2) *$e = 1$, $p = 2$, and $\frac{q+5}{3} \leq N \leq q - 1$,*
(3) *$p^e > 2$, $e|n$, and $\frac{q}{p^e} + 1 \leq N \leq \frac{q-1}{p^e-1}$,*
(4) *$e = n$ and $N = 1$.*

Moreover, if $p^e > 3$ or ($p^e = 3$ and $N = \frac{q}{3} + 1$), then f is a linear map on $\mathbb{F}_q$ viewed as a vector space over $\mathbb{F}_{p^e}$. (All possibilities for N can be determined in principle.)

Here a function $f : \mathbb{F}_q \to \mathbb{F}_q$ determines a point set $\mathcal{P} = \{(x, f(x)) \mid x \in \mathbb{F}_q\}$ of cardinality q. In the case $N = 1$ the point set is a line. In the case $e = 0$ and $N = \frac{q+3}{2}$ then $\mathcal{P}$ is affine equivalent to the point set corresponding to $x \mapsto x^{\frac{q+1}{2}}$.

We remark that affine equivalence is a bit more than our equivalence because we have to respect Δ. The next thing to prove is that integral point sets can not determine too many directions.

Lemma 16. *For $2 \nmid q$ an integral point set over $\mathbb{F}_q^2$ determines at most $\frac{q+3}{2}$ different directions if $-1 \in \square_q$ and at most $\frac{q+1}{2}$ different directions if $-1 \notin \square_q$.*

Proof. We consider the points $p = a + bi$ at integral distance to 0. Thus there exists an element $c' \in \mathbb{F}_q$ with $a^2 + b^2 = c'^2$. In the case $a = 0$ we obtain the direction ∞. Otherwise we set $d := \frac{b}{a}$ and $c := \frac{c'}{a}$, yielding $1 = c^2 - d^2 = (c - d)(c + d)$, where d is the direction of the point. Now we set $c + d =: t \in \mathbb{F}_q^*$ yielding $c = \frac{t+t^{-1}}{2}$, $d = \frac{t-t^{-1}}{2}$. The two values t and $-t^{-1}$ produce an equal direction. Since $t = -t^{-1} \Leftrightarrow t^2 = -1$ we get the desired bounds. □

We need a further lemma on the number of points on a line in a non collinear integral point set:

Lemma 17. *If $2 \nmid q$ and $\mathcal{P}$ is a non collinear integral point set over $\mathbb{F}_q^2$, then each line l contains at most $\frac{q-1}{2}$ points for $-1 \notin \square_q$ and at most $\frac{q+1}{2}$ points for $-1 \in \square_q$.*

Proof. If l is a line with an integral pair of points on it, then its slope is an integral direction. Now we consider the intersections of lines with integral directions containing a point $p \notin l$, with l. □

We remark that there would be only $\frac{q-1}{2}$ integral directions for $q \equiv 1 \mod 4$ if we would not consider 0 as a square as for quadrance graphs. In this case there could be at most $\frac{q-3}{2}$ points on l for $q \equiv 1 \mod 4$ in Lemma 17.

To completely classify maximum integral point sets over $\mathbb{F}_q'$ we need the point set $\mathcal{P}_q := (1 \pm \omega_q i)\square_q$.

Lemma 18. *$\mathcal{P}_q$ is an integral point set of cardinality q.*

Proof.

$$\begin{aligned} d^2(r_1^2 + r_1^2\omega_q i, r_2^2 + r_2^2\omega_q i) &= 0^2, \\ d^2(r_1^2 + r_1^2\omega_q i, r_2^2 - r_2^2\omega_q i) &= (2\omega_q r_1 r_2)^2, \\ d^2(r_1^2 - r_1^2\omega_q i, r_2^2 - r_2^2\omega_q i) &= 0^2. \end{aligned}$$

□

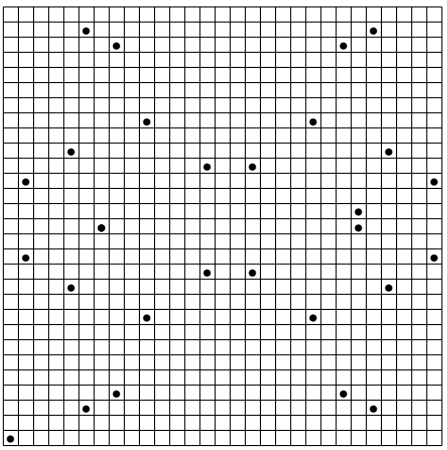

FIGURE 1. The maximum integral point set $\mathcal{P}_{29}$.

In Figure 1 we have depicted $\mathcal{P}_{29}$ as an example. By construction the points of $\mathcal{P}_q$ are located on the two lines $(1, \omega_q)\cdot\mathbb{F}_q$ and $(1, -\omega_q)\cdot\mathbb{F}_q$ which intersect in $(0, 0)$ with an *angle* of 90 degree, but this fact seems not that obvious by looking at Figure 1. We remark that this construction of $\mathcal{P}_q$ works in any commutative ring $\mathcal{R}$ where $-1 \in \square_{\mathcal{R}}$ and that none of these point sets corresponds to a quadrance graph. If we apply this construction on $\mathcal{R} = \mathbb{Z}_{p^r}$ we obtain an integral point set of cardinality $\phi(p^r)+1 = (p-1)\cdot p^{r-1}+1$, where ϕ is the Euler-function defined by $\phi(n) = |\mathbb{Z}_n^*|$.

Lemma 19. *For $2 \mid r$ the point set $\mathcal{P} := \{(a, b) \mid a, b \in \mathbb{F}_{\sqrt{q}}\}$ is an integral point set.*

Proof. We have $\mathbb{F}_{\sqrt{q}} \subset \square_q$. □

We remark that for $\sqrt{q} \equiv 1 \mod 4$ also the point set $\mathcal{P} := \{(a, \omega_q b) \mid a, b \in \mathbb{F}_{\sqrt{q}}\}$ is integral.

We say that an integral point set is maximal if we can not add a further point without destroying the property *integral point set*. All given examples of integral point sets of size q are maximal. This could be proved be applying results on cliques of strongly regular graphs or in the following way.

Lemma 20. *The lines $1 \cdot \mathbb{F}_q$ and $(1 + \omega_q i) \cdot \mathbb{F}_q$ are maximal.*

Proof. We apply Lemma 17. □

Lemma 21. *The integral point set $\mathcal{P} = (1 \pm \omega_q i) \cdot \square_q$ is maximal.*

Proof. Let us assume there is a further point $(a + bi) \notin \mathcal{P}$ with $a, b \in \mathbb{F}_q$ such that $\mathcal{P} \cup \{(a + bi)\}$ is also an integral point set. We know that $(a + bi)$ can not lie on one of the lines $(1 + \omega_q i) \cdot \mathbb{F}_q$

or $(1-\omega_q i)\cdot\mathbb{F}_q$. Thus $a^2+b^2\neq 0$. The points of $\mathcal{P}$ are given by $(1+\omega_q i)r_1^2$ and $(1-\omega_q i)r_2^2$ for arbitrary $r_1, r_2 \in \mathbb{F}_q$. We define functions $f_1, f_2 : \mathbb{F}_q \to \mathbb{F}_q$ via

$$f_1(r_1) = (a-r_1^2)^2 + (b-r_1^2\omega_q)^2 = a^2+b^2-2r_1^2(a+b\omega_q),$$
$$f_2(r_2) = (a-r_2^2)^2 + (b+r_2^2\omega_q)^2 = a^2+b^2-2r_2^2(a-b\omega_q).$$

Since these are exactly the squared distances of the points of $\mathcal{P}$ to the point $(a+bi)$ we have $\mathrm{Bi}(f_1), \mathrm{Bi}(f_2) \subseteq \square_q$. Using a counting argument we have $\mathrm{Bi}(f_1), \mathrm{Bi}(f_2) = \square_q$. The term $-2(a+b\omega_q)$ is a fix number. Let us assume that it is a square. Then for each square r^2 and $c = a^2+b^2 \neq 0$ the difference r^2-c must be a square. But the equation $r^2-c=h^2$ has $\frac{q+1}{2} < q$ solutions for r, which is a contradiction. Thus $-2(a+b\omega_q)$ and $-2(a-b\omega_q)$ are non-squares. But $r^2-c \notin \square_q$ has $\frac{q-1}{2}$ solutions, thus we have a contradiction □

Theorem 6. *For $q=p^r>9$ with $p\neq 2$, $r=1$ or $q\equiv 3 \mod 4$ an integral point set of cardinality q is isomorphic to one of the stated examples.*

Proof. We consider a point set $\mathcal{P}$ of $\mathbb{F}_q$ of cardinality q with at most $\frac{q+3}{2}$ directions and utilize Theorem 5. If $e=r$ and $N=1$ then $\mathcal{P}$ is a line. If $e=1$ then $\mathcal{P}$ is affine equivalent to $X := \{(x, x^{\frac{q+1}{2}}) \mid x \in \mathbb{F}_q\}$. This is only possible for $q \equiv 1 \mod 4$. The set X consists of two orthogonal lines. Since there are only two types of non-isomorphic integral lines in $\mathbb{F}_q^2$ and each point p not on a line l is at integral distance to $\frac{q+1}{2}$ points on l we have two unique candidates of integral point sets of this type. One is given by $(1\pm\omega_q i)\cdot\square_q$. For the other possibility we may assume that $(0,0),(1,0)\in\mathcal{P}$. Thus $(0,\pm\omega_q)\in\mathcal{P}$, $(-1,0),(\pm\omega_q,0),(0,\pm 1)\in\mathcal{P}$. So $\mathcal{P}$ must be symmetric in the following sense: There exists a set $S\subset\mathbb{F}_q^*$ such that $\mathcal{P}=(0,0)\cup\{(0,a),(a,0)\mid a\in S\}$. The elements s of S must fullfill $s\in\mathbb{F}_q^*$, $s^2+1\in\square_q$ and $s^2-1\in\square_q$. Each condition alone has only $\frac{q-1}{2}$ solutions. Fulfilling both conditions, meaning $|S|=\frac{q-1}{2}$ is possible only for $q\leq 9$. For $q=5,9$ there are such examples. For $q\equiv 3 \mod 4$ we refer to [3]. □

We remark that there may be further examples of integral point sets of cardinality q for $q=p^r\equiv 1 \mod 4$ and $r>1$. Those examples would correspond to case (3) of Theorem 5.

Theorem 7. *For $q=p^r$ with $p\neq 2$ we have $\mathcal{I}(\mathbb{F}_q,2)=q$.*

Proof. Let $\mathcal{P}$ be an arbitrary integral point set of cardinality q. Now we show that $\mathcal{P}$ is maximal. If we assume that there is another integral point set $\mathcal{P}'$ with $\mathcal{P}\subset\mathcal{P}'$ and $|\mathcal{P}'|=q+1$ then we can delete a point of $\mathcal{P}'$ in such a way that we obtain an integral point set $\mathcal{P}''$ with $e=1$ in the notation of 5. Thus $\mathcal{P}''\simeq(1\pm\omega_q i)\cdot\square_q$. Since $\mathcal{P}''$ is maximal due to Lemma 4 we have a contradiction. □

5. Maximal integral point sets in the plane $\mathbb{Z}_n^2$

Due to Theorem 1 for the determination of $\mathcal{I}(\mathbb{Z}_n,2)$ we only need to consider the cases $n=p^r$.

Lemma 22.

$$\mathcal{I}(\mathbb{Z}_{p^{r+1}},2) \leq p^2\cdot\mathcal{I}(\mathbb{Z}_{p^r},2).$$

Proof. We consider the natural ring epimorphism $\nu:\mathbb{Z}_{p^{r+1}}\to\mathbb{Z}_{p^r}$. If $\mathcal{P}$ is an integral point set in $\mathbb{Z}_{p^{r+1}}^2$ then $\nu(\mathcal{P})$ is an integral point set in $\mathbb{Z}_{p^r}^2$. □

For $p \geq 3$ we have the following examples of integral point sets in $\mathbb{Z}_{p^r}^2$ with big cardinality (with some abuse of notation in the third case).

$$\left\{\left(i, j \cdot p^{\lceil \frac{r}{2} \rceil}\right) \mid i,j \in \mathbb{Z}_{p^r}\right\},$$
$$\left\{\left(i, i\omega_{\mathbb{Z}_{p^r}} + j \cdot p^{\lceil \frac{r}{2} \rceil}\right) \mid i,j \in \mathbb{Z}_{p^r}\right\}, \text{ and}$$
$$(1, \pm\omega_{\mathbb{Z}_p}) \cdot \square_{\mathbb{Z}_p} + \{(p \cdot a, p \cdot b) \mid a,b \in \mathbb{Z}_{p^r}\} \text{ for } r = 2.$$

Each of these examples has cardinality $p^r \cdot p^{\lfloor \frac{r}{2} \rfloor}$.

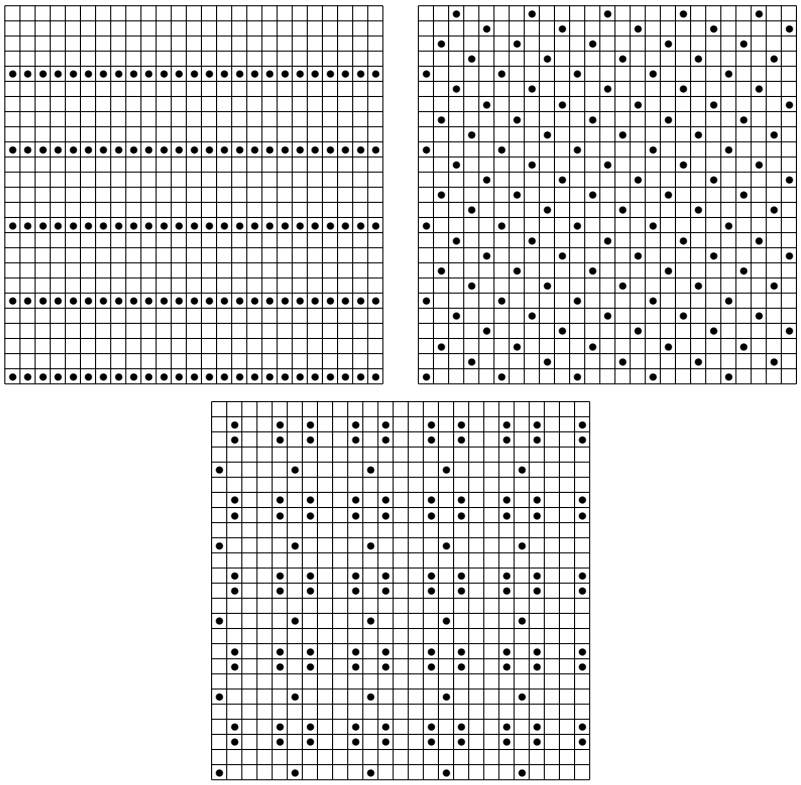

FIGURE 2. Three maximal integral point sets over $\mathbb{Z}_{25}^2$ of cardinality 125.

Conjecture 1. *The above list is the complete list of maximum integral point sets in $\mathbb{Z}_{p^r}^2$ up to isomorphism.*

So far we do not even know the automorphism group of $\mathbb{Z}_n^2$ with respect to Δ. But with Definition 6 Conjecture 1 is well defined. Using Lemma 5 we know at least a subgroup of the automorphism group. If there are any further automorphisms is an open question which has to be analyzed in the future.

Theorem 8. *For $p \geq 3$ we have $\mathcal{I}(\mathbb{Z}_{p^2}, 2) = p^3$ and the above list of extremal examples is complete.*

Proof. With $\mathcal{I}(\mathbb{Z}_p, 2) = p$, Lemma 22 and the examples we get $\mathcal{I}(\mathbb{Z}_{p^2}, 2) = p^3$. Let $\mathcal{P}$ be a maximum integral point set in $\mathbb{Z}_{p^2}$. By S denote the lower left $p \times p$-square of $\mathbb{Z}_{p^2}$

$$S := \{(i, j) + \mathbb{Z}_{p^2}^2 \mid 0 \leq i, j \leq p-1,\, i, j \in \mathbb{Z}\}.$$

Using Theorem 7 and Lemma 22 we can deduce that for each $(u, v) \in \mathbb{Z}_{p^2}^2$ we have

$$|\mathcal{P} \cap ((u, v) + S)| \leq p.$$

Since we can tile $\mathbb{Z}_{p^2}$ with p^2 such sets (including $S + (u, v)$) equality must hold. After a transformation we can assume that $\mathcal{P} \cap S$ equals one of the three following possibilities

(1) $\{(i, 0) \mid 0 \leq i \leq p-1\}$,
(2) $\{(i, \omega_{\mathbb{Z}_p} i) \mid 0 \leq i \leq p-1\}$, or
(3) $(1, \pm\omega_{\mathbb{Z}_p}) \cdot \square_{\mathbb{Z}_p}$.

In the first case we consider $\mathcal{P} \cap (S + (1, 0))$. With Lemma 17 we get $(p, 0) \in \mathcal{P}$ and iteratively we get $(i, 0) \in \mathcal{P}$ for all $i \in \mathbb{Z}_{p^2}$. Now we consider $\mathcal{P} \cap (S + (0, 1))$ and conclude $\mathcal{P} = \{(i, j \cdot p) \mid i, j \in \mathbb{Z}_{p^2}\}$. With the same argument we can derive $\mathcal{P} = \{(i, i\omega_{\mathbb{Z}_p} + j \cdot p) \mid i, j \in \mathbb{Z}_{p^2}\}$ in the second case and $\mathcal{P} = (1, \pm\omega_{\mathbb{Z}_p}) \cdot \square_{\mathbb{Z}_p} + \{(p \cdot a, p \cdot b) \mid a, b \in \mathbb{Z}_{p^r}\}$ in the third case. □

6. Maximal integral point sets with no three collinear points

In this and the next section we study the interplay between the integrality condition for a point set and further common restrictions for lines and circles.

Definition 9. *A set of r points $(u_i, v_i) \in \mathcal{R}^2$ is said to be **collinear** if there are $a, b, t_1, t_2, w_i \in \mathcal{R}$ with*

$$a + w_i t_1 = u_i \quad \text{and} \quad b + w_i t_2 = v_i.$$

There is an easy necessary criterion to decide whether three points are collinear.

Lemma 23. *If three points (u_1, v_1), (u_2, v_2), and $(u_3, v_3) \in \mathcal{R}^2$ are collinear then it holds*

$$\left| \begin{pmatrix} u_1 & v_1 & 1 \\ u_2 & v_2 & 1 \\ u_3 & v_3 & 1 \end{pmatrix} \right| = 0.$$

If $\mathcal{R}$ is an integral domain the above criterion is also sufficient. The proof is easy and left to the reader.

Definition 10. *By $\overline{\mathcal{I}}(\mathcal{R}, 2)$ we denote the maximum cardinality of an integral point set with no three collinear points.*

Lemma 24.

$$\overline{\mathcal{I}}(\mathcal{R}, 2) \leq 2 \cdot |\mathcal{R}|.$$

Proof. We ignore the integrality condition and consider the lines $l_i = \{(i, r) \mid r \in \mathcal{R}\}$ for all $i \in \mathcal{R}$. □

Lemma 25. *If $-1 \in \square_q$ we have $\overline{\mathcal{I}}(\mathbb{F}_q, 2) \leq \frac{q+3}{2}$ and for $-1 \notin \square_q$ we have $\overline{\mathcal{I}}(\mathbb{F}_q, 2) \leq \frac{q+1}{2}$.*

Proof. Let $\mathcal{P}$ be an integral point set over $\mathbb{F}_q$ without a collinear triple. We choose a point $p \in \mathcal{P}$. The directions of p to the other points p' of $\mathcal{P}$ are pairwise different. Since there are at most $\frac{q+3}{2}$ or $\frac{q+1}{2}$ different directions in an integral point set over $\mathbb{F}_q$ (Lemma 16), we obtain $|\mathcal{P}| \leq \frac{q+5}{2}$ for $-1 \in \square_q$ and $|\mathcal{P}| \leq \frac{q+3}{2}$ for $-1 \notin \square_q$. Suppose that this upper bound is achieved. So all points must have exactly one *neighbor* in direction 0 and one in direction ∞. Thus $|\mathcal{P}|$ must be even in this case, which is a contradiction due to Lemma 7. □

Using an element $z \in \mathcal{R}'$ with $z\overline{z} = 1$ we can describe a good construction for lower bounds. Actually this equation describes something like a circle with radius one. An example for $q = 31$ is depicted in Figure 3.

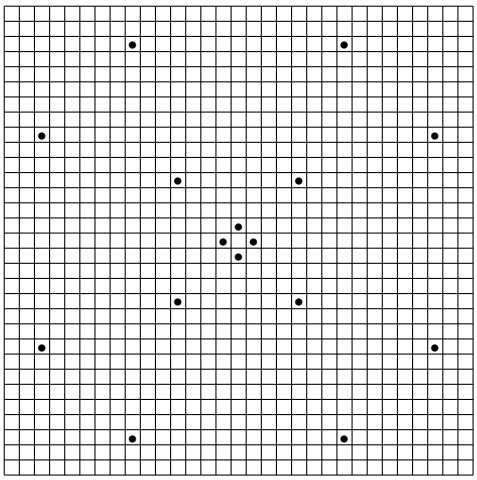

FIGURE 3. Integral point set corresponding to the construction from Lemma 26 for $q = 31$.

Lemma 26. *For $z \in \mathcal{R}'$ with $z\overline{z} = 1$ the set $\mathcal{P} = \{z^{2i} \mid i \in \mathbb{N}\}$ is an integral point set.*

Proof. With $c := a - b$ we have

$$\begin{aligned} d(z^{2a}, z^{2b}) &= (z^{2a} - z^{2b}) \cdot \overline{(z^{2a} - z^{2b})} = (z^{2c} - 1) \cdot \overline{z^{2c} - 1} \\ &= 2 - z^{2c}2 - \overline{z^{2c}} = (\underbrace{z^c i - \overline{z^c} i}_{\in \mathcal{R}})^2 \end{aligned}$$

□

We remark that the set $\mathcal{P}' = \{z^{2i+1} \mid i \in \mathbb{N}\}$ is an isomorphic integral point set. The set of solutions of $z\overline{z} = 1$ forms a cyclic multiplicative group G due to Lemma 9. From Lemma 8 we know that G has size $q + 1$ for $-1 \notin \square_q$ and size $q - 1$ if $-1 \in \square_q$. So by Lemma 26 we get a construction of an integral point set in $\mathbb{F}_q$ which is near the upper bound of Lemma 25. We only have to prove that our construction does not produce three collinear points in $\mathbb{F}_q$.

Lemma 27. *For $\mathcal{R} = \mathbb{F}_q$ with $2 \nmid q$ the point set from Lemma 26 contains no collinear triple.*

Proof. We assume that we have three pairwise different points p_1, p_2, p_3 in $\mathcal{R}'$ which are collinear. So there exist a, b, c, d, t_1, t_2, and t_3 in $\mathcal{R}$ fullfilling

$$\begin{aligned} p_1 &= a + bt_1 + (c + dt_1)i, \\ p_2 &= a + bt_2 + (c + dt_2)i, \\ p_3 &= a + bt_3 + (c + dt_3)i, \end{aligned}$$

and $t_i \neq t_j$ for $i \neq j$. Since $p_i\overline{p_i} = 1$ we have

$$\begin{aligned} a^2 + 2abt_1 + b^2t_1^2 + c^2 + 2cdt_1 + d^2t_1^2 &= 1, \\ a^2 + 2abt_2 + b^2t_2^2 + c^2 + 2cdt_2 + d^2t_2^2 &= 1, \\ a^2 + 2abt_3 + b^2t_3^2 + c^2 + 2cdt_3 + d^2t_3^2 &= 1. \end{aligned}$$

Subtracting the first two and the last two equations yields

$$\begin{aligned} 2ab(t_1 - t_2) + b^2(t_1 - t_2)(t_1 + t_2) + 2cd(t_1 - t_2) + d^2(t_1 - t_2)(t_1 + t_2) &= 0, \\ 2ab(t_2 - t_3) + b^2(t_2 - t_3)(t_2 + t_3) + 2cd(t_2 - t_3) + d^2(t_2 - t_3)(t_2 + t_3) &= 0. \end{aligned}$$

Because $t_1 \neq t_2$, $t_2 \neq t_3$ and $\mathcal{R}$ is an integral domain we obtain

$$\begin{aligned} 2ab + b^2(t_1 + t_2) + 2cd + d^2(t_1 + t_2) &= 0, \\ 2ab + b^2(t_2 + t_3) + 2cd + d^2(t_2 + t_3) &= 0. \end{aligned}$$

Another subtraction yields

$$b^2(t_1 - t_3) + d^2(t_1 - t_3) = 0 \quad \Rightarrow \quad b^2 + d^2 = 0.$$

Inserting yields

$$2ab + 2cd = 0 \quad \Leftrightarrow \quad 2ab = -2cd$$

and

$$a^2 + c^2 = 1.$$

Thus

$$4a^2b^2 = 4c^2d^2 \quad \Leftarrow \quad (a^2 + c^2)4b^2 = 0 \quad \Leftrightarrow \quad b = 0.$$

In the same way we obtain $d = 0$ and so $p_1 = p_2 = p_3$, which is a contradiction. □

Corollary 4. *For $-1 \notin \square_q$ we have $\overline{\mathcal{I}}(\mathbb{F}_q, 2) = \frac{q+1}{2}$ and for $-1 \in \square_q$ we have $\frac{q-1}{2} \leq \overline{\mathcal{I}}(\mathbb{F}_q, 2) \leq \frac{q+3}{2}$.*

Conjecture 2. *For $-1 \in \square_q$ we have $\overline{\mathcal{I}}(\mathbb{F}_q, 2) = \frac{q-1}{2}$.*

We remark that Conjecture 2 would be true for quadrance graphs. Following the proof of Lemma 25 we would get $\frac{q-1}{2}$ as an upper bound for $q \equiv 1 \mod 4$. Since $z^c - \overline{z^c} = 0$ would imply $2c = q - 1$ the construction from Lemma 26 does not contain a pair of points with squared distance 0.

7. Integral point sets in general position

Our best construction for integral point sets where no three points are collinear consists of points on a *circle*. So it is interesting to study integral point sets where additionally no 4 points are allowed to be situated on a *circle*.

Definition 11. *Points $p_i = (x_i, y_i)$ in $\mathcal{R}^2$ are said to be situated on a circle if there exist $a, b, r \in \mathcal{R}$ with $(x_i - a)^2 + (y_i - b)^2 = r$ for all i.*

We have the following condition:

Lemma 28. *Four distinct points $p_i = (x_i, y_i)$ in $\mathbb{F}_q^2$ which contain no collinear triple are situated on a circle if and only if*

$$\left| \begin{pmatrix} x_1 & y_1 & x_1^2 + y_1^2 & 1 \\ x_2 & y_2 & x_2^2 + y_2^2 & 1 \\ x_3 & y_3 & x_3^2 + y_3^2 & 1 \\ x_4 & y_4 & x_4^2 + y_4^2 & 1 \end{pmatrix} \right| = 0.$$

Proof. If there exist $a, b, r \in \mathbb{F}_q$ with $(x_i-a)^2+(y_i-b)^2 = r$ for all $1 \le i \le 4$ then the determinant clearly vanishes since $r = (x_i - a)^2 + (y_i - b)^2 = (x_i^2 + y_i^2) - 2a \cdot x_i - 2b \cdot y_i + (a^2 + b^2)$. For the other direction we consider the unique circle $\mathcal{C}$ through the points (x_1, y_1), (x_2, y_2), (x_3, y_3) described by the parameters $a, b, r \in \mathbb{F}_q$. With the same idea as before we get

$$\left| \begin{pmatrix} x_1 & y_1 & 0 & 1 \\ x_2 & y_2 & 0 & 1 \\ x_3 & y_3 & 0 & 1 \\ x_4 & y_4 & (x_4 - a)^2 + (y_4 - b)^2 - r & 1 \end{pmatrix} \right| = 0.$$

If (x_4, y_4) is not on the circle $\mathcal{C}$ then we can develop the determinant after the third column and obtain

$$\left| \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} \right| = 0.$$

which is a contradiction to the fact that (x_1, y_1), (x_2, y_2), and (x_3, y_3) are not collinear, see Lemma 23. □

We remark that for arbitrary commutative rings $\mathcal{R}$ the determinant criterion from Lemma 28 is a necessary condition.

Definition 12. *By $\dot{\mathcal{I}}(\mathcal{R}, 2)$ we denote the maximum cardinality of an integral point set in $\mathcal{R}^2$ which is in general position, this means that it contains no collinear triple and no four points on a circle.*

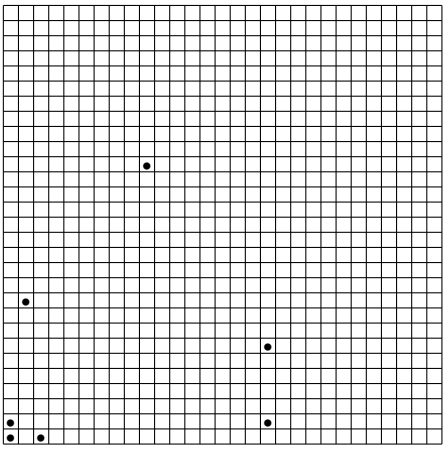

FIGURE 4. A maximum integral point set in general position over $\mathbb{F}_{29}^2$.

As a shorthand for the conditions of Definition 12 we also say that the points are in general position. An example of seven points over $\mathbb{F}_{29}^2$ in general position which pairwise integral distances is depicted in Figure 4. As trivial upper bound we have $\dot{\mathcal{I}}(\mathcal{R}, 2) \le \overline{\mathcal{I}}(\mathcal{R}, 2)$. By applying the automorphisms of $\mathbb{F}_q^2$ with respect to Δ we see that they conserve circles.

Via an exhaustive combinatorial search we have determined $\dot{\mathcal{I}}(\mathbb{F}_p, 2)$ for small values of p, see Table 1. Since it is a non-trivial task to determine these numbers exactly, at least for $p \ge 100$, we give an outline of our used algorithm.

n	$\dot{\mathcal{I}}(n,2)$	n	$\dot{\mathcal{I}}(n,2)$	n	$\dot{\mathcal{I}}(n,2)$	n	$\dot{\mathcal{I}}(n,2)$	n	$\dot{\mathcal{I}}(n,2)$
2	4	17	5	41	9	67	9	97	11
3	2	19	5	43	8	71	11	101	13
5	4	23	5	47	7	73	10	103	11
7	3	29	7	53	9	79	11	107	11
11	4	31	6	59	9	83	11	109	12
13	5	37	7	61	10	89	11	113	12

TABLE 1. Values of $\dot{\mathcal{I}}(\mathbb{F}_p,2) = \dot{\mathcal{I}}(\mathbb{Z}_p,2)$ for small primes p.

Algorithm 1. ***(Generation of integral point sets in general position over*** $\mathbb{F}_\mathbf{q}$***)***
Input: q
Output: Integral point sets $\mathcal{P} \subset \mathbb{F}_q$ *in general position*
begin
  $\mathcal{P} = [(0,0),(0,1)]$
  $blocked[(0,0)] = blocked[(0,1)] = true$
  loop over $d \in \mathbb{F}_q$ $\mathcal{L}_d = []$ **end**
  loop over $x \in \mathbb{F}_q^2 \backslash \{(0,0),(0,1)\}$
    $blocked[x] = false$
    if $\Delta((0,0),x) = 0$ **or** $\Delta((0,1),x) = 0$ **then** $blocked[x] = true$ **end**
    if $collinear((0,0),(0,1),x)$ **then** $blocked[x] = true$ **end**
    if $blocked[x] = true$ **then** $\mathcal{L}_{get\_direction(x)}.append(x)$ **end**
  end
  $add\_point(\mathcal{P},0)$
end

So far almost nothing is done. We restrict our search to integral point sets $\mathcal{P}$ of cardinality at least 3. So we may assume that $\mathcal{P}$ contains the points $(0,0)$ and $(0,1)$. For each $x \in \mathbb{F}_q^2$ the variable $blocked[x]$ says whether x can be appended to $\mathcal{P}$ without destroying the property integral point set or general position. The lists $\mathcal{L}_d$ cluster the points of $\mathbb{F}_q^2$ according to their direction. The fact that $\mathcal{P}$ can contain besides $(0,0)$ and $(0,1)$ at most one member from each $\mathcal{L}_d$ can be used to prune the search tree if one searches only for integral point sets with maximum cardinality.

Algorithm 2. ***(*add_point*)***
Input: Lower bound l *on the direction and an integral point set* $\mathcal{P}$
Output: Integral point sets $\mathcal{P} \subset \mathbb{F}_q$ *in general position*
begin
  loop over $d \in \mathbb{F}_q$ **with** $d \geq l$
    loop over $x \in \mathcal{L}_d$ **with** $blocked[x] = false$
      if $canon\_check(\mathcal{P},x) = true$ **then**
        $\mathcal{P}.append(x)$
        block all $y \in \mathbb{F}_q^2$ *where* $\Delta(y,x) = 0$ **or** $collinear(p_1,x,y) = true$
        or $on\_circle(p_1,p_2,x,y) = true$ *for* $p_1,p_2 \in \mathcal{P}$
        output $\mathcal{P}$
        $add\_point(\mathcal{P},d+1)$
        unblock
        $\mathcal{P}.remove(x)$
      end

```
        end
    end
end
```

The subroutine *add_point* simply adds another point to the point set $\mathcal{P}$ and maintains the set of further candidates for adding a further point. Some lookahead is possible to implement. Since the automorphism group of $\mathbb{F}_q^2$ with respect to Δ is very large we would obtain lots of isomorphic integral point sets if we do without isomorphism pruning. With the framework of orderly generation, see i.e. [21], it is possible to write a subroutine *canon_check* that let our algorithm output a complete list of pairwise non-isomorphic integral point sets in general position. For our purpose it suffices to have a subroutine *canon_check* that rejects the majority of isomorphic copies but as a return has a good performance. Let $m : \mathbb{F}_q^2 \to \mathbb{F}_q^2$, $(x, y) \mapsto (-x, y)$ the automorphism that mirrors at the y-axis and let $\preceq$ be a total ordering on the points of $\mathbb{F}_q^2$ if $u \prec v$ for $direction(u) < direction(v)$. For the latter comparison we use an arbitrary but fix total ordering of $\mathbb{F}_q$, where 0 is the smallest element and which is also used for the looping over $\mathbb{F}_q$. By $\mathcal{P}[2]$ we denote the third point of a list $\mathcal{P}$.

Algorithm 3. ***(canon_check)***
Input: An integral point set $\mathcal{P}$
Output: Returns false if $\mathcal{P}$ *should be rejected due to isomorphism pruning*

```
begin
    loop over some disjoint triples (u,v,w) ∈ P × P × P with δ²(u,v) ≠ 0
        determine an automorphism α with α(u) = (0,0) and α(v) = (0,1)
        if α(w) ≺ P[2] or m(α(w)) ≺ P[2] then return false end
    end
    return true
end
```

For further examples we refer to [15] where we list the coordinates of one extremal example for $p \leq 113$.

A formal proof of the correctness of the proposed algorithm is not difficult but a bit technical and so left to the reader. We remark that there are several non-isomorphic integral point sets in general position which achieve the upper bound $\dot{\mathcal{I}}(\mathbb{Z}_n, 2)$. So far we have no insight in their structure or in the asymptotic behavior of. $\dot{\mathcal{I}}(\mathbb{Z}_n, 2)$. It seems that we have $\dot{\mathcal{I}}(\mathbb{Z}_p, 2) \geq 7$ for all sufficiently large primes p. This is interesting because the question whether $\dot{\mathcal{I}}(\mathbb{Z}, 2) \geq 7$ is unsolved so far. In other words, there is no known 7_2-cluster [9]. This is a set of seven points in the plane, no three points on a line, no four points on a circle, where the coordinates and the pairwise distances are integral.

Conjecture 3. *For each* l *there is a* p' *so that for all* $p \geq p'$ *we have* $\dot{\mathcal{I}}(\mathbb{Z}_p, 2) \geq l$.

8. Conclusion and outlook

In this paper we have considered sets of points $\mathcal{P}$ in the affine plane $\mathrm{AG}(2, q)$ with pairwise integral distances. We have presented several connections to other discrete structures and problems. Some questions concerning maximum cardinalities and complete classifications of extremal examples remain open. Clearly similar questions could be asked in $\mathrm{AG}(3, q)$ or higher dimensional spaces.

Acknowledgment

I am thankful to Aart Blokhuis, Stancho Diemiev, Michael Kiermaier, Harald Meyer, and Ivo Radloff whose comments were very helpful during the preparation of this article.

References

[1] A. Antonov and M. Brancheva. Algorithm for finding maximal Diophantine figures. In *Spring Conference 2007 of the Union of Bulgarian Mathematicians*, 2007.

[2] R.D. Baker, G.L. Ebert, J. Hemmeter, and A. Woldar. Maximal cliques in the Paley graph of square order. *J. Stat. Plann. Inference*, 56(1):33–38, 1996.

[3] A. Blokhuis. On subsets of $GF(q^2)$ with square differences. *Indag. Math.*, 46:369–372, 1984.

[4] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. Comb. Theory, Ser. A*, 86(1):187–196, 1999.

[5] P.J. Cameron, G.R. Omidi, and B. Tayfeh-Rezaie. 3-designs from PGL$(2, q)$. *The Electronic Journal of Combinatorics*, 13(1), 2006.

[6] L. Carlitz. A theorem on permutations in a finite field. *Proc. Amer. Math. Soc.*, 11:456–459, 1960.

[7] L.E. Dickson. *Linear groups. With an exposition of the Galois field theory. With an introduction by Wilhelm Magnus. Unabridged and unaltered republ. of the first ed.* New York: Dover Publications, Inc. XVI, 312 p. , 1958.

[8] S. Dimiev. A setting for a Diophantine distance geometry. *Tensor (N.S.)*, 66(3):275–283, 2005.

[9] R.K. Guy. *Unsolved problems in number theory. 2nd ed.* Unsolved Problems in Intuitive Mathematics. 1. New York, NY: Springer- Verlag. xvi, 285 p. , 1994.

[10] H. Harborth. Integral distances in point sets. In *Butzer, P. L. (ed.) et al., Karl der Grosse und sein Nachwirken. 1200 Jahre Kultur und Wissenschaft in Europa. Band 2: Mathematisches Wissen. Turnhout: Brepols*, pages 213–224. 1998.

[11] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen. 134. Berlin-Heidelberg-New York: Springer-Verlag. XII, 793 S. mit 15 Abb. , 1967.

[12] T. Khoon Lim and C.E. Praeger. On generalised Paley graphs and their automorphism groups. *ArXiv Mathematics math/0605252*, May 2006.

[13] A. Kohnert and S. Kurz. Integral point sets over $\mathbb{Z}_n^m$. *Electronic Notes in Discrete Mathematics*, 27:65–66, 2006.

[14] T. Kreisel and S. Kurz. There are integral heptagons, no three points on a line, no four on a circle. *submitted*, 2006.

[15] S. Kurz. Coordinates of maximal integral point sets over $\mathbf{F}_q^2$ in general position. http://www.wm.uni-bayreuth.de/index.php?id=322.

[16] S. Kurz. *Konstruktion und Eigenschaften ganzzahliger Punktmengen*. PhD thesis, Bayreuth. Math. Schr. 76. Universität Bayreuth, 2006.

[17] S. Kurz and A. Wassermann. On the minimum diameter of plane integral point sets. *submitted*, 2007.

[18] A. Neumaier. Cliques and claws in edge-transitive strongly regular graphs. *Math. Z.*, 174:197–202, 1980.

[19] A. Neumaier. Regular cliques in graphs and special 1,5-designs. Finite geometries and designs, Proc. 2nd Isle of Thorns Conf. 1980, Lond. Math. Soc. Lect. Note Ser. 49, 244–259, 1981.

[20] L.C. Noll and D.I. Bell. n-clusters for $1 < n < 7$. *Math. Comput.*, 53(187):439–444, 1989.

[21] R.C. Read. Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. *Ann. Discrete Math.*, 2:107–120, 1978.

[22] W.M. Schmidt. *Equations over finite fields. An elementary approach. 2nd ed.* Heber City, UT: Kendrick Press. x, 333 p. , 2004.

[23] J. Sheehan. Finite Ramsey theory is hard. Combinatorial mathematics VIII, Proc. 8th Aust. Conf., Geelong/ Aust. 1980, Lect. Notes Math. 884, 99-106 (1981)., 1981.

[24] S.Y. Song. Commutative association schemes whose symmetrizations have two classes. *J. Algebr. Comb.*, 5(1):47–55, 1996.

[25] D.B. Surowski. Automorphism groups of certain unstable graphs. *Math. Slovaca*, 53(3):215–232, 2003.

[26] P. Sziklai. On subsets of GF(q^2) with dth power differences. *Disc. Math.*, 208-209:547–555, 1999.

[27] L.A. Vinh. On chromatic number of unit-quadrance graphs (finite euclidean graphs). *ArXiv Mathematics math/0510092*, 2005.

[28] L.A. Vinh. Quadrance polygons, association schemes and strongly regular graphs. *ArXiv Mathematics math/0509598*, 2005.

[29] L.A. Vinh. Quadrance graphs. *Australian Mathematical Society Gazette*, 33(5):330–332, 2006.

[30] L.A. Vinh. Some colouring problems for unit-quadrance graphs. *ArXiv Mathematics math/0606482*, 2006.

[31] N. Wage. Character sums and Ramsey properties of generalized Paley graphs. *INTEGERS: Electronic Journal of Combinatorial Number Theory*, 6, 2006.

[32] N.J. Wildberger. *Divine proportions. Rational trigonometry to universal geometry.* Kingsford: Wild Egg. xx, 300 p. , 2005.

Sascha Kurz, Fakultät für Mathematik, Physik und Informatik, Universität Bayreuth, Germany
E-mail address: sascha.kurz@uni-bayreuth.de