Integral point sets over finite fields

Sascha Kurz
sascha.kurz@uni-bayreuth.de
www.wm.uni-bayreuth.de

University of Bayreuth

1. Workshop on Integral Figure Geometry in Sofia,
05.-12.10.2007
Integral point sets over finite fields

Introduction

Integral point sets

Definition

(1) By $d^2(x, y) = \sum_{i=1}^{m} (x_i - y_i)^2$ we denote the squared distance between two points $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_m) \in \mathbb{F}_q^m$. 

(2) By $\mathbb{F}_q^2 := \{s^2 | s \in \mathbb{F}_q\}$ we denote the set of squares.

(3) Two points $x$ and $y$ are at integral distance if $d^2(x, y) \in \mathbb{F}_q^2$.

(4) An integral point set $P$ over $\mathbb{F}_q^m$ is a set of $n$ points in the $m$-dimensional space $\mathbb{F}_q^m$ with pairwise integral distances.
Integral point sets

Definition

(1) By $d^2(x, y) = \sum_{i=1}^{m} (x_i - y_i)^2$ we denote the squared distance between two points $x = (x_1, \ldots, x_m)$,
    $y = (y_1, \ldots, y_m) \in \mathbb{F}_q^m$.

(2) By $\square_q := \{ s^2 \mid s \in \mathbb{F}_q \}$ we denote the set of squares.
Integral point sets over finite fields

Introduction

Integral point sets

Definition

(1) By $d^2(x, y) = \sum_{i=1}^{m} (x_i - y_i)^2$ we denote the squared distance between two points $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_m) \in \mathbb{F}_q^m$.

(2) By $\square_q := \{ s^2 \mid s \in \mathbb{F}_q \}$ we denote the set of squares.

(3) Two points $x$ and $y$ are at integral distance if $d^2(x, y) \in \square_q$. 
Integral point sets over finite fields

Introduction

Integral point sets

Definition

(1) By $d^2(x, y) = \sum_{i=1}^{m} (x_i - y_i)^2$ we denote the squared distance between two points $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_m) \in \mathbb{F}_q^m$.

(2) By $\square_q := \{ s^2 \mid s \in \mathbb{F}_q \}$ we denote the set of squares.

(3) Two points $x$ and $y$ are at integral distance if $d^2(x, y) \in \square_q$.

(4) An integral point set $\mathcal{P}$ over $\mathbb{F}_q$ is a set of $n$ points in the $m$-dimensional space $\mathbb{F}_q^m$ with pairwise integral distances.
Figure: An integral point set of cardinality $q = 29$ in $\mathbb{F}_{29}^2$. 
Another integral line

Figure: Another integral point set of cardinality $q = 29$ in $\mathbb{F}_{29}^2$. 
Integral point sets over finite fields

Introduction

Figure: Another integral point set of cardinality $q = 29$ in $\mathbb{F}_{29}^2$. 
Maximum cardinality of an integral point set

Definition

By $\mathcal{I}(\mathbb{F}_q, 2)$ we denote maximum cardinality of an integral point set in $\mathbb{F}_q^2$. 
Maximum cardinality of an integral point set

Definition

By $\mathcal{I}(\mathbb{F}_q, 2)$ we denote maximum cardinality of an integral point set in $\mathbb{F}_q^2$.

Lemma (K. 2006)

$q \leq \mathcal{I}(\mathbb{F}_q, 2) \leq q^2$
Definition

By $\mathcal{I}(F_q, 2)$ we denote maximum cardinality of an integral point set in $F_q^2$.

Lemma (K. 2006)

$q \leq \mathcal{I}(F_q, 2) \leq q^2$

Lemma (K. 2006)

$\mathcal{I}(F_{2^r}, 2) = |F_{2^r}^2| = 2^{2r} = q^2$.

Proof

For each $(x_1, y_1), (x_2, y_2) \in F_{2^r}^2$, we have

$$(x_1 - x_2)^2 + (y_1 - y_2)^2 = (x_1 + x_2 + y_1 + y_2)^2.$$
The graph of integral distances

Definition

By $G_q$ we denote the graph consisting of $\mathbb{F}_q^2$ as vertices, where the edges correspond to integral distances.
The graph of integral distances

Definition

By $\mathcal{G}_q$ we denote the graph consisting of $\mathbb{F}_q^2$ as vertices, where the edges correspond to integral distances.

Lemma (Kiermaier and K. 2007)

$\mathcal{G}_q$ is a strongly regular graph with parameters $(v, k, \lambda, \mu) =$

$$
\left( q^2, \frac{(q-1)(q+3)}{2}, \frac{(q+1)(q+3)}{4} - 3, \frac{(q+1)(q+3)}{4} \right)
$$

for $q \equiv 1 \pmod{4}$ and $(v, k, \lambda, \mu) =$

$$
\left( q^2, \frac{q^2 - 1}{2}, \frac{q^2 - 1}{4} - 1, \frac{q^2 - 1}{4} \right)
$$

for $q \equiv 3 \pmod{4}$. 
Definition (Neumaier, 1980)

A clique $C$ is called regular if every point not in $C$ is adjacent with the same number $e > 0$ of points in $C$. 
Clique of strongly regular graphs

Definition (Neumaier, 1980)
A clique $C$ is called regular if every point not in $C$ is adjacent with the same number $e > 0$ of points in $C$.

Lemma (Neumaier, 1980)
Let $G$ be a strongly regular graph with parameters

$$
\nu = \mu^{-1}(\mu + (m - 1)(n - m))(\mu + m(n + 1 - m)),
$$

$$
k = \mu + m(n - m), \quad \lambda = \mu + n - 2m,
$$

then we have

1. a clique $C$ is regular iff $|C| = 1 + m^{-1}k$ and $e = m^{-1}\mu$, and
2. a non-regular clique contains less than $1 + m^{-1}k$ points.
Corollary

For $2 
\n\n\not\divides q$ we have $I(\mathbb{F}_q, 2) = q$. 
For $2 
mid q$ we have $\mathcal{I}(\mathbb{F}_q, 2) = q$.

By $\mathcal{P}(q)$ we denote the Paley graph, which consists of $\mathbb{F}_q$ as vertices. Two nodes $u, v \in \mathbb{F}_q$ are joined by an edge iff $u - v$ is a square.
Maximum cardinality and old friends

**Corollary**
For $2 
\n\not| q$ we have $\mathcal{I}(\mathbb{F}_q, 2) = q$.

**Definition**
By $\mathcal{P}(q)$ we denote the Paley graph, which consists of $\mathbb{F}_q$ as vertices. Two nodes $u, v \in \mathbb{F}_q$ are joined by an edge iff $u - v$ is a square.

**Lemma (Blokhuys, 1984)**
If $q \equiv 3 \mod 4$ then we have $\mathcal{G}_q \simeq \mathcal{P}(q^2)$ and cliques of size $q$ correspond to lines in $\mathbb{F}_q^2$. 
Directions in $\mathbb{F}_q^2$

**Definition**
The direction of a point $(x, y) \in \mathbb{F}_q^2$ is given by $\frac{y}{x} \in \mathbb{F}_q \cup \{\infty\}$.

**Theorem** ((Ball, Blokhuis, Brouwer, Storme, Szőnyi, 1999))
Let $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$, 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 $N = 1$. 

Classification of integral point sets with maximum cardinality

Theorem (K. 2007)

If $P$ is an integral point set over $\mathbb{F}_q^2$ where $q = p \equiv 1 \mod 4$ then $P$ is isomorphic to

(1) the line $(1, 0) \cdot \mathbb{F}_q$,

(2) the line $(1, \omega_q) \cdot \mathbb{F}_q$, or

(3) the cross $(1, \pm \omega_q) \cdot \Box_q$,

where $\omega_q^2 = -1$. 

Remark

For $q = p^r$ with $r > 2$ we additionally have integral point sets of cardinality $q$ being isomorphic to sub vector spaces like $\{(x, y) | x, y \in \mathbb{F}_r/2q\}$ for $r \equiv 0 \mod 2$. 

Classification of integral point sets with maximum cardinality

**Theorem (K. 2007)**

If $P$ is an integral point set over $\mathbb{F}_q^2$ where $q = p \equiv 1 \mod 4$ then $P$ is isomorphic to

1. the line $(1, 0) \cdot \mathbb{F}_q$,
2. the line $(1, \omega_q) \cdot \mathbb{F}_q$, or
3. the cross $(1, \pm \omega_q) \cdot \mathbb{F}_q^r$

where $\omega_q^2 = -1$.

**Remark**

For $q = p^r$ with $r \geq 2$ we additionally have integral point sets of cardinality $q$ being isomorphic to sub vector spaces like

$$\left\{ (x, y) \mid x, y \in \mathbb{F}_q^{r/2} \right\}$$

for $r \equiv 0 \mod 2$. 


Definition

By $I(\mathbb{F}_q, 2)$ we denote the maximum cardinality of an integral point set in $\mathbb{F}_q^2$ where no three points are collinear.
No three points on a line

**Definition**

By \( \overline{I}(\mathbb{F}_q, 2) \) we denote the maximum cardinality of an integral point set in \( \mathbb{F}_q^2 \) where no three points are collinear.

**Theorem (Segre, 1967)**

For \( 2 \mid q \) we have \( \overline{I}(\mathbb{F}_q, 2) = q + 2 \).
Integral point sets over finite fields

No three points on a line

**Definition**

By $\overline{I}(\mathbb{F}_q, 2)$ we denote the maximum cardinality of an integral point set in $\mathbb{F}_q^2$ where no three points are collinear.

**Theorem (Segre, 1967)**

For $2 \mid q$ we have $\overline{I}(\mathbb{F}_q, 2) = q + 2$.

**Theorem (K. 2007)**

For $q \equiv 3 \pmod{4}$ we have $\overline{I}(\mathbb{F}_q, 2) = \frac{q+1}{2}$, for $q \equiv 1 \pmod{4}$ we have $\frac{q-1}{2} \leq \overline{I}(\mathbb{F}_q, 2) \leq \frac{q+3}{2}$

and conjecture $\overline{I}(\mathbb{F}_q, 2) = \frac{q-1}{2}$.
Lemma (K. 2007)

For $z \in \mathbb{F}_q[x]/(x^2 + 1)$ with $z \bar{z} = 1$ the set $\mathcal{P} = \{z^{2i} \mid i \in \mathbb{N}\}$ is an integral point set in $\mathbb{F}_q[x]/(x^2 + 1) \simeq \mathbb{F}_q^2$. 
Integral point sets over finite fields
No four points on a circle

Definition
By $\mathcal{I}(\mathbb{F}_q, 2)$ we denote the maximum cardinality of an integral point set in $\mathbb{F}_q^2$ where no three points are collinear and no four points are situated on a circle.

Related open question (Erdős, Bell and Noll)
Are there seven points in the plane, no three on a line, no four on a circle, with pairwise integral distances and integral coordinates? (Do $7^2$-clusters exist?)

Remark
Without the integrality of the coordinates the question was answered positively very recently by Kreisel and K.
Integral point sets over finite fields
No four points on a circle

No four points on a circle

Definition

By \( \hat{I}(\mathbb{F}_q, 2) \) we denote the maximum cardinality of an integral point set in \( \mathbb{F}_q^2 \) where no three points are collinear and no four points are situated on a circle.

Related open question (Erdős, Bell and Noll)

Are there seven points in the plane, no three on a line, no four on a circle, with pairwise integral distances and integral coordinates? (Do 7\(_2\)-cluster exist?)
Integral point sets over finite fields

No four points on a circle

Definition

By \( \mathcal{I}(\mathbb{F}_q, 2) \) we denote the maximum cardinality of an integral point set in \( \mathbb{F}_q^2 \) where no three points are collinear and no four points are situated on a circle.

Related open question (Erdős, Bell and Noll)

Are there seven points in the plane, no three on a line, no four on a circle, with pairwise integral distances and integral coordinates? (Do \( 7_2 \)-cluster exist?)

Remark

Without the integrality of the coordinates the question was answered positively very recently by Kreisel and K.
Integral heptagon

Figure: Integral heptagon in general position with diameter 22270.
Do $7_2$-cluster exist?

**Lemma (K. 2007)**

A $7_2$-cluster in the Euclidean plane has a diameter greater than 520 000.
Do $7_2$-cluster exist?

**Lemma (K. 2007)**

A $7_2$-cluster in the Euclidean plane has a diameter greater than 520,000.

**Lemma (K. 2007)**

For finite fields we have

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\tilde{I}(n, 2)$</th>
<th>$n$</th>
<th>$\tilde{I}(n, 2)$</th>
<th>$n$</th>
<th>$\tilde{I}(n, 2)$</th>
<th>$n$</th>
<th>$\tilde{I}(n, 2)$</th>
<th>$n$</th>
<th>$\tilde{I}(n, 2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>17</td>
<td>5</td>
<td>41</td>
<td>9</td>
<td>67</td>
<td>9</td>
<td>97</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>19</td>
<td>5</td>
<td>43</td>
<td>8</td>
<td>71</td>
<td>11</td>
<td>101</td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>23</td>
<td>5</td>
<td>47</td>
<td>7</td>
<td>73</td>
<td>10</td>
<td>103</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>29</td>
<td>7</td>
<td>53</td>
<td>9</td>
<td>79</td>
<td>11</td>
<td>107</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>31</td>
<td>6</td>
<td>59</td>
<td>9</td>
<td>83</td>
<td>11</td>
<td>109</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>5</td>
<td>37</td>
<td>7</td>
<td>61</td>
<td>10</td>
<td>89</td>
<td>11</td>
<td>113</td>
<td>12</td>
</tr>
</tbody>
</table>
A maximum integral point set in general position over $\mathbb{F}_{29}^2$
Thank you very much for your attention.

References

- M. Kiermaier and S. Kurz: Inclusion-maximal integral point sets over finite fields, in preparation
- T. Kreisel and S. Kurz: There are integral heptagons, no three points on a line, no four on a circle, submitted
- S. Kurz: Integral point sets over finite fields, submitted