Integral point sets over $\mathbb{Z}_{\mathbf{n}}^{\mathbf{m}}$

Axel Kohnert

University of Bayreuth, Department of Mathematics, D-95440 Bayreuth, Germany

Sascha Kurz

University of Bayreuth, Department of Mathematics, D-95440 Bayreuth, Germany

Abstract

There are many papers studying properties of point sets in the Euclidean space $\mathbb{E}^m$ or on integer grids $\mathbb{Z}^m$, with pairwise integral or rational distances. In this article we consider the distances or coordinates of the point sets which instead of being integers are elements of $\mathbb{Z}/\mathbb{Z}n$, and study the properties of the resulting combinatorial structures.

Key words: integral distances, exhaustive search, finite rings, orderly generation,
1991 MSC: 52C10, 51E99

1 Introduction

There are many papers studying properties of point sets in the Euclidean space $\mathbb{E}^m$, with pairwise integral or rational distances (for short integral point sets or rational point sets, respectively), see [17] for an overview and applications. A recent collection of some classical open problems is given in [6, Section 5.11]. Some authors also require that the points are located on an integer grid $\mathbb{Z}^m$ [11,31]. In this paper we modify the underlying space and study instead of $\mathbb{Z}$ the integers modulo n, which we denote by $\mathbb{Z}_n$. This was a suggestion of S. Dimiev. Our motivation was to gain some insight for the original problem in $\mathbb{Z}^m$ and $\mathbb{E}^m$. In the next subsection we shortly repeat the basic facts and questions about integral point sets in $\mathbb{Z}^m$ and $\mathbb{E}^m$.

Email addresses: axel.kohnert@uni-bayreuth.de (Axel Kohnert), sascha.kurz@uni-bayreuth.de (Sascha Kurz).

URLs: www.mathe2.uni-bayreuth.de (Axel Kohnert), www.wm.uni-bayreuth.de (Sascha Kurz).

1.1 Integral point sets in $\mathbb{Z}^{\mathbf{m}}$ and $\mathbb{E}^{\mathbf{m}}$

So let us now consider integral point sets in $\mathbb{E}^m$. If we denote the largest distance of an integral point set, consisting of n points, as its diameter, the natural question for the minimum possible diameter $d(n,m)$ arises, see Figure 1 for an example. Obviously we have $d(n,1) = n-1$. To avoid the corresponding trivial 1-dimensional configuration in higher dimensions, it is common to request that an m-dimensional integral point set is not contained in a hyperplane of $\mathbb{E}^m$. We call a set of $m+1$ points in $\mathbb{Z}^{\mathbf{m}}$ or $\mathbb{E}^{\mathbf{m}}$ degenerated, if the points are indeed contained in a hyperplane. There are quite a lot of constructions which show that $d(n,m)$ exists for $n+1 \geq m$, see i.e. [18]. Some exact values are determined in [21,24,27,28,33]. The best known upper bound $d(n,m) \in O\left(e^{c\,\log(n-m)\log\log(n-!m)}\right)$ is given in [18]. For $m=2$ Solymosi [36] gives the best known lower bound $d(n,2) \geq cn$. For $m=2$ and $n \geq 9$ the shape of the examples with minimum diameter is conjectured to consist of $n-1$ collinear points and one point apart [28], see Figure 1 for an example with $n=9$. We would like to remark that this conjecture is confirmed for $n \leq 122$ by an exhaustive search [28]. If for a fix $\rho > 0$, we have a sequence of plane integral point set $\mathcal{P}_i$, each containing a collinear subset of cardinality least n^ρ, then the diameters of the $\mathcal{P}_i$ are in $\Omega\left(e^{c\,\log n \log\log n}\right)$ [24,28]. For $m \geq 3$ we refer to [24,27], where some bounds and exact numbers are given.

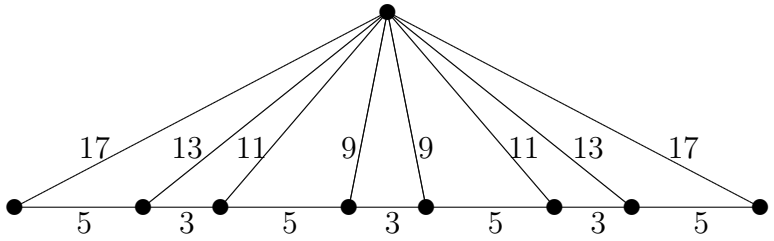

Figure 1. A 2-dimensional integral point set with $n=9$ and diameter 29.

Some authors require integral point sets to fulfill certain further conditions. The two classical conditions are, that no $m+1$ points are contained in an $(m-1)$-dimensional hyperplane, and that no $m+2$ points are located on an $(m-1)$-dimensional hypersphere. For ease of notation we speak of semi-general position in the first case and of general position if both conditions are fulfilled. We denote the minimum diameter of integral point sets in semi-general position by $\overline{d}(n,m)$ and of integral point sets in general position by $\dot{d}(n,m)$. For some small parameters the exact values have been determined in [21,23,24,28,33]. We would like to remark that for dimension $m=2$ and $3 \leq n \leq 36$ points, the examples with minimum possible diameter $\overline{d}(n,2)$, consist of points on a circle [24,28].

A famous question of Erdős asks for point sets in the plane with seven points in general position (i.e. no three on a line and nou four on a circle) with pairwise integral distances. Actually he first asked for such a set with five points, which was answered by Harborth [15,16], then for a set with six points, which was answered

by Kemnitz [21]. Kemnitz even gives a construction for infinitely many such sets with coprime distances. For a long time no example consisting of seven points was known. Very recently one of the authors has discovered two such examples with diameters 22270 and 66810 [23]. For dimensions $m \geq 3$ we refer to [24,17].

As a specialization, integral point sets in general position, with all n points on an integer grid $\mathbb{Z}^m$, are called n_m-clusters. Noll and Bell have found n_m-clusters for $m \leq 5$ and $n \leq m+4$ but have no example for $n \geq m+5$ [31]. For $m \geq 3$ even no integral point set in semi-general position with at least $m+5$ points is known.

Conjecture 1 *(Erdős and Noll) For any $m > 1$, $n > 1$, there exists either none or an infinite number of non-isomorphic n_m-clusters.*

An important invariant of an integral point set is its characteristic, which is defined as follows:

Definition 1 *Let $\mathcal{S}$ be a non-degenerated integral point set of $m+1$ points in the m-dimensional Euclidean space $\mathbb{E}^m$. By V_m we denote the m-dimensional volume of the simplex being formed by the convex hull of $\mathcal{S}$. Since the pairwise differences of $\mathcal{S}$ are integral and $\mathcal{S}$ is not degenerated we have $(V_m)^2 \in \mathbb{N}\backslash\{0\}$. Thus V_m can be uniquely written as $V_m = q\sqrt{c}$ with $q \in \mathbb{Q}$ and a squarefree integer c. This integer c is called the* ***characteristic*** *char$(\mathcal{S})$ of an integral simplex $\mathcal{S}$.*

The following theorem allows us to define the characteristic of an integral point set.

Theorem 1 *In an m-dimensional integral point set $\mathcal{P}$ each non-degenerate integral simplex $\mathcal{S}$ has the same characteristic char$(\mathcal{S})$.*

Definition 2 *Let $\mathcal{P}$ be an m-dimensional integral point set and $\mathcal{S} \subseteq \mathcal{P}$ be an arbitrary m-dimensional non-degenerate integral sub-simplex of $\mathcal{P}$. The* ***characteristic*** *char$(\mathcal{P})$ of $\mathcal{P}$ is given by char$(\mathcal{P})$ = char$(\mathcal{S})$.*

For dimension $m = 2$ Theorem 1 can be traced back at least to Kummer [21], for $m \geq 3$ we refer to [25]. We would like to remark that if we are in the special case, where also the coordinates of an m-dimensional integral point set $\mathcal{P}$ are integral, every subset $\mathcal{S}$ of $\mathcal{P}$, consisting of $m+1$ points, has an integral volume. In our notation this means, that for an integral point set $\mathcal{P}$ in $\mathbb{Z}^m$ we have char$(\mathcal{P}) = 1$. So all n_m-clusters have characteristic one.

From [13,25] we know, that if $\mathcal{P}$ is an m-dimensional integral point set in $\mathbb{E}^m$ with characteristic char$(\mathcal{P}) = 1$, then there exists an embedding of $\mathcal{P}$ in $\mathbb{E}^m$ using only rational coordinates. The existence of an embedding using only integral coordinates is an interesting open conjecture of [13].

2 Integral point sets over $\mathbb{Z}_\mathbf{n}^\mathbf{m}$

In the previous section we have seen, that almost certainly there is a lot of hidden structure in the set of integral point sets which attain the minimum possible diameter and fulfill certain further conditions. Although the problem of integral point sets is a very classical one, not much progress has been achieved towards structure results or tight bounds on the minimum diameter. The idea of this paper is to study similar problems, which might be easier to handle, but may give some insight in the original problem. At first we want to consider the study of integral point sets in $\mathbb{Z}^m$ as our *original problem* and relate it to some problem of point sets in $\mathbb{Z}_n^m$.

So let $\mathcal{P}'$ be an integral point set over $\mathbb{Z}^m$. To relate $\mathcal{P}'$ to a set $\mathcal{P}$ of points in $\mathbb{Z}_n^m$ we consider the canonical mapping $\phi_n : \mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto x + \mathbb{Z}n = \overline{x}$, which maps coordinates in $\mathbb{Z}^m$ to coordinates in $\mathbb{Z}_n^m$. If n is suitably large no two points of $\mathcal{P}'$ will be mapped onto the same point in $\mathcal{P}$. To be able to translate results in $\mathbb{Z}_n^m$ back to $\mathbb{Z}^m$, we define the inverse mapping $\Psi_n : \mathbb{Z}_n \to \{0, \ldots, n-1\}$ by $\Psi(\phi_n(x)) = x$ for $x \in \{0, \ldots, n-1\}$. As an abbreviation we set $\Psi_n(x) = \widehat{x}$ and $\phi_n(x) = \overline{x}$, whenever the value of n is clear from the context. Since points in $\mathcal{P}'$ have integral distances in $\mathbb{Z}^m$ we need a similar definition of integral distances in $\mathbb{Z}_n^m$. The most natural way to define an integral distance over $\mathbb{Z}_n^m$ is:

Definition 3 *Two points $(u_1, \ldots, u_m), (v_1, \ldots, v_m) \in \mathbb{Z}_n^m$ are at **integral distance**, if there exists a number $d \in \mathbb{Z}_n$ with*

$$\sum_{i=1}^{m} (u_i - v_i)^2 = d^2.$$

With this definition an integral point set $\mathcal{P}'$ over $\mathbb{Z}^m$ is mapped via ϕ_n onto an integral point set $\mathcal{P}$ over $\mathbb{Z}_n^m$. Since ϕ_n may map some point set $\mathcal{P}'$ over $\mathbb{Z}^m$, which is not contained in a hyperplane of $\mathbb{Z}^m$, onto a point set $\mathcal{P}'$, where all points are contained in a hyperplane of $\mathbb{Z}_n^m$, we do not make any requirements on the distribution of the points in an integral point set over $\mathbb{Z}_n^m$ in the first run. The next definition to translate from $\mathbb{Z}^m$ or $\mathbb{E}^m$ to $\mathbb{Z}_n^m$ is the minimum diameter. In $\mathbb{Z}^m$ and $\mathbb{E}^m$ we need the concept of a minimum diameter to get a finite space, whereas $\mathbb{Z}_n^m$ is finite for itself. So we find it natural to consider the maximum number of integral points.

Definition 4 *By $\mathcal{I}(n, m)$ we denote the maximum number of points in $\mathbb{Z}_n^m$ with pairwise integral distances.*

Theorem 2 *$\mathcal{I}(n, 1) = n$, $\mathcal{I}(1, m) = 1$, and $\mathcal{I}(2, m) = 2^m$.*

PROOF. Because there are only n^m different elements in $\mathbb{Z}_n^m$ we have the trivial upper bound $\mathcal{I}(n, m) \leq n^m$. This upper bound is only attained if $m = 1$ or $n \leq 2$, since $\mathbb{Z}_n$ has at least one quadratic non residue for $n \geq 3$. □

$m\backslash n$	3	4	5	7	8	9	11	13	16	17
2	3	8	5	7	16	27	11	13	64	17
3	4	16	25	8	64	81	11	169	256	289
4	9	32	25	49	512	324	121	≥ 169	1024	
5	27	128	125	343	2048	≥ 893	≥ 1331	≥ 2197		
6	33	256	≥ 125		≥ 15296					
7	≥ 35	1024			≥ 81792					

Table 1
Values of $\mathcal{I}(n,m)$ for small parameters n and m.

For $n \geq 3$ we so far were not able to derive explicit formulas for $\mathcal{I}(n,m)$ and so we give in Table 1 some values for small parameters n and m, obtained by exhaustive enumeration via clique search, which we will describe in the next subsection. Further exact values or lower bounds can be determined using Theorem 2 and 3 of Subsection 2.2.

2.1 Exhaustive enumeration of integral point sets over $\mathbb{Z}_{\mathbf{n}}^{\mathbf{m}}$ via clique search

In this subsection we describe how the exact values $\mathcal{I}(n,m)$ of Table 1 were obtained. We model our problem as a graph $\mathcal{G}$, so that the cliques (i.e. complete subgraphs) of $\mathcal{G}$ are in bijection to integral point sets over $\mathbb{Z}_n^m$. Therefore we choose the elements of $\mathbb{Z}_n^m$ as vertices and connect $x, y \in \mathbb{Z}_n^m$ via an edge, if and only if x and y are at integral distance.

To determine $\mathcal{I}(n,m)$, we only have to determine the maximum cardinality of a clique of $\mathcal{G}$. Unfortunately this is an $\mathcal{NP}$-hard problem in general, but practically this approach was also successful in the case of integral point sets over $\mathbb{E}^m$ [24,28], due to good heuristic maximum-clique algorithms. Besides an implementation of the Bron-Kerbosch algorithm [7] written by ourself we use the software package CLIQUER [30,32] of Niskanen and Östergård.

By prescribing points or distances of an integral point set $\mathcal{P}$, it is possible to reduce the complexity for the clique-search algorithm. The first variant is, that due to symmetry we can assume that the point $0 = (\overline{0}, \ldots, \overline{0}) \in \mathbb{Z}_n^m$ is part of $\mathcal{P}$. As vertices of $\mathcal{G}$ we choose the points in $\mathbb{Z}_n^m \backslash \{0\}$, which have an integral distance to 0. Again two vertices $x, y \in \mathcal{G}$ are joined by an edge, if the corresponding points are at integral distance.

For the second variant we consider the set $D_{n,m}$ of all points $d = (d_1, \ldots, d_m) \in \mathbb{Z}_n^m$, which have an integral distance to 0 and which fulfill $\widehat{d_i} \leq \left\lfloor \frac{n}{2} \right\rfloor$, for all $1 \leq i \leq m$. So for every two points $u = (u_1, \ldots, u_m) \neq v = (v_1, \ldots, v_d) \in \mathbb{Z}_n^m$, having an integral distance, the tuple

$$\delta_n(u,v) = \left(\overline{\min\left(|\widehat{u}_1 - \widehat{v}_1|, n - |\widehat{u}_1 - \widehat{v}_1|\right)}, \ldots, \overline{\min(|\widehat{u}_m - \widehat{v}_m|, n - |\widehat{u}_m - \widehat{v}_m|)} \right)$$

is an element of $D_{n,m}$. Actually we consider the vector of the Lee weights [34] of the coordinates of the difference $u - v$. Now we choose an arbitrary numbering of this set $D_{n,m}\backslash\{0\} = \{e_0, \ldots, e_{|D_{n,m}|-2}\}$ and consider the graphs $\mathcal{G}_i$, which consist of the points of $\mathbb{Z}_n^m\backslash\{0, e_i\}$, with integral distances to 0 and e_i, as vertices. Two vertices $x \neq y \in \mathcal{G}$ are joined by an edge if and only if the corresponding points fullfill $\delta_n(x, y) = e_j$ with $i \leq j$. Again one can show, that an integral point set in $\mathbb{Z}_n^m$ corresponds to a clique in some graph $\mathcal{G}_i$ and vice versa. For some values of n and m it is worth to put some effort in a suitable choice of the numbering of $D_{n,m}\backslash\{0\}$.

2.2 Hamming spaces and homomorphisms

In this subsection we want to relate the problem of integral point sets over $\mathbb{Z}_n^m$ to problems in Hamming spaces. In coding theory the Hamming distance $h(u, v)$ of two vectors $u = (u_1, \ldots, u_m)$, $v = (v_1, \ldots, v_m) \in \mathbb{Z}_n^m$ is the number of positions i where u_i and v_i differ. Normally one is interested in large subsets of $\mathbb{Z}_n^m$ where all the Hamming distances are either 0 or larger than a given constant c. In our subject, we are interested in large subsets of $\mathbb{Z}_n^m$, where all the Hamming distances are taken from a specific proper subset of $\{0, 1, \ldots, m\}$. This point of view has been proven useful i.e. also in the $0/1$-Borsuk problem in low dimensions, see [37]. Here we also want to mention the study of two-weight codes, see i.e. [9,22].

So let us go back to the determinantion of $\mathcal{I}(n, m)$. As there are trivial formulas for $\mathcal{I}(1, m)$ and $\mathcal{I}(2, m)$, the next open case for fixed ring order n is the determination of $\mathcal{I}(3, m)$. Due to $1^2 \equiv 2^2 \equiv 1 \mod 3$, integral point sets over $\mathbb{Z}_3^m$ correspond to sets of $\mathbb{Z}_3^m$ with Hamming distances $h(u, v) \not\equiv 2 \mod 3$. So this is our first example of a selection problem in a Hamming space.

For the determination of $\mathcal{I}(2n, m)$ we can utilize homomorphisms to make the problem easier. Therefore we need some definitions.

Definition 5 *For an integer n we define the mapping $\tilde{\varphi}_{2n} : \mathbb{Z}_{2n} \to \mathbb{Z}_n$, $x \mapsto \widehat{x}+\mathbb{Z}n$, and by $\varphi_{2n,m}$ we denote its extensions to $\mathbb{Z}_{2n}^m$.*

Definition 6 *The weight function $\tilde{w}_{2n} : \mathbb{Z}_n^2 \to \mathbb{Z}_{2n}$ is defined by $(u_i, v_i) \mapsto (\widehat{u}_i - \widehat{v}_i)^2 + \mathbb{Z} \cdot 2n$.*

$$\mathbb{H}_{2n}^m := \left\{ S \subseteq \mathbb{Z}_n^m \mid \forall\, s_1, s_2 \in S : \exists d \in \mathbb{Z}_{2n} : d^2 = w(s_1, s_2) \right\},$$

where $w_{2n,m} : \left(\mathbb{Z}_n^m\right)^2 \to \mathbb{Z}_{2n}$ is given by $((u_1, \ldots, u_m), (v_1, \ldots, v_m)) \mapsto \sum_{i=1}^{m} \tilde{w}_{2n}(u_i, v_i)$. By $\mathbb{I}_n^m$ we denote the set of integral point sets in $\mathbb{Z}_n^m$.

Lemma 1

$$2^m \,|\, \mathcal{I}(2n, m).$$

PROOF. We consider the ring homomorphism $\varphi_{2n,m}$ and restrict it to $\varphi'_{2n,m} : \mathbb{I}_{2n}^m \to \mathbb{H}_{2n}^m$. If $\mathcal{P}$ is an element of $\mathbb{H}_{2n}^m$ then the preimage $\varphi_{2n,m}^{-1}(\mathcal{P})$ is an integral point set, due to $(x+n)^2 \equiv x^2 + n \mod 2n$ for odd n and $(x+n)^2 \equiv x^2 \mod 2n$ for even n. For all $x \in \mathbb{Z}_n^m$ we have $|\varphi_{2n,m}^{-1}(x)| = 2^m$. □

So for the determination of $\mathcal{I}(2n, m)$, it suffices to determine the maximum cardinality of the elements of $\mathbb{H}_{2n}^m$, which actually are subsets of $\mathbb{Z}_n^m$.

$$\mathcal{I}(2n, m) = 2^m \cdot \max_{S \in \mathbb{H}_{2n}^m} |S|$$

As an example we want to apply this result for $n = 2$. Here $w_{4,m}$ is exactly the Hamming distance in $\mathbb{Z}_2^m$. Since the squares of $\mathbb{Z}_4$ are given by $\{0, 1\}$, we conclude that $\mathbb{H}_4^m$ is the set of all subsets of $\mathbb{Z}_2^m$, with Hamming distance congruent to 0 or 1 modulo 4. With the mapping $\varphi'_{4,m}$ at hand, we can exhaustively generate the maximal sets in $\mathbb{H}_4^m$, via a clique search, to extend Table 1:

$$(\mathcal{I}(4, m))_{m \leq 12} = 4, 8, 16, 32, 128, 256, 1024, 4096, 16384, 32768, 65536, 131072.$$

The next theorem shows, that it suffices to determine $\mathcal{I}(a, m)$ for prime powers $a = p^r$.

Theorem 3 *For two coprime integers a and b we have $\mathcal{I}(a \cdot b, m) = \mathcal{I}(a, m) \cdot \mathcal{I}(b, m)$.*

PROOF. Since a and b are coprime we have $\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b$. If $\mathcal{P}$ is an integral point set in $\mathbb{Z}_a \times \mathbb{Z}_b$, then the projections into $\mathbb{Z}_a$ and $\mathbb{Z}_b$ are also integral point sets. If on the other hand, $\mathcal{P}_1$ and $\mathcal{P}_2$ are integral point sets over $\mathbb{Z}_a$ and $\mathbb{Z}_b$, respectively, then $\mathcal{P} := \mathcal{P}_1 \times \mathcal{P}_2$ is an integral point set over $\mathbb{Z}_a \times \mathbb{Z}_b$, due to a straight forward calculation. □

If we drop the condition that a and b are coprime Theorem 3 does not remain valid in general. One can see this by looking at the example $\mathcal{I}(2, 3) \cdot \mathcal{I}(4, 3) > \mathcal{I}(8, 3)$ in table 1. Also $\mathcal{I}(a, m) \mid \mathcal{I}(a \cdot b, m)$ does not hold in general, as on can see by a look at the example $\mathcal{I}(3, 3) \nmid \mathcal{I}(9, 3)$. We would like to mention, that in a recent preprint [26] the exact values of $\mathcal{I}(p, 2)$ and $\mathcal{I}(p^2, 2)$ have been determined.

Theorem 4 *For a prime $p \geq 3$ we have*

$$\mathcal{I}(p, 2) = p \quad \textit{and} \quad \mathcal{I}(p^2, 2) = p^3.$$

2.3 Integral point sets over the plane $\mathbb{Z}_{\mathbf{n}}^{\mathbf{2}}$

In Theorem 2 we have given an exact formula for $\mathcal{I}(n, 1)$. So, if we fix the dimension m, the next case is the determination of $\mathcal{I}(n, 2)$. At first we give two

constructions to obtain lower bounds for $\mathcal{I}(n,2)$.

Lemma 2 *If the prime factorization of n is given by $n = \prod_{i=1}^{s} p_i^{r_i}$, with pairwise different primes p_i, we have*

$$\mathcal{I}(n,2) \geq n \cdot \prod_{i=1}^{s} p_i^{\lfloor \frac{r_i}{2} \rfloor}.$$

PROOF. We choose the points $(u_i, v_j\overline{k})$, where $u_i, v_j \in \mathbb{Z}_n$ and $k = \prod_{i=1}^{s} p_i^{\lceil \frac{r_i}{2} \rceil}$. Since

$$(u_{i_1} - u_{i_2})^2 + (v_{j_1}\overline{k} - v_{j_2}\overline{k})^2 = (u_{i_1} - u_{i_2})^2,$$

all occurring distances are integral. □

An example of the construction of Lemma 2 is given in Figure 2, for $n = 12 = 2^2 \cdot 3$.

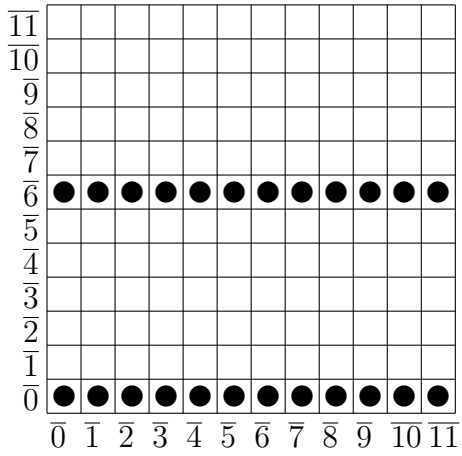

Figure 2. An integral pointset over $\mathbb{Z}_{12}^2$ constructed via Lemma 2.

In the case of $n = 2 \mod 4$ we can improve the above lemma:

Lemma 3 *If the prime factorization of n is given by $n = 2 \cdot \prod_{i=2}^{s} p_i^{r_i}$, with pairwise different primes $p_i \neq 2$ we have*

$$\mathcal{I}(n,2) \geq 2n \cdot \prod_{i=2}^{s} p_i^{\lfloor \frac{r_i}{2} \rfloor}.$$

PROOF. We choose the points $(u_i, v_j\overline{k})$, where $u_i, v_j \in \mathbb{Z}_n$ and $k = \prod_{i=2}^{s} p_i^{\lceil \frac{r_i}{2} \rceil}$. Since $2k^2 \equiv 0 \mod n$ and

$$(u_{i_1} - u_{i_2})^2 + (v_{j_1}\overline{k} - v_{j_2}\overline{k})^2 = (u_{i_1} - u_{i_2})^2 + (v_{j_1}^2 + v_{j_2}^2)\overline{k^2}$$

either

$$(u_{i_1} - u_{i_2})^2 + (v_{j_1}\overline{k} - v_{j_2}\overline{k})^2 = (u_{i_1} - u_{i_2})^2$$

or

$$(u_{i_1} - u_{i_2})^2 + (v_{j_1}\overline{k} - v_{j_2}\overline{k})^2 = (u_{i_1} - u_{i_2} + \overline{k^2})^2$$

holds. □

Conjecture 2 *For all $n \in \mathbb{N}$ either the lower of Lemma 2 or the lower bound of Lemma 3 is tight.*

Remark 1 *By Theorem 3 and an exhaustive enumeration of integral point sets over $\mathbb{Z}_n^2$, via clique search, we have verified Conjecture 2 up to $n = 307$.*

If n is squarefree and 2 does not divide n, then our constructions from Lemma 2 and Lemma 3 yield point sets of the form $\mathcal{P} = \{(u, 0) \mid u \in \mathbb{Z}_n\}$. This is somewhat similar to the situation in $\mathbb{E}^2$, where integral collinear point sets with small diameter can consist of many points. Since we also want to speak of collinear point sets in $\mathbb{Z}_n^2$ we give:

Definition 7 *A set of r points $(u_i, v_i) \in \mathbb{Z}_n^2$ is collinear, if there are $a, b, t_1, t_2, w_i \in \mathbb{Z}_n$ with*

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

Let us first look at collinearity from the algorithmic point of view. Checking three points for being collinear, by running through the possible values of $a, b, t_1, t_2, w_i \in \mathbb{Z}_n$, would cost $\mathcal{O}(n^7)$ time. Setting, w.l.o.g., $a = u_1$, $b = v_1$, $w_1 = \overline{0}$ reduces this to $\mathcal{O}(n^4)$. If n is prime, then we are working in a field, and there is an easy and well known way to check, whether three points are collinear, in $\mathcal{O}(1)$ time:

Lemma 4 *For a prime n the points $(u_1, v_1), (u_2, v_2), (u_3, v_3) \in \mathbb{Z}_n^2$ are collinear, if and only if*

$$\begin{vmatrix} u_1 & v_1 & \overline{1} \\ u_2 & v_2 & \overline{1} \\ u_3 & v_3 & \overline{1} \end{vmatrix} = \overline{0}. \tag{1}$$

We remark that in $\mathbb{Z}_8$ the points $(\overline{0}, \overline{0})$, $(\overline{2}, \overline{4})$, $(\overline{4}, \overline{4})$ fulfill equation (1), but are not collinear with respect to Definition 7. So in general equation (1) is necessary but not sufficient for three points to be collinear. We propose the development of a fast algorithm, which checks three points in $\mathbb{Z}_n^2$ for being collinear, as an interesting open problem. In practice one simply determines for each pair $x, y \in \mathbb{Z}_n^2$, whether the triple $0, x, y$ is collinear or not, in a precalculation.

The study of collinear point sets is motivated by the situation in the case of non-modular point sets. Due to a theorem of Erdős each integral point set in $\mathbb{E}^2$, with infinitely many points, is located on a line [1,12]. And, as already mentioned in the

introduction the, non-collinear integral point sets in $\mathbb{E}^2$ with minimum diameter, are conjectured to consist of $n-1$ collinear points and one point apart.

In this context we would like to mention a theorem, which was recently proven in [26].

Theorem 5 *For p being a prime, with $p \equiv 3 \mod 4$, each integral point set over $\mathbb{Z}_p^2$, consisting of p points, is collinear.*

For primes p, of the form $p \equiv 1 \mod 4$, also a different type of integral point sets occurs. To describe these sets, we need some new notation. For a prime $p \equiv 1 \mod 4$, there is a unique element $\omega(p) \in \mathbb{N}$, with $\omega(p) < \frac{p}{2}$ and $\omega^2(p) \equiv -1 \mod p$. By $\square_n = \{i^2 \mid i \in \mathbb{Z}_n\}$ we denote the set of squares in $\mathbb{Z}_n$.

Lemma 5 *For a prime $p \geq 3$, the set $\mathcal{P} = (1, \pm\omega(p)) \cdot \square_p$ is a non-collinear integral point set over $\mathbb{Z}_p^2$ with cardinality p.*

PROOF. For an odd prime p we have exactly $\frac{p+1}{2}$ squares in $\mathbb{Z}_p$. Since $(0,0)$, $(1,\omega(p))$, and $(1,-\omega(p))$ are elements of $\mathcal{P}$, the point set is clearly non-collinear. For the property of pairwise integral distances we consider two arbitrary elements $q, q' \in \square_p$ and the corresponding distances

$$
\begin{aligned}
&(q-q')^2 + \omega^2(p)(q-q')^2 = \overline{0},\\
&(q-q')^2 + \omega^2(p)(q+q')^2 = (2\omega(p))^2 qq',\\
&(q+q')^2 + \omega^2(p)(q-q')^2 = 2^2 qq',\\
&(q+q')^2 + \omega^2(p)(q+q')^2 = \overline{0}.
\end{aligned}
$$

□

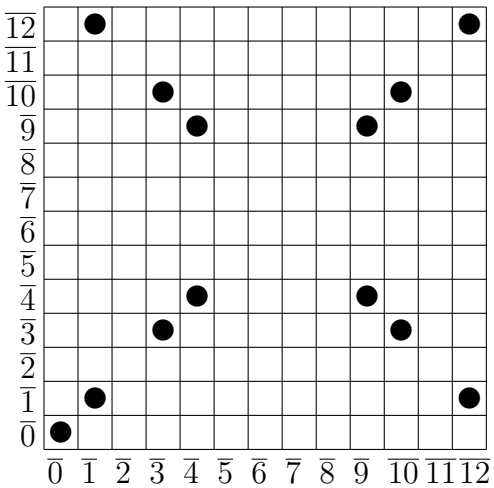

Figure 3. The integral point set $\mathcal{P} = (1, \omega(p)) \cdot \square_p$ for $p = 13$.

In Figure 3 we have depicted an integral point set, being constructed as described in Lemma 5 for $p = 13$. We remark that recently in [26] it was proven, that integral point sets $\mathcal{P}$ over $\mathbb{Z}_p^2$, with cardinality $p \geq 3$, are either collinear or a translated version of the integral point set constructed in Lemma 5.

2.4 Integral point sets over $\mathbb{Z}_{\mathbf{n}}^{\mathbf{2}}$ with further conditions

In the last subsection we have recognized, that integral point sets over $\mathbb{Z}_n^2$ are, similar to integral point sets over $\mathbb{E}^2$, somewhat attracted by collinear sets. So we investigate in this subsection integral point sets $\mathcal{P}$ over $\mathbb{Z}_n^2$, where no three points are collinear.

Definition 8 *By $\overline{\mathcal{I}}(n, m)$ we denote the maximum number of points in semi-general position over $\mathbb{Z}_n^m$, where are pairwise distances are integral.*

If we drop the condition of pairwise integral distances, our studied objects become very familiar discrete structures. In the case of affine finite geometries (classical [19] in the case of $\mathbb{Z}_n$ with n a prime, Hjelmslev geometries [8] in the other cases) point sets in semi-general position, with arbitrary pairwise distances, are called arcs in the case of planes or caps [3] in the three dimensional case. With the results from Subsection 2.2 in mind, we would like to mention the connection of these objects to linear coding theory, see i.e. [4] for the details.

In Table 2 we give some values of $\overline{\mathcal{I}}(n, 2)$ for small n, obtained by Algorithm 1 described later on.

n	$\overline{\mathcal{I}}(n,2)$	n	$\overline{\mathcal{I}}(n,2)$	n	$\overline{\mathcal{I}}(n,2)$	n	$\overline{\mathcal{I}}(n,2)$	n	$\overline{\mathcal{I}}(n,2)$	n	$\overline{\mathcal{I}}(n,2)$
1	1	11	6	21	4	31	16	41	20	51	8
2	4	12	4	22	8	32	14	42	6	52	12
3	2	13	6	23	12	33	6	43	22	53	26
4	4	14	6	24	6	34	10	44	10	54	≥ 13
5	4	15	4	25	10	35	6	45	11	55	8
6	4	16	8	26	10	36	12	46	14	56	10
7	4	17	8	27	10	37	18	47	24	57	10
8	6	18	10	28	8	38	12	48	8	58	≥ 16
9	6	19	10	29	14	39	6	49	≥ 18	59	30
10	6	20	8	30	6	40	10	50	≥ 17	60	8

Table 2
Values of $\overline{\mathcal{I}}(n, 2)$ for small parameters n.

Now we want to derive an upper bound for $\overline{\mathcal{I}}(n,2)$, by relaxing the condition of pairwise integral distances. Let $\mathcal{P}$ be a point set over $\mathbb{Z}_n^2$ in semi-general position. We consider the lines $\{(i,j) \mid j \in \mathbb{Z}_n\}$ for $i \in \mathbb{Z}_n$. Since these n lines form a partition of $\mathbb{Z}_n^2$ and each line can contain at most two points of $\mathcal{P}$, we obtain the trivial upper bound $\overline{\mathcal{I}}(n,2) \leq 2n$. This is connected to a famous open problem in number theory [14, sec. F4], where people work on an upper bound for the *no-three-in-a-line* problem. Considering all lines in $\mathbb{Z}_n^2$ we receive

$$\overline{\mathcal{I}}(p,2) \leq p+1$$

for odd primes p [5] and

$$\overline{\mathcal{I}}(n,2) \leq n \cdot (1 + p^{-\lceil \frac{a+1}{2} \rceil} + p^{-a})$$

where $p^a \mid n$ and $p^{a+1} \nmid n$ for a prime p [20].

Very recently for the case of odd primes p, tight bounds on $\overline{\mathcal{I}}(p,2)$ are proven [26]:

Theorem 6 *For $p \equiv 3 \mod 4$ we have*

$$\overline{\mathcal{I}}(2,p) = \frac{p+1}{2}$$

and for $p \equiv 1 \mod 4$ we have

$$\frac{p-1}{2} \leq \overline{\mathcal{I}}(2,p) \leq \frac{p+3}{2}.$$

We would like to remark that the known construction uses half of the points of the circle $\{(a,b) \in \mathbb{Z}_p^2 \mid a^2+b^2 = \overline{1}\}$, see [26] for the details. For $p \equiv 1 \mod 4$, $p \neq 5$ we conjecture $\overline{\mathcal{I}}(p,2) = \frac{p-1}{2}$.

By a look at the situation in $\mathbb{E}^2$ and with the famous question of Erdős in mind. it seems interesting to investigate integral point sets over $\mathbb{Z}_n^2$, where no three points are collinear and no four points are situated on a circle.

Definition 9 *Four points $p_i = (x_i, y_i)$ in $\mathbb{Z}_n^2$ are said to be situated on a circle if there exist $a, b \in \mathbb{Z}_n$, $r \in \mathbb{Z}_n \backslash \{\overline{0}\}$ with*

$$(x_i - a)^2 + (y_i - b)^2 = r^2$$

for all i.

We have the following necessary condition:

Lemma 6 *Four points $p_i = (x_i, y_i)$ in $\mathbb{Z}_n^2$ being situated on a circle fulfill*

$$\begin{vmatrix} x_1^2 + y_1^2 & x_1 & y_1 & \overline{1} \\ x_2^2 + y_2^2 & x_2 & y_2 & \overline{1} \\ x_3^2 + y_3^2 & x_3 & y_3 & \overline{1} \\ x_4^2 + y_4^2 & x_4 & y_4 & \overline{1} \end{vmatrix} = \overline{0}. \tag{2}$$

Definition 10 *By $\dot{\mathcal{I}}(n, m)$ we denote the maximum number of points in $\mathbb{Z}_n^m$ with pairwise integral distances, where no three points are collinear and no four points are situated on a circle. Here we also talk of general position.*

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	$\dot{\mathcal{I}}(n,2)$	n	$\dot{\mathcal{I}}(n,2)$	n	$\dot{\mathcal{I}}(n,2)$
1	1	11	4	21	4	31	6	41	9	51	7	61	≥ 9
2	4	12	4	22	8	32	8	42	6	52	≥ 9	62	≥ 11
3	2	13	5	23	5	33	4	43	8	53	≥ 9	63	8
4	4	14	6	24	4	34	10	44	8	54	≥ 11	64	≥ 10
5	4	15	4	25	6	35	5	45	8	55	6	65	7
6	4	16	6	26	8	36	≥ 10	46	10	56	6	66	8
7	3	17	5	27	7	37	7	47	7	57	6	67	≥ 9
8	4	18	8	28	6	38	8	48	8	58	≥ 11	68	≥ 10
9	4	19	5	29	7	39	6	49	≥ 11	59	≥ 9	69	7
10	6	20	6	30	6	40	6	50	≥ 12	60	8	70	≥ 9

Table 3
Values of $\dot{\mathcal{I}}(n, 2)$ for small parameters n.

Trivially we have $\dot{\mathcal{I}}(n, 2) \leq \overline{\mathcal{I}}(n, 2)$. In Table 3 we give some exact values of $\dot{\mathcal{I}}(n, 2)$, obtained by Algorithm 1 described later on. One might conjecture that $\dot{\mathcal{I}}(n, 2)$ is unbounded.

Because semi-general position or general position is a property of three or four points, respectively, we cannot apply our approach via clique search for the determination of $\overline{\mathcal{I}}(n, 2)$ and $\dot{\mathcal{I}}(n, 2)$ directly. Instead of going over to hypergraphs we use a variant of orderly generation [35], which glues two integral point sets consisting of r points, having $r - 1$ points in common, to obtain recursively integral point sets of $r + 1$ points. The used variant of orderly generation was introduced, and applied for the determination of the minimum distance $\dot{d}(n, 2)$ of integral point sets in general position in $\mathbb{E}^2$, in [24,28].

Now we go into detail. To describe integral point sets over $\mathbb{Z}_n^2$, we utilize the set $D_{n,2}$, where the coordinates of the points are *reduced* with respect to the Lee weight

via

$$\delta_n((x_1,y_1),(x_2,y_2)) = \Big(\min(|\hat{x}_1-\hat{x}_2|, n-|\hat{x}_1-\hat{x}_2|), \min(|\hat{y}_1-\hat{y}_2|, n-|\hat{y}_1-\hat{y}_2|) \Big).$$

By $\mathcal{B} = \{b_0, b_1, \ldots, b_t\}$ we denote the subset of $D_{n,2} = \{\delta_n(0,x) \mid x \in \mathbb{Z}_n^2\}$, where the points x are at integral distance to 0. We define $b_0 = (\overline{0}, \overline{0})$. The numbering of the remaining b_i is arbitrary but fix. Each integral point set $\mathcal{P} = \{p_1, \ldots, p_r\}$ over $\mathbb{Z}_n^2$ is, up to translations and reflections, completely described by a matrix

$$\Delta_n(\mathcal{P}) = \Big(\iota\left(\delta_n\left(p_i, p_j\right)\right) \Big)_{i,j},$$

where we set $\delta_n(p_i, p_i) = b_0$ and $\iota : \mathcal{B} \to \mathbb{N}$, $b_i \mapsto i$. We use these matrices as a data structure for integral point sets over $\mathbb{Z}_n^2$. Next we extend the natural order $\leq$ on $\mathbb{N}$ to $\preceq$ for symmetric matrices, with zeros on the main diagonal as Δ_n, by using a column-lexicographical order of the upper right matrix. A matrix Δ_n is said to be *canonical* if $\Delta_n \geq \pi(\Delta_n)$ for every permutation $\pi \in S_r$ acting on the rows and columns of Δ_n. If $\downarrow\Delta_n$ denotes the removal of the last column and last row of a matrix Δ_n, then Δ_n is said to be *semi-canonical* if $\downarrow\Delta_n \geq \downarrow\pi(\Delta_n)$ for every permutation $\pi \in S_r$. The function Γ_r does the glueing of two integral point sets over $\mathbb{Z}_n^2$ consisting of r points having $r-1$ points in common. The result of the function Γ_r is an, with respect to $\preceq$, ordered list of integral point sets consisting of $r+1$ points. By $\mathcal{L}_r$ we denote the ordered list of all semi-canonical matrices Δ_n, with respect to $\preceq$, which correspond to integral point sets over $\mathbb{Z}_n^2$. It can be figured out easily that Γ_r produces a list with at most two integral point sets. With these definitions we can state:

Algorithm 1
Input: $\mathcal{L}_r$
Output: $\mathcal{L}_{r+1}$
begin
  $\mathcal{L}_{r+1} = \emptyset$
  loop over $x_1 \in \mathcal{L}_r$, x_1 *is canonical* **do**
    loop over $x_2 \in \mathcal{L}_r$, $x_2 \preceq x_1$, $\downarrow x_1 = \downarrow x_2$ **do**
      loop over $y \in \Gamma_r(x_1, x_2)$
        if y *is semi-canonical* **then** *add* y *to* $\mathcal{L}_{r+1}$ **end**
      end
    end
  end
end

A starting list $\mathcal{L}_3$ of the integral triangles can be generated by a nested loop. In order to apply Algorithm 1 for the determination of $\overline{\mathcal{I}}(n,2)$ or $\dot{\mathcal{I}}(n,2)$, we only have to modify it in that way, that it only accepts integral point sets in semi-general or general position, respectively, for the lists $\mathcal{L}_r$.

3 Integral point sets over $(\mathbb{R}/\mathbb{Z}\mathbf{n})^2$

In the previous section we have required also the coordinates of the point sets to be *integral*. This corresponds somewhat to integral point sets in $\mathbb{Z}^m$. In this section we try to develop a setting for an analogous treatment of integral point sets in $\mathbb{E}^m$ over the ring $\mathbb{Z}_n$ instead of $\mathbb{Z}$ for the distances. We start with $n = p$ being an odd prime.

Let p be an odd prime, then $\mathbb{Z}_p$ is a finite field. Given three elements $a, b, c \in \mathbb{Z}_p \backslash \{\overline{0}\}$, which we consider as edge lengths of a triangle. Then we can determine a coordinate represention, given by three points (x_1, y_1), (x_2, y_2), (x_3, y_3) in $(\mathbb{R}/\mathbb{Z}p)^2$, as follows. Due to translations, rotations and reflections we can assume $(x_1, y_1) = (\overline{0}, \overline{0})$ and $(x_2, y_2) = (a, \overline{0})$. For the third point (x_3, y_3) we get the system of equations

$$\begin{aligned} x_3^2 + y_3^2 &= b^2, \\ (x_3 - a)^2 + y_3^2 &= c^2. \end{aligned}$$

Solving this system yields

$$\begin{aligned} x_3 &= \frac{b^2 - c^2 + a^2}{2a}, \\ y_3^2 &= \frac{(a+b+c)(a+b-c)(a-b+c)(-a+b+c)}{(2a)^2}, \end{aligned}$$

which is defined in $\mathbb{Z}_p$ because of $2a \neq \overline{0}$. By $\alpha(p)$ we denote the smallest quadratic non-residue in $\mathbb{Z}_p$. With the above system of equations it can be seen that $x_3 \in \mathbb{Z}_p$ and y_3 is either also in $\mathbb{Z}_p$ or in $\mathbb{Z}_p \cdot \sqrt{\alpha(p)}$. Since this is similar to the case in $\mathbb{E}^m$, see [24,25], we define the characteristic of an integral triangle similarly.

Definition 11 *For an odd prime p the characteristic of three side lengths $a, b, c \in \mathbb{Z}_p$ with $V^2 = (a+b+c)(a+b-c)(a-b+c)(-a+b+c) \neq \overline{0}$ is defined as $\overline{1}$ if V^2 is a quadratic residue in $\mathbb{Z}_p$ and as $\alpha(p)$ otherwise.*

For the ease of notation we associate $\mathbb{E}_p^m$ with $(\mathbb{R}/\mathbb{Z}p)^m$. We remark that the three points are collinear exactly if V^2 equals $\overline{0}$. So, similarly to the case in $\mathbb{E}^2$ [29], we have the following lemma, where the determinant equals V^2, if we associate $a = \delta(v_1, v_2)$, $b = \delta(v_1, v_3)$, and $c = \delta(v_2, v_3)$.

Lemma 7 *Points $v_1, v_2, v_3 \in \mathbb{E}_p^2$ are collinear if and only if their Euclidean dis-*

tances $\delta(v_i, v_j)$ fulfill

$$\begin{vmatrix} \delta^2(v_1,v_1) & \delta^2(v_1,v_2) & \delta^2(v_1,v_3) & \overline{1} \\ \delta^2(v_2,v_1) & \delta^2(v_2,v_2) & \delta^2(v_2,v_3) & \overline{1} \\ \delta^2(v_3,v_1) & \delta^2(v_3,v_2) & \delta^2(v_3,v_3) & \overline{1} \\ \overline{1} & \overline{1} & \overline{1} & \overline{0} \end{vmatrix} = \overline{0}.$$

Our definition of the characteristic of an integral triangle in $\mathbb{Z}_p$ is properly chosen in the sense that we have the following theorem.

Theorem 7 *In an integral point set over $\mathbb{E}_p^2$ where p is an odd prime the characteristic of each non-degenerated triangle is equal.*

PROOF. Without loss of generality we assume that the two triangles have two points in common and the points are given by the coordinates $(\overline{0}, \overline{0})$, $(\overline{0}, a)$, $(x, y\sqrt{c})$, $(x', y'\sqrt{c'})$, where a, x, x', y, y' are elements of $\mathbb{Z}_p$ and c, c' are the characteristics. The squared distance of the last two points is given by

$$(x-x')^2 + (y\sqrt{c} - y'\sqrt{c'})^2 = (x-x')^2 + y^2c - 2yy'\sqrt{cc'} + {y'}^2c'.$$

Because this number must be an element of $\mathbb{Z}_p$ we have that cc' is a quadratic residue in $\mathbb{Z}_p$ yielding $c = c'$. □

As we have proceeded completely analogous to the case in $\mathbb{E}^m$ we can generalize Definition 11 and Theorem 7.

Definition 12 *For an odd prime p the characteristic of an integral point set with $m+1$ points in $\mathbb{E}_p^m$ given by its distances $\delta_{i,j}$ is 1 if V_m^2 is a quadratic residue in $\mathbb{Z}_p$ and $\alpha(p)$ otherwise, where*

$$V_m^2 = \begin{vmatrix} \delta_{1,1}^2 & \dots & \delta_{1,m+1}^2 & \overline{1} \\ \vdots & \ddots & \ddots & \vdots \\ \delta_{m+1,1}^2 & \dots & \delta_{m+1,m+1}^2 & \overline{1} \\ \overline{1} & \dots & \overline{1} & \overline{0} \end{vmatrix}.$$

Theorem 8 *In an integral pointset over $\mathbb{E}_p^m$ where p is an odd prime the characteristic of each non-degenerated simplex the same.*

PROOF. We do the corresponding calculations as in [25] over $\mathbb{Z}_p$ instead of $\mathbb{Q}$. □

For completeness we give a necessary coordinatefree criterion for $m+2$ points being situated on an m-dimensional sphere.

Lemma 8 *If $m+2$ points in $\mathbb{E}_n^m$ described by their distances $\delta_{i,j}$ are situated on an m-dimensional sphere then*

$$\begin{vmatrix} \delta_{1,1}^2 & \dots & \delta_{1,m+1}^2 \\ \vdots & \ddots & \vdots \\ \delta_{m+1,1}^2 & \dots & \delta_{m+1,m+1}^2 \end{vmatrix} = \overline{0}.$$

So far we have transferred the theory of integral point sets in $\mathbb{E}^m$ to integral point sets over $\mathbb{E}_p^m$ for odd primes p. For general n instead of p there are some twists if we use coordinates. The most natural approach to settle these would be, with respect to the situation in $\mathbb{E}^m$, to leave out coordinates and use Mengers characterization of embedable distance matrices [29] and replace the conditions over $\mathbb{Z}$ by conditions over $\mathbb{Z}_n$.

Definition 13 *An integral point set $\mathcal{P}$ over $\mathbb{E}_n^m$ is a set of $r \geq m+1$ points with distances $\delta_{i,j} \in \mathbb{Z}_n \backslash \{\overline{0}\}$ for $1 \leq i \neq j \leq r$ which fulfill*

$$V_{t-1}^2(\{i_1, \dots, i_t\}) = \begin{vmatrix} \delta_{i_1,i_1}^2 & \dots & \delta_{i_1,i_t}^2 & \overline{1} \\ \vdots & \ddots & \ddots & \vdots \\ \delta_{i_t,i_1}^2 & \dots & \delta_{i_t,i_t}^2 & \overline{1} \\ \overline{1} & \dots & \overline{1} & \overline{0} \end{vmatrix} = \overline{0}$$

for each subset of points $\{i_1, \dots, i_t\}$ of cardinality $t = m+2$ and $t = m+3$, and there exists a subset $\{\tilde{\imath}_1, \dots, \tilde{\imath}_t\}$ of cardinality $t = m+1$ with $V_{t-1}^2(\{\tilde{\imath}_1, \dots, \tilde{\imath}_t\}) \neq \overline{0}$.

To model the extra conditions we could define that $\mathcal{P}$ is in semi-general position if for every $m+1$ points $\{i_1, \dots, i_{m+1}\}$ we have $V_{m+1}^2(\{i_1, \dots, i_{m+1}\}) \neq \overline{0}$ and that $\mathcal{P}$ is in general position if the condition of Lemma 8 is fulfilled. We remark that for $m = 2$ the determinant of Lemma 8 can be factorized to

$$\begin{aligned} &-(\delta_{1,2}\delta_{3,4} + \delta_{1,3}\delta_{2,4} + \delta_{1,4}\delta_{2,3})(\delta_{1,2}\delta_{3,4} + \delta_{1,3}\delta_{2,4} - \delta_{1,4}\delta_{2,3}) \cdot \\ &(\delta_{1,2}\delta_{3,4} - \delta_{1,3}\delta_{2,4} + \delta_{1,4}\delta_{2,3})(-\delta_{1,2}\delta_{3,4} + \delta_{1,3}\delta_{2,4} + \delta_{1,4}\delta_{2,3}). \end{aligned}$$

For $m = 2$ we also have

$$\begin{aligned} V_2^2(\{1,2,3\}) = &(\delta_{1,2} + \delta_{1,3} + \delta_{2,3})(\delta_{1,2} + \delta_{1,3} - \delta_{2,3}) \cdot \\ &(\delta_{1,2} - \delta_{1,3} + \delta_{2,3})(-\delta_{1,2} + \delta_{1,3} + \delta_{2,3}). \end{aligned}$$

So one may leave out the first factor and request that one of the remaining factors equals $\overline{0}$ instead of the condition in Definition 13 and the condition in Lemma 8,

respectively. For $m \geq 3$ the two corresponding determinants are irreducible [10].

Another way to generalize integral point sets is to consider the edge lengths and coordinates as elements in a finite field $\mathbb{F}_{p^k}$ or a commutative ring $\mathcal{R}$ instead of $\mathbb{F}_p = \mathbb{Z}_p$. For some results we refer to [2,26]. Here we only give a very general definition of an integral point set over an commutative ring $\mathcal{R}$:

Definition 14 *For a commutative ring $\mathcal{R}$ a set $\mathcal{P}$ of n points in $\mathcal{R}^m$ is called an integral point set if for each $(x_1, \ldots, x_m), (y_1, \ldots, y_m) \in \mathcal{R}^m$ there exists an element $d \in \mathcal{R}$ fulfilling*

$$\sum_{i=1}^{m} (x_i - y_i)^2 = d^2.$$

4 Conclusion

We have generalized the theory of integral point sets over $\mathbb{Z}^m$ to integral point sets over $\mathbb{Z}_n^m$. Some exact values $\mathcal{I}(n, m)$ of the maximal cardinality of a set with pairwise integral distances in $\mathbb{Z}_n^m$ with or without further conditions on the position are given together with algorithms to determine them.

There are two connections to coding theory, first via the special case of arcs and caps, secondly by the observation that $\mathcal{I}(n, m)$ leads to a class of codes where the Hamming distances of the codewords have to fulfill certain modular restrictions.

For odd primes p the theory of integral point sets in $\mathbb{E}^m$ is transferred to a theory of integral point sets over $\mathbb{E}_p^m$ including the fundamental theorem about the characteristic of an integral simplex.

There are some open questions left and the given results motivate for further research on integral point sets over $\mathbb{Z}_n^m$ and $\mathbb{E}_n^m$, as they seem to be interesting combinatorial structures.

References

[1] N.H. Anning and P. Erdős. Integral distances. *Bull. Am. Math. Soc.*, 51:598–600, 1945.

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

[3] J. Bierbrauer. Large caps. *J. Geom.*, 76(1-2):16–51, 2003.

[4] J. Bierbrauer. *Introduction to coding theory.* Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC. xxiii, 390 p. , 2005.

[5] J. Bierbrauer and Y. Edel. Bounds on affine caps. *J. Comb. Des.*, 10(2):115–115, 2002.

[6] P. Brass, W. Moser, and J. Pach. *Research problems in discrete geometry.* New York, NY: Springer, 2005.

[7] C. Bron and J. Kerbosch. Finding all cliques of an undirected graph. *Commun. ACM*, 16:575–577, 1973.

[8] Francis (ed.) Buekenhout. *Handbook of incidence geometry: buildings and foundations.* Amsterdam: North-Holland. xi, 1420 p. , 1995.

[9] R. Calderbank and W.M. Kantor. The geometry of two-weight codes. *Bull. Lond. Math. Soc.*, 18:97–122, 1986.

[10] C. d'Andrea and M. Sombra. The Cayley-Menger determinant is irreducible for $n \geq 3$. *Siberian Mathematical Journal*, 46:90–97, 2005.

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

[12] P. Erdős. Integral distances. *Bull. Am. Math. Soc.*, 51:996, 1945.

[13] J. Fricke. On Heron simplices and integer embeding . *preprint*, 2002.

[14] R.K. Guy. *Unsolved problems in number theory. 3rd ed.* Problem Books in Mathematics. New York, NY: Springer-Verlag., 2004.

[15] H. Harborth. On the problem of P. Erdös concerning points with integral distances. *Ann. N.Y. Acad. Sci.*, 175:206–207, 1970.

[16] H. Harborth. Antwort auf eine Frage von P. Erdös nach fünf Punkten mit ganzzahligen Abständen. (Answer to a question of P. Erdös for five points with integer distances). *Elem. Math.*, 26:112–113, 1971.

[17] 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.

[18] H. Harborth, A. Kemnitz, and M. Möller. An upper bound for the minimum diameter of integral point sets. *Discrete Comput. Geom.*, 9(4):427–432, 1993.

[19] J.W.P. Hirschfeld. *Projective geometries over finite fields. 2nd ed.* Oxford Mathematical Monographs. Oxford: Clarendon Press., 1998.

[20] J. Huizenga. The maximum size of caps in $(\mathbb{Z}/n\mathbb{Z})^2$. *preprint*, 2005.

[21] A. Kemnitz. Punktmengen mit ganzzahligen Abständen. Habilitationsschrift, TU Braunschweig, 1988.

[22] A. Kohnert. Constructing two-weight codes with prescribed groups of automorphisms. *Discrete Appl. Math.*, 155(11):1451–1457, 2007.

[23] T. Kreisel and S. Kurz. There are integral heptagons, no three points on a line, no four on a circle. *Discr. Comput. Geom.*, to appear.

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

[25] S. Kurz. On the characteristic of integral point sets in $\mathbb{E}^m$. *Australas. J. Comb.*, 36:241–248, 2006.

[26] S. Kurz. Integral point sets over finite fields. *submitted*, 2007.

[27] S. Kurz and R. Laue. Bounds for the minimum diameter of integral point sets. *Australas.J.Comb.*, to appear.

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

[29] K. Menger. Untersuchungen über allgemeine Metrik. *Math. Ann.*, 100:75–163, 1928.

[30] S. Niskanen and P.R.J. Östergård. Cliquer user's guide, version 1.0. Technical Report T48, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, 2003.

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

[32] P.R.J. Östergård. A fast algorithm for the maximum clique problem. *Discrete Appl. Math.*, 120(1-3):197–207, 2002.

[33] L. Piepmeyer. Räumliche ganzzahlige Punktmengen. Master's thesis, TU Braunschweig, 1988.

[34] V.S. (ed.) Pless and W.C. (ed.) Huffman. *Handbook of coding theory. Vol. 1. Part 1: Algebraic coding. Vol. 2. Part 2: Connections, Part 3: Applications.* Amsterdam: Elsevier. 2169 p. $ 373.50 , 1998.

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

[36] J. Solymosi. Note on integral distances. *Discrete Comput. Geom.*, 30(2):337–342, 2003.

[37] G.M. Ziegler. Coloring Hamming graphs, optimal binary codes, and the 0/1-Borsuk problem in low dimensions. Alt, Helmut (ed.), Computational discrete mathematics. Advanced lectures. Berlin: Springer. Lect. Notes Comput. Sci. 2122, 159-171 (2001)., 2001.