ASSOCIATING A NUMERICAL SEMIGROUP TO
THE TRIANGLE-FREE CONFIGURATIONS

KLARA STOKES AND MARIA BRAS-AMORÓS
Universitat Rovira i Virgili
Av. Països Catalans 26
43007, Tarragona, Catalonia, Spain

(Communicated by Jintai Ding)

Abstract. It is proved that a numerical semigroup can be associated to the
triangle-free \((r, k)\)-configurations, and some results on existence are deduced.
For example it is proved that for any \(r, k \geq 2\) there exists infinitely many \((r, k)\)-
configurations. Most proofs are given from a graph theoretical point of view,
in the sense that the configurations are represented by their incidence graphs.
An application to private information retrieval is described.

1. Introduction

A combinatorial configuration is an incidence structure; a set of ‘points’ and a set
of ‘lines’, together with a symmetric incidence relation, such that there are \(k\) points
on every line, \(r\) lines through every point and through every pair of points there is
at most one line. A general reference for combinatorial configurations is [13] and
the recently published [14] collects many results on combinatorial configurations,
although it focuses on geometrically realizable configurations. One main problem
related to combinatorial configurations is the characterization of the parameters that
guarantee for their existence. Another related problem is the explicit construction of
combinatorial configurations, provided that they exist. One can find combinatorial
configurations in many applications such as in cryptography, coding theory, etc.

A field where combinatorial configurations are crucial is user-private information
retrieval (UPIR). UPIR aims to protect the query profile of users in front of a
data base or a search engine. One can define UPIR systems that do not need the
cooperation of the server by means of a peer-to-peer community [8, 9, 30]. Indeed, a
user, as a peer, can submit queries on behalf of other user peers and get the answers
to her/his own queries through other user peers. In [8, 9] user peers are distributed
among different private communication spaces using combinatorial configurations.

The use of combinatorial configurations implies that all users are connected to
the same number of communication spaces, each of these communication spaces
is shared by the same number of users and no two users share more than one
communication space.

It is proved in [27] that the optimal configurations for this scenario are exactly the
projective planes. However, this means that the number of users and communication
spaces as well as the number of communication spaces per user are very inflexible.
In [6] we developed some results on the existence and construction of combinatorial

2000 Mathematics Subject Classification: Primary: 05B30; Secondary: 51E30, 20M99.
Keywords and phrases: Block design, combinatorial configuration, partial linear space, girth,
umerical semigroup.
(r, k)-configurations for any pair (r, k), where r and k are respectively the number of communication spaces per user and the number of users per communication space. In particular it is proved in the latter that we can associate a subset of the natural numbers to the set of (r, k)-configurations and that this subset has the structure of a numerical semigroup.

One problem that the UPIR system could have is that two dishonest users connected to an honest user through two different communication spaces, could communicate themselves through a third communication space and infer some joint information. This can be avoided by simply avoiding circuits of length 6 in the bipartite graph representing the combinatorial configuration. Avoiding circuits of length 6 in this graph means avoiding triangles in the configuration. In another context, triangle-free configurations are also called (0,1)-geometries [7, 28].

Using the existence of regular graphs of girth 8 and any degree [25] we can demonstrate the existence of triangle-free (r, k)-configurations for every pair r, k ≥ 2. Composing triangle-free configurations we deduce that the subset of the natural numbers associated to the triangle-free (r, k)-configurations constitute a submonoid of the non-negative integers and with a particular construction, analogous to that in [6], we prove that this submonoid is in fact a numerical semigroup. This means, in particular, that there exists at least one (r, k)-configuration for any size large enough.

1.1. NOTIONS AND NOTATIONS. In this section we define the concepts that we will need later.

Definition 1. An incidence structure is a triple \( S = (\mathcal{P}, \mathcal{L}, \mathcal{I}) \), where \( \mathcal{P} \) is a set of points, \( \mathcal{L} \) a set of lines and \( \mathcal{I} \subset (\mathcal{P} \times \mathcal{L}) \cup (\mathcal{L} \times \mathcal{P}) \) is a symmetric incidence relation.

We are interested in a particular type of incidence structure called partial linear space.

Definition 2. A nonempty partial linear space is an incidence structure \( S \) where
- each point is on at least two lines,
- each line has at least two points and
- any two different points are incident with at most one line, or equivalently, any two different lines are incident with at most one point.

The partial linear spaces that we consider in this article, all have the same number \( k \) of points on any line and the same number \( r \) of lines through any point.

Definition 3. A partial linear space is said to have order \( (r - 1, k - 1) \) if each point is incident with \( r \) lines and each line is incident with \( k \) points. If \( r = k \) then the partial linear space is called balanced and is said to have order \( r - 1 \).

Definition 4. A combinatorial \((v_r, b_k)\)-configuration is a connected partial linear space with \(|\mathcal{P}| = v, |\mathcal{L}| = b\) and order \((r - 1, k - 1)\). When the number of points and lines is not important or not known, we will use the notation \((r, k)\)-configuration.

Definition 5. A geometric \((v_r, b_k)\)-configuration is a combinatorial \((v_r, b_k)\)-configuration which can be embedded into the real euclidean or the real projective plane.
Remark 1. In this text, when we use the word configuration we mean combinatorial configuration, and we do not attach any geometrical significance to the terms point and line.

Remark 2. In this article we consider the empty configuration, that is, a \((v_r, b_k)\)-configuration with \(v = |P| = 0\) and \(b = |L| = 0\), to be a \((0_r, 0_k)\)-configuration for every \(r,k \in \mathbb{N}, r,k \geq 2\).

From the definition of configuration the following well-known result is deduced:

**Proposition 1.** In a \((v_r, b_k)\)-configuration we have the relationship \(v_r = b_k\).

**Proof.** We have \(v = |P|\) points, each of these in \(r\) incidence relations with lines \(L\), hence \(v\) incidence relations \((p, L) \in \mathcal{I} \cap (P \times L)\). On the other hand we have \(b = |L|\) lines, each of these in \(k\) incidence relations with points, hence \(bk\) incidence relations \((L, p) \in \mathcal{I} \cap (L \times P)\). The incidence relation \(\mathcal{I}\) is symmetric, and the result follows. 

**Definition 6.** In a configuration, by a triangle we mean a triplet of points, pairwise connected by lines, such that there is no line incident with all the three points.

**Definition 7.** A triangle-free configuration is a configuration without triangles.

**Remark 3.** The triangle-free configurations are a special case of \((\alpha, \beta)\)-geometries \([7]\), with \((\alpha, \beta) = (0, 1)\). An equivalent definition of triangle-free configuration is therefore that, given a line \(L\) and a point \(p\) not on \(L\), there is at most one line through \(p\) intersecting \(L\), or equivalently, at most one point on \(L\) collinear with \(p\).

Sometimes it is easier to work with the incidence graph associated to an incidence structure, than to work with the incidence structure itself.

**Definition 8.** We define the incidence graph \(G = (V, E)\) of an incidence structure to be the graph with \(V = P \cup L\) as vertices and \(E = \mathcal{I}\) as edges.

A bipartite, \((r,k)\)-biregular graph is a bipartite graph which is \(r\)-regular in one vertex set and \(k\)-regular in the other. The incidence graph of a nonempty \((r,k)\)-configuration is a connected, bipartite, \((r,k)\)-biregular graph with girth at least 6. The incidence graph of a nonempty triangle-free configuration has girth at least 8. Conversely, for \(r,k \geq 2\), any connected, bipartite, \((r,k)\)-biregular graph of girth at least 8 is the incidence graph of a triangle-free configuration. This is easy to see. Let the \(r\)-regular vertex set represent the points of an incidence structure, and let the \(k\)-regular vertex set represent the lines. Any point in this incidence structure is then incident with exactly \(r \geq 2\) lines and any line is incident with exactly \(k \geq 2\) points. The third condition in Definition 2 of a partial linear space is that there should be at most one line through any pair of points. But two lines through a pair of points are represented in the incidence graph as a cycle of length 4. Since the girth of the incidence graph is at least 8, there can be no cycle of length 4. Indeed it is clear that the set of configurations and the set of connected, bipartite, \((r,k)\)-biregular graphs of girth at least 6 are in bijection. A triangle is represented in the incidence graph as a cycle of length 6, so an incidence graph of girth at least 8 represents a configuration without triangles. It is obvious from this reasoning that the incidence graph of an incidence structure determines it exactly.

In this article we will not distinguish the incidence graph of a configuration from the configuration itself. In particular we will treat the set of edges of the incidence graph, as if it was the set of elements in the incidence relation \(\mathcal{I}\).
1.2. Previous results. Below the state of the art of the research on the existence of triangle-free configurations is explained, as far as it is known to the authors. The smallest polygon that can be contained in a triangle-free configuration is a quadrangle. A quadrangle is a set of four different lines \( \{L_i\}_{i=1}^4 \) and four different points \( \{p_i\}_{i=1}^4 \) such that the incidence relation of the configuration defines a sequence

\[
L_1 I p_1 I L_2 I p_2 I L_3 I p_3 I L_4 I p_4 I L_1,
\]

that is, a cycle of length 8 in the incidence graph. A triangle-free configuration in which every point is on a quadrangle is called a generalized quadrangle. The incidence graph of a generalized quadrangle of order \((r-1,k-1)\) is a bipartite, \((r,k)\)-biregular graph with girth 8 and diameter 4. The following is a necessary condition for a generalized quadrangle to exist.

**Proposition 2.** [20] If a generalized quadrangle of order \((r-1,k-1)\) exists, then it has number of points

\[
v = |\mathcal{P}| = k((r-1)(k-1) + 1)
\]

and number of lines

\[
b = |\mathcal{L}| = r((r-1)(k-1) + 1).
\]

There are several known families of generalized quadrangles [20]. All these families, except one, have order \((r-1,k-1)\) where \(r-1\) and \(k-1\) are powers of the same prime. The exception is a family containing generalized quadrangles of order \((r-1,k-1) = (q-1,q+1)\) where \(q\) is a power of a prime. The results on the orders of known generalized quadrangles as appearing in the book ‘Finite generalized quadrangles’ by Payne and Thas [20] is concluded in Proposition 3.

**Proposition 3.** Let \(q\) be a power of a prime. Then there exists a generalized quadrangle of order \((r-1,k-1)\) if \((r-1,k-1) \in \{(q,1), (q,q),(q,q^2),(q^2,q^3),(q-1,q+1)\}\).

The first question on the existence of triangle-free configurations, is answered by the following Theorem 1, but only in the balanced case. We have not found previous general results in the non-balanced case, that is, when \(r \neq k\).

**Theorem 1.** [14] For every \(r \geq 2\) there exist (geometric) \((r,r)\)-configurations that are triangle-free.

The \((r,r)\)-configuration used in the proof is what Pisanski calls a generalized Grey configuration [21] and Grünbaum a LC\((r)\) configuration [14], which has \(r^r\) points and \(r^r\) lines.

Grünbaum’s book [14], which mostly treats configurations that are geometrically realizable, contains the following theorem which collects the available knowledge on the existence of triangle-free geometric \((3,3)\)-configurations.

**Theorem 2.** For every \(n \geq 15\) except \(n = 16\) and possibly \(n = 23\) and 27, there are triangle-free geometric \((3,3)\)-configurations.

Theorem 2 contains the results by Betten et al. [3], who counted all triangle-free combinatorial configurations with \(v \leq 21\) for \(r = k = 3\). Their calculations show us that there exist triangle-free combinatorial \((3,3)\)-configurations with

\[
v \in \{15, 17, 18, 19, 20, 21\}.
\]
The unique triangle-free \((3,3)\)-configuration with \(n = 15\) is the famous Cremona-Richmond configuration, which is a generalized quadrangle. In the tables of [3] it can be observed how the number of triangle-free combinatorial configurations grows very quickly with \(v\).

Theorem 2 also contains results by Visconti [31]. Finally, the proof of Theorem 2 constructs larger configurations joining smaller ones in two different ways. This is interesting, and it is worth pointing out that both these constructions are different from the ‘addition’ of configurations used in this article. Using these constructions, starting with two triangle-free \((r,r)\)-configurations with \(p\) and \(q\) points and \(p\) and \(q\) lines, the result is either a triangle-free \((r,r)\)-configuration with \(p + q - 1\) points and \(p + q - 1\) lines, or a triangle-free \((r,r)\)-configuration with \(p + q + 1\) points and \(p + q + 1\) lines.

Any geometric configuration is also a combinatorial configuration, and there is no triangle-free \((3,3)\)-configuration with \(v = 16\) [18], so available knowledge on the existence of combinatorial \((3,3)\)-configurations at this moment coincides with the knowledge on the existence of geometric \((3,3)\)-configurations in Theorem 2. Observe that Theorem 2 does not count the number of triangle-free \((3,3)\)-configurations. It is not known how many of the triangle-free \((3,3)\)-configurations counted by Betten et al. are geometrically realizable [14].

Considering larger parameters, there is much less known already for triangle-free \((4,4)\)-configurations. Recently a triangle-free \((4,4)\)-configuration with \(v = 40\) was constructed by van Maldeghem [5]. Since it satisfies the bound from Proposition 2, Proposition 12 says that it is a generalized quadrangle. There are also triangle-free \((4,4)\)-configurations with \(v = 60\) (found by Boben), \(v = 120\) and \(v = 256\) [14], plus infinite families of triangle-free \((4,4)\)-configurations constructed from these using the two constructions from the proof of Theorem 2.

For triangle-free \((k,k)\)-configurations the generalized Gray / LC \((r)\) configuration can be used to construct infinite families of triangle-free \((k,k)\)-configurations in the same way.

In [26], Sinha constructs a family of triangle-free \((r,k)\)-configurations with \(r = 3\) and special parameters. The Cremona-Richmond configuration appears as the smallest example of the members of this family.

Graphs and configurations are not the same thing, but some results in graph theory can be interpreted as if they treated configurations. Many proofs in this article are also expressed in the language of graphs. In particular, the following result on the existence of regular graphs, due to Sachs [25], is important and will be used later.

**Theorem 3.** Let \(r \geq 3\) and \(g \geq 2\) be two integers. Then there always exists an \(r\)-regular graph of girth \(g\).

Because of Sachs’ Theorem 3, there is always an \(r\)-regular graph of girth \(g\), so it makes sense to ask for the smallest one. In graph theory an \((r,g)\)-cage is an \(r\)-regular graph of girth \(g\) with the smallest possible number of vertices. It is conjectured that all cages of even girth are bipartite [22, 32]. We can identify a triangle-free \((r,k)\)-configuration with its incidence graph, a connected, bipartite, \((r,k)\)-biregular graph of girth at least 8. If we suppose the conjecture true, we therefore have that a triangle-free \((r,r)\)-configuration with the smallest possible number of points and lines is exactly an \((r,8)\)-cage.
There is a well-known lower bound for the number of vertices in an \((r,g)-\)cage [4] giving us the lower bound for the number of vertices in an \((r,8)-\)cage

\[
n_0(r) = 2(1 + (r - 1) + (r - 1)^2 + (r - 1)^3) = \frac{2(r - 1)^4 - 2}{r - 2}.
\]

A regular cage of even girth that reaches this bound, is the incidence structure of a (balanced) generalized quadrangle [4]. Lazebnik, Ustimenko and Woldar constructed small \(r\)-regular graphs of girth \(g\) for any \(r \geq 2\) and \(g \geq 3\) [15].

**Proposition 4.** [15] Let \(r \geq 2\) and \(g \geq 5\) be integers, and let \(q\) denote the smallest odd prime power for which \(q \geq r\). Then there exists an \(r\)-regular graph of girth \(g\) and number of vertices \(2rq^{3/4-a}\), with \(a = 4, 11/4, 7/2, 13/4\) for \(g = 0, 1, 2, 3\) (mod 4) respectively.

The smallest known \(r\)-regular graphs of girth 8, when \(r\) is not a power of a prime, are at the moment the ones constructed by Balbuena.

**Proposition 5.** [2] Let \(r\) be an integer and \(q\) a power of a prime such that \(3 \leq r \leq q\). Then there exists an \(r\)-regular bipartite graph of girth 8 with \(rq^2 - q\) vertices in each bipartite set.

The smallest known \(q\)-regular graphs when \(q\) is a power of a prime, were constructed by Gács and Héger.

**Proposition 6.** [12] Let \(q\) be a power of a prime. If \(q\) is even then there exists a \(q\)-regular graph of girth 8 and with \(2(q^3 - 3q - 2)\) vertices. If \(q\) is odd, then there exists a \(q\)-regular graph of girth 8 and with \(2q(q^2 - 2)\) vertices.

As recently was proved by Araujo-Pardo [1], small odd girth \(g\) graphs can be obtained from small even girth \(g + 1\) graphs. In particular, upper bounds on the number of vertices of an \((r,7)-\)cage can be obtained from the upper bound on the number of vertices of an \((r,8)-\)cage.

**Proposition 7.** [1] Let \(r \geq 3\) be an odd integer. If \(f(r)\) is an upper bound for the number of vertices of an \((r,8)-\)cage, then an upper bound for the number of vertices of an \((r,7)-\)cage is

\[
f(r) - \frac{2(r - 1)^2 - 2}{r - 2}.
\]

2. The numerical semigroup associated to the triangle-free \((r,k)-\)configurations

2.1. Associating a set of integers to the existence of triangle-free \((r,k)-\)configurations. From Proposition 1 we can deduce that for any \((v_r,b_k)-\)configuration we have the following expressions for \(v\) and \(b\):

\[
v = \frac{bk}{r} = d\frac{k}{\gcd(r,k)}
\]

and symmetrically

\[
b = \frac{vr}{k} = d'\frac{r}{\gcd(r,k)}.
\]
Since \( v \) and \( b \) are integers, so are \( d \) and \( d' \). We also have

\[
\begin{align*}
d &= \frac{v \gcd(r,k)}{k} \\
&= \frac{bk \gcd(r,k)}{r} \\
&= \frac{b \gcd(r,k)}{r} = d'.
\end{align*}
\]

To any \((r,k)\)-configuration, with or without triangles, we can therefore associate the integer \( d \). On the other hand, given \( r \) and \( k \), any \( d \in \mathbb{N} \) determines two integers \( v \) and \( b \), perhaps corresponding to the number of points and lines of a configuration.

In the following we will consider the set of integers such that they may be associated to a triangle-free configuration. The aim of this article is to prove that this set is a numerical semigroup.

**Definition 9.** For \( r, k \in \mathbb{N} \), \( r, k \geq 2 \) we define

\[
\mathcal{S}_{(r,k)} := \{ d \in \mathbb{N} : \exists \text{ triangle-free } (v_r, b_k) - \text{configuration and } v = \frac{d k}{\gcd(r,k)}, b = \frac{d r}{\gcd(r,k)} \}.
\]

2.2. **The set of integers which we have associated to the triangle-free \((r,k)\)-configurations forms a numerical semigroup.** In this section we will prove that \( \mathcal{S}_{(r,k)} \) is a numerical semigroup. A numerical semigroup is a subset \( S \subset \mathbb{N} \cup \{0\} \), so that \( S \) is closed under addition, \( 0 \in S \) and the complement \( (\mathbb{N} \cup \{0\}) \setminus S \) is finite.

We will use the following standard result on numerical semigroups. We say that a set of integers are coprime if the ideal they generate is \( \mathbb{Z} \).

**Lemma 1.** A set of integers generate a numerical semigroup if and only if they are coprime.

The proof of this lemma can be found in [24].

Lemma 1 says that in order to prove that a set is a numerical semigroup it is enough to prove that the set is a submonoid of the natural numbers with coprime elements. In particular it is enough to prove that

- \( 0 \in \mathcal{S}_{(r,k)} \),
- \( \mathcal{S}_{(r,k)} \) is closed under addition,
- at least two elements of \( \mathcal{S}_{(r,k)} \) are coprime.

The two first conditions ensure that the subset \( \mathcal{S}_{(r,k)} \) of the natural numbers is a monoid. The operation of the monoid is addition. The last condition ensures that the monoid contains the numerical semigroup generated by the two coprime elements. The complement of this numerical semigroup is finite, therefore also the complement of the monoid, and we deduce that it is a numerical semigroup.

2.2.1. **The set of integers associated to the triangle-free \((r,k)\)-configurations is a submonoid of the natural numbers.** We first observe that since we consider the empty set being a triangle-free \((r,k)\)-configuration, we have \( 0 \in \mathcal{S}_{(r,k)} \).

We will now prove that the set \( \mathcal{S}_{(r,k)} \) is closed under addition.

**Lemma 2.** If there exist triangle-free \((r,k)\)-configurations \( S_1 = (P_1, L_1, I_1) \) and \( S_2 = (P_2, L_2, I_2) \) with mutually disjoint point and line sets, then there also exists a triangle-free \((r,k)\)-configuration

\[
S_1 \oplus S_2 = (P_1 \cup P_2, L_1 \cup L_2, I).
\]
Proof. First observe that if we denote the empty triangle-free \((r, k)\)-configuration by \(\emptyset\), then, for any triangle-free \((r, k)\)-configuration \(S\), we have in a natural way
\[
S \oplus \emptyset = S
\]
and
\[
\emptyset \oplus S = S.
\]
Now suppose we have a nonempty triangle-free \((r, k)\)-configuration \(S\) with vertices \(P_1 = \{p_{1,1}, \ldots, p_{1,t}\}\), \(L_1 = \{L_{1,1}, \ldots, L_{1,b}\}\) and another nonempty triangle-free \((r, k)\)-configuration \(S_2\) with vertices \(P_2 = \{p_{2,1}, \ldots, p_{2,t}\}\), \(L_2 = \{L_{2,1}, \ldots, L_{2,b}\}\). Consider the graph with vertices
\[
P_1 \cup L_1 \cup P_2 \cup L_2\]
and edges
\[
I_1 \cup I_2.
\]
Observe that from the definition of nonempty partial linear space we have \(r, k \geq 2\), so we can assume without loss of generality that
\[
(p_{1,1}^1, L_{1,1}^1), (p_{1,1}^2, L_{1,1}^2) \in I_1 \cup I_2.
\]
Replace the edges \((p_{v_1}^1, L_{b_1}^1)\) and \((p_{v_1}^2, L_{b_1}^2)\) by \((p_{v_1}^1, L_{b_1}^0)\) and \((p_{v_1}^2, L_{b_1}^0)\) and consider the resulting incidence relation \(I\). We want to prove that the incidence graph of \((P_1 \cup P_2, L_1 \cup L_2, I)\) is a connected, bipartite, \((r, k)\)--biregular graph of girth at least 8.

But that \((P_1 \cup P_2, L_1 \cup L_2, I)\) is a connected, bipartite \((r, k)\)--biregular graph is obvious, so we only need to prove that the girth is at least 8. Now almost all incidence relations in \(I\) are the same as in \(I_1 \cup I_2\), so the only delicate part of the graph is where the two original graphs were connected, that is, we need to check that the vertices \(p_{v_1}^1, p_{v_1}^2, L_{b_1}^1, L_{b_1}^2\) are not on any cycle of length less than 8.

But \(S_1\) and \(S_2\) have girth at least 8, so the shortest path between \(p_{v_1}^1\) and \(L_{b_1}^1\) inside \(S_1\) other than \((p_{v_1}^1, L_{b_1}^1)\) (which we have removed) has length at least 7, and the shortest path between \(p_{v_1}^2\) and \(L_{b_1}^2\) inside \(S_2\) other than \((p_{v_1}^2, L_{b_1}^2)\) (which we have removed) has also length at least 7. Therefore, in \((P_1 \cup P_2, L_1 \cup L_2, I)\) the vertices \(p_{v_1}^1, p_{v_1}^2, L_{b_1}^1, L_{b_1}^2\) can not be on a cycle of length less than 8. We get that \((P_1 \cup P_2, L_1 \cup L_2, I)\) is a triangle-free \((r, k)\)-configuration. \(\square\)

**Proposition 8.** \(\mathcal{S}_{(r,k)}\) is a submonoid of the natural numbers.

Proof. As commented before, after we consider the empty set to be a triangle-free \((r, k)\)-configuration, we have \(0 \in \mathcal{S}_{(r,k)}\). Now from Lemma 2 we get that if we have two triangle-free \((r, k)\)-configurations \(S_1\) and \(S_2\) with parameters satisfying
\[
|P_1| = v_1 = d_1 \frac{k}{\gcd(r, k)},
\]
\[
|L_1| = b_1 = d_1 \frac{r}{\gcd(r, k)}
\]
and
\[
|P_2| = v_2 = d_2 \frac{k}{\gcd(r, k)},
\]
\[
|L_2| = b_2 = d_2 \frac{r}{\gcd(r, k)}.
\]
then there exists a triangle-free \((r, k)\)-configuration \(S = S_1 \oplus S_2\) with point and line sets satisfying
\[
v = |\mathcal{P}| = |\mathcal{P}_1 \cup \mathcal{P}_2| = d_1 \frac{k}{\gcd(r, k)} + d_2 \frac{k}{\gcd(r, k)} = (d_1 + d_2) \frac{k}{\gcd(r, k)}
\]
and
\[
b = |\mathcal{L}| = |\mathcal{L}_1 \cup \mathcal{L}_2| = d_1 \frac{r}{\gcd(r, k)} + d_2 \frac{r}{\gcd(r, k)} = (d_1 + d_2) \frac{r}{\gcd(r, k)}.
\]
So if \(d_1, d_2 \in \mathcal{G}_{(r,k)}\), then also \(d_1 + d_2 \in \mathcal{G}_{(r,k)}\).
2.2.2. The submonoid contains two coprime elements. We start by proving that given any pair of natural numbers \( r, k \geq 2 \), there exists at least one element in \( \mathcal{S}_{(r,k)} \) different from 0. We do this by constructing a nonempty triangle-free \((r,k)\)-configuration.

For the construction we use a regular graph of girth at least 8.

Theorem 3 says that for any \( n \geq 3 \) and \( g \geq 2 \) there exists an \( n \)-regular graph of girth \( g \). In particular for any \( n \geq 3 \) there exists an \( n \)-regular graph of girth at least 8. We will use one of these graphs to construct a connected, bipartite, \((r,k)\)-configuration.

Proposition 9. For any pair of integers \( r, k \geq 2 \), there exists at least one non-zero integer in \( \mathcal{S}_{(r,k)} \).

Proof. Consider the complete bipartite graph \( K_{r,k} \), with edge set \( E \) and vertex set \( V \). We consider one spanning tree \( T_{r,k} \) of \( K_{r,k} \). Then \( T_{r,k} \) has the same vertex set \( V \) as \( K_{r,k} \), but its edge set \( E' \subset E \) is smaller. We have

\[
|E'| = r + k - 1.
\]

The number of edges in \( K_{r,k} \) outside \( T_{r,k} \), that is, in \( E - E' \), is

\[
n = rk - r - k + 1 = (r - 1)(k - 1).
\]

Suppose \( n \geq 3 \). (This excludes the cases \((r,k) \in \{(2,2), (2,3), (3,2)\}\), which must be treated separately and will be so, at the end of this proof.)

From Theorem 3 we know that there exists at least one \( n \)-regular graph of girth at least 8. Take one of these graphs and call it \( G \). Associate to each of the vertices of \( G \) a copy of the complete bipartite graph \( K_{r,k} \). For all edges \( ab \) in \( G \), consider its end vertices \( a \) and \( b \) and let \( A \) and \( B \) be the copies of \( K_{r,k} \) associated to these vertices. Also let \( T_A \) and \( T_B \) be the corresponding spanning trees in \( A \) and \( B \). Now choose one edge \( x_{AB} \) in \( A \), but not in \( T_A \) and one edge \( x_{BY} \) in \( B \), but not in \( T_B \) and swap them so that we instead get two edges \( x_{AY} \) and \( x_{BY} \). Since \( G \) is \( n \)-regular and \( n \) is the number of edges in \( K_{r,k} \) that are not in its spanning tree, we can choose different edges \( x_{AY} \) and \( x_{BY} \) for every edge in \( G \).

In this way we get a bipartite, \((r,k)\)-biregular graph of girth at least 8, from a \( n \)-regular graph of girth at least 8, with \( n = (r - 1)(k - 1) \).

The resulting graph may not be connected. If this is the case, we can proceed in two ways.

- We can choose any of the connected subgraphs, and consider that graph to be the incidence graph of the triangle-free configuration we want to construct.
- If we choose the smallest connected subgraph, then we minimize the size of the smallest known triangle-free \((r,k)\)-configuration proved to exist in this manner.

We can use the ‘addition’ law from Lemma 2 to connect all the connected subgraphs.

In any case we get a connected, bipartite, \((r,k)\)-biregular graph of girth at least 8, hence the incidence graph of a triangle-free \((r,k)\)-configuration.

We still must treat the cases \((r,k) \in \{(2,2), (2,3), (3,2)\}\).

- When \((r,k) = (2,2)\), the connected graph with 8 vertices of degree 2 is a connected, bipartite, \((2,2)\)-biregular graph of girth 8, so it is the incidence graph of the smallest nonempty triangle-free \((2,2)\)-configuration. It has parameters \( d = v = b = 4 \).
• When \((r, k) = (2, 3)\), the following is an incidence list of a triangle-free \((2, 3)\)-configuration. We have represented the points as \(P = \{1, \ldots, 9\}\) and the lines as \(L = \{A, \ldots, F\}\). Consequently \(v = 9\), \(b = 6\) and \(d = 3\).

\[
\begin{array}{c|ccc}
A & 1 & 2 & 9 \\
B & 2 & 3 & 8 \\
C & 3 & 4 & 7 \\
D & 4 & 5 & 1 \\
E & 5 & 6 & 8 \\
F & 6 & 7 & 9 \\
\end{array}
\]

• When \((r, k) = (3, 2)\), we can consider the dual triangle-free configuration of the previous example. This concludes the proof.

Remark 4. Observe that since a bipartite graph always has even girth, even if we start with a \(n\)-regular graph of girth at least 7, the result will be a graph with girth at least 8. This is interesting if we want the corresponding triangle-free configuration to be as small as possible.

We will now construct a second element of \(S_{(r,k)}\), such that the element of Proposition 9 and the new one are coprime. In order to do so we need the following lemma.

Lemma 3. Suppose that \(r \geq 3\) and \(k \geq 3\). Consider a nonempty triangle-free \((r,k)\)-configuration \((P, L, I)\). Then there exist three different points \(p_1, p_2\) and \(p_3\) and three different lines \(L_1, L_2\) and \(L_3\), such that \((p_1, L_1), (p_2, L_2), (p_3, L_3) \in I\), but \((p_i, L_j) \notin I\) if \(i \neq j\).

Proof. Since the girth of the incidence graph is at least 8, no cycle of length 7 exists. The graph is connected and has at least 8 edges. It therefore exists a path of length 6 not passing through the same vertex twice. Without loss of generality we may suppose that if \(r \geq 3\), then the path starts with a vertex representing a point and ends with a vertex representing a point, and if \(r < 3\) but \(k \geq 3\), then the path starts with a vertex representing a line and ends with a vertex representing a line. (Remember that the graph is bipartite, with the points on one side and the lines on the other.)

Take the first and the fourth edge of this path. The ends of these edges are separated by paths of length at least two. Also take the seventh (the last) vertex of the path. It is separated from the first and the forth edge by paths of length at least two. If \(r \geq 3\), then we have chosen the path so that the seventh vertex represents a point, so it has degree at least 3. If \(r < 3\) but \(k \geq 3\), then we have chosen the path so that the seventh vertex represents a line, so also in this case it has degree at least 3. Therefore it will have at least two neighbors not in the path. Since the girth of the graph is larger than 4, these two neighbors can not be simultaneously neighbors of the first vertex of the path. Moreover, since the girth is larger than 7, if we choose a vertex, neighbor to the seventh vertex, but not to the first vertex, it will be separated from all first six vertices on the path by paths of at least length 2. We take the edge between the seventh vertex an this vertex. Together with the two edges selected before, they constitute a set of three edges where the ends are all different and ends of different edges are not neighbors.
Consequently we obtain three edges \((p_1, L_1), (p_2, L_2), (p_3, L_3)\), so that the three points and the three lines are all different and such that \((p_i, L_j) \notin \mathcal{I}\) if \(i \neq j\).

We are now ready to prove the existence of two coprime elements of \(\mathcal{S}(r, k)\).

**Proposition 10.** \(\mathcal{S}(r, k)\) contains two elements \(m \neq 0\) and \(am + 1\), with \(a \in \mathbb{N}\), so that the two elements are coprime.

**Proof.** Consider first the case \((r, k) = (2, 2)\). We saw in the proof of Proposition 9 that the connected graph with 8 vertices of degree 2 is a connected, bipartite, \((2, 2)\)-biregular graph of girth 8, so it is the incidence graph of the smallest nonempty triangle-free \((2, 2)\)-configuration. The parameters of this triangle-free configuration were \(v = b = d = 4\).

Actually, for any integer \(d \geq 4\), the connected graph with \(2d\) vertices of degree 2 gives us a triangle-free \((2, 2)\)-configuration with associated integer \(d = v = b\). Therefore we have \(\mathcal{S}_{2,2} = \mathbb{N}_0 \setminus \{1, 2, 3\}\). This proves that \(\mathcal{S}_{2,2}\) is a numerical semigroup and also reveals completely the structure of \(\mathcal{S}_{2,2}\).

Now we may suppose \(r \geq 3\) or \(k \geq 3\). By Proposition 9 and since \(\mathcal{S}(r, k) \subseteq \mathbb{N}_0\), there is a minimal non-zero element \(m\) in \(\mathcal{S}(r, k)\).

Select a triangle-free \((r, k)\)-configuration \(\mathcal{S}\) with

\[
v = m \frac{k}{\gcd(r, k)}
\]

and

\[
b = m \frac{r}{\gcd(r, k)}.
\]

Take

\[
a = \frac{rk}{\gcd(r, k)}
\]
copies of \(\mathcal{S}\). Let us call the vertices of the \(i\)th copy

\[
p_1^{(i)}, \ldots, p_v^{(i)}, L_1^{(i)}, \ldots, L_b^{(i)}.
\]

By Lemma 3 we can assume that

\[
(p_1^{(i)}, L_1^{(i)}), (p_2^{(i)}, L_2^{(i)})\text{ and } (p_v^{(i)}, L_b^{(i)})
\]

are edges of the \(i\)th copy and that all other combinations

\[
(p_a^{(i)}, L_b^{(i)})
\]

with \(a \in \{1, 2, v\}\) and \(b \in \{1, 2, b\}\), are not edges of the \(i\)th copy.

Consider \(\alpha := k/\gcd(r, k)\) further vertices

\[
p_1', \ldots, p_{\alpha}',
\]

and \(\beta := r/\gcd(r, k)\) further vertices

\[
L_1', \ldots, L_{\beta}'.
\]

Now perform the following changes to the edge set of the graph defined by the union of all parts previously mentioned. It may be clarifying to contemplate Figure 2. In the figure the edges to be removed are dashed, while the edges to add are thick lines.
“Add” together the \(a\) copies of the original configurations. That is, for all \(1 \leq i \leq a - 1\) replace the edges 
\[(p^{(i)}_v, L^{(i)}_b) \text{ and } (p^{(i+1)}_1, L^{(i+1)}_1)\]
by 
\[(p^{(i)}_v, L^{(i+1)}_1) \text{ and } (p^{(i+1)}_1, L^{(i)}_b).\]

Also, remove the edges \((p^{(i)}_2, L^{(i)}_2)\) for all \(1 \leq i \leq a\).

Add the edges
\[(p'_1, L_2^{(1)}), (p'_1, L_2^{(2)}), \ldots, (p'_1, L_2^{(a)}),\]
\[(p'_2, L_2^{(r+1)}), (p'_2, L_2^{(r+2)}), \ldots, (p'_2, L_2^{(2r)}),\]
\[
\vdots
\]
\[(p'_a, L_2^{(a-r+1)}), (p'_a, L_2^{(a-r+2)}), \ldots, (p'_a, L^{(a)}_2)\]
and
\[(p_2^{(1)}, L_1^{(1)}), (p_2^{(2)}, L_1^{(2)}), \ldots, (p_2^{(k)}, L_1^{(k)}),\]
\[(p_2^{(k+1)}, L_2^{(1)}), (p_2^{(k+2)}, L_2^{(2)}), \ldots, (p_2^{(2k)}, L_2^{(1)}),\]
\[
\vdots
\]
\[(p_2^{(a-k+1)}, L_2^{(a)}), (p_2^{(a-k+2)}, L_2^{(b)}), \ldots, (p_2^{(a)}, L_2^{(b)}).\]

The constructed graph is connected, bipartite, and \((r, k)\)-biregular. Since the edges \((p_1^{(i)}, L_1^{(i)})\), \((p_2^{(i)}, L_2^{(i)})\) and \((p^{(i)}_v, L^{(i)}_b)\) have been chosen as permitted by Lemma 3 and the copies of the original graph are bipartite, we get that a cycle passing through two different copies has length at least \(8\). Together with the fact that the girth of the \(a\) original copies was at least \(8\), this implies that the girth of the resulting graph also must be at least \(8\). So we constructed an incidence graph of a triangle-free \((r, k)\)-configuration, which we may call \(S'\).

We have
\[v' = |P'| = a|P| + \alpha\]
\[= a|P| + \frac{k}{\gcd(r, k)}\]
\[= \frac{k \cdot \gcd(r, k)}{\gcd(r, k)}\]
\[= \frac{amk}{\gcd(r, k)} + \frac{k}{\gcd(r, k)}\]
\[= (am + 1)\frac{k}{\gcd(r, k)}\]
and
\[b' = |L'| = a|L| + \beta\]
\[= a|L| + \frac{r}{\gcd(r, k)}\]
\[= \frac{amr}{\gcd(r, k)} + \frac{r}{\gcd(r, k)}\]
\[= (am + 1)\frac{r}{\gcd(r, k)}\]
and so \(am + 1 \in \mathcal{S}_{(r,k)}\) \(\Box\)

From Proposition 10 we deduce that \(\mathcal{S}_{(r,k)}\) contains two coprime elements, so that they generate a numerical semigroup and this semigroup is contained in \(\mathcal{S}_{(r,k)}\).
So the complement of \(\mathcal{S}_{(r,k)}\) in \(\mathbb{N}_0\) is finite and \(\mathcal{S}_{(r,k)}\) is a numerical semigroup.
Figure 2. Construction of a triangle-free \((r,k)\)-configuration with associated integer \(am + 1\) from a smaller triangle-free \((r,k)\)-configuration with associated integer \(m\) using \(\alpha + \beta\) extra vertices.
3. Bounds on the existence of triangle-free configurations

Given the numerical semigroup structure of $\mathcal{S}_{(r,k)}$ it is natural to formulate the following questions.

- Which is the smallest non-zero element in $\mathcal{S}_{(r,k)}$?
- Since the complement $\mathbb{N} \setminus \mathcal{S}_{(r,k)}$ is finite, which is the largest element in the complement?

The following notation is standard.

**Definition 10.** The multiplicity of a numerical semigroup is its smallest non-zero element.

**Definition 11.** The conductor of a numerical semigroup is the smallest element of the semigroup such that all subsequent natural numbers belong to the semigroup.

### 3.1. Lower bounds on the existence of triangle-free configurations.

The smallest number of points and lines of a triangle-free $(r,k)$-configuration is necessarily the number of points and lines of a generalized quadrangle of order $(r-1,k-1)$, should it exist (see Section 1.2).

**Proposition 11.** A triangle-free $(v_r,b_k)$-configuration satisfies

$$ v \geq k((r-1)(k-1) + 1) $$

and

$$ b \geq r((r-1)(k-1) + 1). $$

**Proof.** Consider a line $L \in \mathcal{L}$ and the two sets

$$ A = \{ x : x \in \mathcal{P} \text{ and } (x,L) \notin \mathcal{I} \} $$

and

$$ B = \{ x : x \in \mathcal{P} \text{ and } (x,L) \notin \mathcal{I} \text{ and } \exists M \in \mathcal{L}, y \in \mathcal{P} \text{ such that } xIMyIL \}. $$

The number of points not on $L$ is $|A| = |\mathcal{P}| - k$. The number of lines concurrent with $L$ is $k(r-1)$ and these lines have together $|B| = k(r-1)(k-1)$ points which are not their intersection points with $L$. Obviously $A \supset B$, so

$$ |\mathcal{P}| - k = |A| \geq |B| = k(r-1)(k-1), $$

that is,

$$ v = |\mathcal{P}| \geq k((r-1)(k-1) + 1). $$

Dually

$$ b = |\mathcal{L}| \geq r((r-1)(k-1) + 1). $$

**Proposition 12.** If the bounds in Proposition 11 are attained, then the triangle-free $(v_r,b_k)$-configuration is a generalized quadrangle.

**Proof.** If the bounds in Proposition 11 are attained, then the sets $A$ and $B$ have the same cardinality, and since $B \subset A$, they are equal. Therefore the points $x$ not incident with $L$ but connected to $L$ through a pair $(M,y) \in \mathcal{L} \times \mathcal{P}$ are all points of $\mathcal{P}$ except those incident with $L$. In other words, for every point $x$ not incident with $L$ there is a pair $(M,y) \in \mathcal{L} \times \mathcal{P}$ for which $xIMyIL$. On the other hand, $\mathcal{S}$ is a $(0,1)$-geometry (see Remark 3), so for any point $x$ not incident with $L$, there can be at most one pair $(M,y)$ such that $xIMyIL$. Since the existence of a unique pair of such $(M,y)$ is exactly the definition of a generalized quadrangle [20], this proves the statement.

---

**Advances in Mathematics of Communications**

Volume 5, No. 2 (2011), 351–371
Remark 5. The proof of Proposition 11 is a simple generalization of the proof of Proposition 2 as it appears in [20].

Remark 6. Proposition 11 gives a lower bound on the multiplicity of the numerical semigroup $S_{(r,k)}$.

3.2. Upper bounds on the existence of triangle-free configurations.
In this section we consider two different upper bounds on the existence of triangle-free configurations. The first bound is an upper bound on the multiplicity of the numerical semigroup $S_{(r,k)}$, hence an upper bound on the size of the smallest existing triangle-free configuration for fixed $r$ and $k$. The second bound is an upper bound on the conductor of the numerical semigroup $S_{(r,k)}$, hence an upper bound on the size of configuration from which there exists at least one configuration for all admissible sizes which are larger than this bound.

3.2.1. Upper bounds on the existence of triangle-free configurations based on the multiplicity of $S_{(r,k)}$. If the lower bound on the multiplicity is deduced from the definition of triangle-free configurations, the upper bound on the other hand relies on their explicit constructions. Expressed in terms of graphs, in order to prove that there always exists a triangle-free $(r,k)$-configuration it is necessary to prove that for every pair of natural numbers $r, k \geq 2$ there exists a connected, bipartite, $(r,k)$-biregular graph of girth at least 8. This was proved in Proposition 9. In the proof of Proposition 9 we needed the existence of an $r$-regular graph of girth 8. For this we used Theorem 3 due to Sachs. The graphs that Sachs used to prove Theorem 3 are constructed recursively. As the parameters grow they get large quickly. In order to obtain smaller, general, upper bounds on the multiplicity of $S_{(r,k)}$, the $n$-regular graphs from Propositions 5, 6 and 7 are better suited. From Proposition 4 we get that there exists an $n$-regular graph of girth 7 and $2nq^2$ vertices, for a prime power $q \geq \frac{n-1}{2}$. Replacing each vertex of this graph with the vertices of the complete, bipartite $(r,k)$-regular graph on $r+k$ vertices, means multiplying the number of vertices by $r+k$. So the resulting incidence graph has
\[2nq^2(r+k) = 2(r-1)(k-1)(r+k)q^2\]
vertices. We get the following:

Proposition 13. For any integers $r, k \geq 2$
1. there exists a triangle-free $(r,k)$-configuration with $2(r-1)(k-1)q^2$ points and $2(r-1)(k-1)rq^2$ lines, for $q \geq (r-1)(k-1)$ a prime power;
2. $S_{(r,k)}$ has multiplicity at most $2(r-1)(k-1)q^2\gcd(r,k)$, where $q$ is as before.

If $n$ is odd, that is, if both $r$ and $k$ are even, then instead of Proposition 4 we can use the graphs of girth 8 from Proposition 5 together with the result from Proposition 7 to deduce the existence of an $n$-regular graph of girth 7 with
\[2(nq^2 - q) - \frac{2(n-1)^2 - 2}{n-2}\]
vertices, so the resulting incidence graph will have
\[(r+k)\left(2(nq^2 - q) - \frac{2(n-1)^2 - 2}{n-2}\right)\]
\[= (r+k)\left(2((r-1)(k-1)q^2 - q) - \frac{2((r-1)(k-1)-1)^2 - 2}{(r-1)(k-1)-2}\right),\]
for a prime power $q \geq n = (r-1)(k-1)$.
When \( n = (r - 1)(k - 1) \) is a power of a prime Proposition 6 can be used together with Proposition 7 to improve further and then if \( n \) is odd we get an incidence graph with

\[
(r + k) \left( 2q(q^2 - 2) - \frac{2((r - 1)(k - 1) - 1)^2 - 2}{(r - 1)(k - 1) - 2} \right)
\]

vertices.

These results can now be combined with results on the distribution of primes to express the number of points and lines of the constructed configuration as a function of \( r \) and \( k \).

3.2.2. Upper bounds on the existence of triangle-free configurations based on the multiplicity of \( S_{(r,k)} \) for special parameters. When the configuration is balanced, so that \( r = k \), and if we suppose that the conjecture that all cages of even girth are bipartite is true [32], then the upper bound on the multiplicity of \( S_{(r,r)} \) is given by an upper bound on the existence of a \((r,8)\)-cage. If \( r \) is a power of a prime, then Proposition 6 implies that there exists a triangle-free \((r,r)\)-configuration with

\[
v \leq r(r^2 - 2)
\]

\[
b \leq r(r^2 - 2).
\]

If \( r \) is not a power of a prime, then Proposition 5 implies that, if \( q \) is a power of a prime such that \( 3 \leq r \leq q - 1 \), then there exists a triangle-free \((r,r)\)-configuration with

\[
v \leq rq^2 - q
\]

\[
b \leq rq^2 - q.
\]

Whenever a generalized quadrangle exists, it is the smallest existing triangle-free \((r,k)\)-configuration. Then the bound in Proposition 11 is reached:

\[
v = k((r - 1)(k - 1) + 1)
\]

and

\[
b = r((r - 1)(k - 1) + 1).
\]

For example, when \( r = k \) and \( r - 1 \) is a power of a prime, it is proved that there is a generalized quadrangle of order \((r - 1, r - 1)\), with

\[
v = b = r((r - 1)^2 + 1)
\]

(see [20] or Proposition 3 and 2).

We also repeat the results stated in Proposition 3: Let \( q \) be a power of a prime. Then there exists a generalized quadrangle of order \((r - 1, k - 1)\) if

\[
(r - 1, k - 1) \in \{(q,1), (q,q), (q,q^2), (q^2,q^3), (q-1,q+1)\}.
\]

Among small famous known configurations, the Cremona-Richmond \((15_3,15_3)\)-configuration is an example of a smallest triangle-free configuration for its parameters, so the multiplicity of \( S_{(3,3)} \) is 15.
3.2.3. **Upper bounds on the existence of triangle-free configurations based on the conductor of \( S_{(r,k)} \).** Using our construction of a second element in \( S_{(r,k)} \), coprime with the first, it is easy to construct bounds on the conductor using the following well-known result.

**Proposition 14.** Two coprime positive integers \( a, b \) generate a numerical semigroup whose conductor is \( (a - 1)(b - 1) \).

When more than two generators of the numerical semigroup are involved, then the calculation of the conductor of a numerical semigroup generated by \( n \) elements is difficult [23].

Regarding the case \( r = k = 4 \), as we saw in Section 1.2, \( 40, 60, 120 \in S_{(4,4)} \) and applying the two constructions from the proof of Theorem 2 together with the addition of the numerical semigroup it can be calculated that the numerical semigroup generated by these elements has conductor 411. More specifically:

\[
\{ \quad 40, 60, 79, 80, 81, 99, 100, 101, 118, 119, 120, 121, 122, 138, 139, \\
140, 141, 142, 157, 158, 159, 160, 161, 162, 163, 177, 178, 179, 180, \\
181, 182, 183, 196, 197, 198, 199, 200, 201, 202, 203, 204, 216, 217, \\
218, 219, 220, 221, 222, 223, 224, 235, 236, 237, 238, 239, 240, 241, \\
242, 243, 244, 245, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, \\
265, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, \\
294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 313, \\
314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, \\
333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, \\
347, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, \\
365, 366, 367, 368, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, \\
382, 383, 384, 385, 386, 387, 388, 391, 392, 393, 394, 395, 396, 397, \\
398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 411, \ldots \}
\subset S_{(4,4)},
\]
and all natural numbers larger than 411 are also contained in \( S_{(4,4)} \).

4. **Conclusion**

In this article we have proved that we can associate a subset of the natural numbers \( S_{(r,k)} \) to the triangle-free \((r,k)\)-configurations and we have then proved the following theorem.

**Theorem 4.** For every pair of integers \( r, k \geq 2 \), \( S_{(r,k)} \) is a numerical semigroup.
In particular, we have proved that for every pair of natural numbers \( r, k \geq 2 \), \( \mathcal{S}(r,k) \) contains at least one non-zero element \( m \). This integer \( m \) corresponds to a triangle-free \((v_r, b_k)\)-configuration with number of points \( v = |P| = m\frac{k}{\gcd(r,k)} \) and number of lines \( b = |\mathcal{L}| = m\frac{r}{\gcd(r,k)} \). As was proved in Proposition 13 we get the following:

**Corollary 1.** For any pair of integers \( r, k \geq 2 \) and a prime power \( q \geq (r-1)(k-1) \) there exists a triangle-free \((r,k)\)-configuration with \( 2(r-1)(k-1)kq^2 \) points and \( 2(r-1)(k-1)rq^2 \) lines.

As we saw in Section 3.2.1, for many cases there are much smaller triangle-free configurations. These results should be compared with the previous bound for the smallest balanced triangle-free \((r,r)\)-configuration given in Theorem 1, which uses the generalized Gray / LC\((r)\) configuration with \( r^2 \) points and \( r^2 \) lines. Beside the fact that this bound was of exponential size, while our bound is polynomial, our bound is more general, since we also treat unbalanced configurations.

The proof of Corollary 1 is constructive and can be used as an algorithm to construct a triangle-free \((r,k)\)-configuration. The construction can be found in Proposition 9. Further constructions are given in Lemma 2 and Proposition 10.

From Theorem 4 we can also deduce the existence of infinite families of triangle-free \((r,k)\)-configurations. These families are different from the families which can be constructed from the results presented in [14], and also in this case it should be noticed that we treat both balanced and unbalanced configurations.

**Corollary 2.** For any pair of integers \( r, k \geq 2 \) there exist infinitely many triangle-free \((r,k)\)-configurations.

A numerical semigroup has a conductor, a lowest number from which all larger integers pertain to the numerical semigroup. Using this we get

**Corollary 3.** Given a pair of integers \( r, k \geq 2 \) there exists a positive number \( N \) such that for all integers \( n \geq N \) there exists at least one configuration with parameters

\[
\left( \frac{n}{\gcd(r,k)} \right)_r, \left( \frac{n}{\gcd(r,k)} \right)_k,
\]

that is, when the number of points (and lines) is big enough, there is at least one configuration for any admissible parameters.

Using the construction of the triangle-free configuration with associated integer \( am + 1 \), coprime with \( m \) (Proposition 10), and the combination of triangle-free configurations which defines the addition of the numerical semigroup (Lemma 2), it is possible to explicitly construct triangle-free configurations with associated integers in the numerical semigroup generated by \( m \) and \( am + 1 \).

In the introduction we described briefly an application of configurations to P2P UPIR. Also we pointed out that in order to avoid collusions of two users spying on a third, configurations without triangles should be used. For further details on P2P UPIR see [9, 8, 27].

This is of course not the only application of triangle-free configurations. Configurations have been used in coding theory, for example in the construction of LDPC codes [11, 10, 19, 29], where a large girth is important. In this context a girth which is at least 8 may be considered to be large. The results on the existence and the explicit constructions of triangle-free configurations presented in this article have
therefore applications to coding theory. One should also notice that the arguments used in this article in general works for configurations with an incidence graph of girth at least \( n \in \mathbb{N} \), for \( n \geq 6 \).

Another example of an application of configurations is the deterministical key distribution scheme for distributed sensor networks described in [16, 17].

For all applications it is obviously useful to know that there are plenty of triangle-free configurations, so that it is possible to find one for any specified parameters. Finding means explicit construction, which we provide. Also, the addition in \( \mathcal{S}_{(r,k)} \) comes from combining two triangle-free configurations, so we can construct larger \((r,k)\)-configurations from smaller ones, which is very useful in many applications. We do not call it addition of configurations, since it is not well-defined. Indeed we can combine the same two configurations in many ways, by choosing different vertices in the combination process.

Future work includes a more explicit description of the numerical semigroups associated to the existence of triangle-free configurations, and also a generalization of the results presented in this article to the sets of combinatorial \((r,k)\)-configurations without \( n \)-gons.

ACKNOWLEDGMENTS

This work was partly supported by the Spanish Government through the projects TIN2009-11689 “RIPUP” and CONSOLIDER INGENIO 2010 CSD2007-00004 “ARES”, and by the Government of Catalonia under grant 2009 SGR 1135.

The authors would like to thank Marcus Greferath for the idea to use triangle-free configurations for P2P UPIR.

REFERENCES

[1] G. Araujo-Pardo, On upper bounds of odd girth cages, Discrete Math., 310 (2010), 1622–1626.
[2] C. Balbuena, A construction of small regular bipartite graphs of girth 8, Discrete Math. Theor. Comp. Sci., 11 (2009), 33–46.
[3] A. Betten, G. Brinkmann and T. Pisanski, Counting symmetric configurations \( v_3 \), Discrete Appl. Math., 99 (2000), 331–338.
[4] N. Biggs, “Algebraic Graph Theory,” 2nd edition, Cambridge University Press, Cambridge, 1993.
[5] J. G. Bokowski, “Computational Oriented Matroids,” Cambridge University Press, Cambridge, 2006.
[6] M. Bras-Amorós and K. Stokes, The semigroup of combinatorial configurations, preprint, arXiv:0907.4230v3
[7] F. De Clerck, J. A. Thas and H. Van Maldeghem, Generalized polygons and semipartial geometries, EIDMA minicourse, 1996.
[8] J. Domingo-Ferrer and M. Bras-Amorós, Peer-to-peer private information retrieval, in “Privacy in Statistical Databases,” (2008), 315–323.
[9] J. Domingo-Ferrer, M. Bras-Amorós, Q. Wu and J. Manjón, User-private information retrieval based on a peer-to-peer community, Data Knowl. Eng., 68 (2009), 1237–1252.
[10] M. Flanagan, M. Greferath and C. Roessing, An encoding scheme, and a decoding scheme using a series of LDPC codes based on finite inversive spaces, Technical Publication, 2007.
[11] M. Flanagan, M. Greferath and C. Roessing, On LDPC codes from \((0,1)\)-geometries induced by finite inversive spaces of even order, in “Workshop on Coding and Cryptography 2007, WCC '07,” Versailles, France, 2007.
[12] A. Gács and T. Héger, On geometric constructions of \((k, g)\)-graphs, Contrib. Discrete Math., 3 (2008), 63–80.
[13] H. Gropp, Configurations, in “The CRC Handbook Of Combinatorial Designs” (eds. C.J. Colbourn and J.H. Dinitz), 2nd edition, CRC Press, Boca Raton, FL, (2007), 352–355.
[14] B. Grünbaum, “Configurations of Points and Lines,” American Mathematical Society, Providence, RI, 2009.
[15] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, New upper bounds on the order of cages, Electr. J. Combin., 4 (1997), 11.
[16] J. Lee and D. R. Stinson, A combinatorial approach to key predistribution for distributed sensor networks, in “IEEE Wireless Communications and Networking Conference, CD-ROM,” paper PHYS0-06, (2005), 6.
[17] J. Lee and D. R. Stinson, On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs, ACM Trans. Inf. Syst. Secur., 11 (2008), 1–35.
[18] V. Martinetti, Sopra alcune configurazioni piane, Annali Mat. Pura Appl (1867-1897), 14 (1886), 161–192.
[19] J. M. F. Moura, J. Lu and H. Zhang, Structured LDPC codes with large girth, in “IEEE Signal Processing Magazine, Special Issue on Iterative Signal Processing for Communications,” 21 (2004), 42–55.
[20] S. E. Payne and J. A. Thas, “Finite Generalized Quadrangles,” European Math. Soc., Zürich, 2009.
[21] T. Pisanski, Yet another look at the Gray graph, New Zealand J. Math, 36 (2007), 85–92.
[22] T. Pisanski, M. Boben and D. Marušić, A. Orbanić and A. Graovac, The 10-cages and derived configurations, Discrete Math., 275 (2004), 265–276.
[23] J. L. Ramírez Alfonsín, “The Diophantine Frobenius Problem,” Oxford University Press, Oxford, 2005.
[24] J. C. Rosales and P. A. García-Sánchez, “Numerical Semigroups,” Springer, New York, 2009.
[25] H. Sachs, Regular graphs with given girth and restricted circuits, J. London Math. Soc., 38 (1963), 423–429.
[26] K. Sinha, A triangle free configuration, Časopis Pěst. Mat., 103 (1978), 147–148, 202.
[27] K. Stokes and M. Bras-Amorós, Optimal configurations for peer-to-peer user-private information retrieval, Comp. Math. Appl., 59 (2010), 1568–1577.
[28] L. Storme, Finite geometry, in “The CRC Handbook Of Combinatorial Designs” (eds. C.J. Colbourn and J.H. Dinitz), 2nd edition, CRC Press, Boca Raton, FL, (2007), 702–729.
[29] B. Vasic and O. Milenkovic, Combinatorial constructions of low-density parity-check codes for iterative decoding, IEEE Trans. Inform. Theory, 50 (2004), 1156–1176.
[30] A. Viejo and J. Castellá-Roca, Using social networks to distort users’ profiles generated by web search engines, Computer Networks, 54 (2010), 1343–1357.
[31] E. Visconti, Sulle configurazioni piane atrigone, Giornale Mat. Battaglini, 54 (1916), 27–41.
[32] P. K. Wong, Cages—a survey, J. Graph Theory, 6 (1982), 1–22.

Received April 2010; revised March 2011.
E-mail address: klara.stokes@urv.cat
E-mail address: maria.bras@urv.cat