Maria Bras-Amorós and Klara Stokes
Universitat Rovira i Virgili
Tarragona

Abstract

A (v, b, r, k) combinatorial configuration can be defined as a connected, (r, k)-biregular bipartite graph with v vertices on one side and b vertices on the other and with no cycle of length 4. Combinatorial configurations have become very important for some cryptographic applications to sensor networks and to peer-to-peer communities. Configurable tuples are those tuples (v, b, r, k) for which a (v, b, r, k) combinatorial configuration exists. It is proved in this work that the set of configurable tuples with fixed r and k has the structure of a numerical semigroup. The semigroup is completely described whenever $r = 2$ or $r = 3$. For the remaining cases some bounds are given on the multiplicity and the conductor of the numerical semigroup. This leads to some concluding results on the existence of configurable tuples.

1 Introduction

Combinatorial configurations are a particular case of so-called incidence structures which have been recently used for defining peer-to-peer communities for preserving privacy of users in front of search engines [2, 3]. Other applications of configurations related to sensor networks can be found in [12].

A (v, b, r, k)-configuration is a set of v "points" $\mathcal{P} = \{p_1, \ldots, p_v\}$ and a set of b "lines" $\mathcal{L} = \{l_1, \ldots, l_b\}$, such that there are k points on each line, through each point pass r lines and no two points are joined by more than one line. There is a natural bijection between combinatorial configurations

and connected bipartite biregular graphs with girth larger than 5. Observe that since these graphs are bipartite, the girth is always even and therefore larger than or equal to 6. In the present work we will treat configurations as such graphs.

One problem when using configurations is the limited number of known configurations, specially for large v and b. We refer the reader to [7, 6] for previously known results on the existence of combinatorial configurations.

In [3] larger configurations are constructed by combining smaller configurations; a (v, b, r, k)-configuration is obtained with parameters of the form $b = b' + b''$ and $v = v' + v''$, from existing configurations with parameters (v', b', r, k) and (v'', b'', r, k). In this article we interpret this result as giving structure to the set of parameters of existing configurations.

A numerical semigroup is a subset of $\mathbb{N}_0$ that contains 0, is closed under addition and has finite complement in $\mathbb{N}_0$.

Fix $r > 1, k > 1$. We will show that the set of all tuples (v, b, r, k) such that there exists a (v, b, r, k) configuration has the structure of a numerical semigroup. This semigroup can be explicitly described if $r = 2$ or $r = 3$. For the general case we give bounds on the multiplicity and the conductor of the numerical semigroup. The new results on the existence of configurable tuples deduced from this work are summarized in Theorem 30.

2 The semigroup of combinatorial configurations

2.1 Previous results on the existence of configurations

Definition 1 An incidence structure is a triple $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, 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.

In this article, no geometric meaning is attached to the terms point and line.

Definition 2 A (v, b, r, k)-configuration is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$, which has

- v points,
- b lines,
- r lines through any point,

- k points on any line,

and in which any two different points are incident with at most one line, or equivalently, any two different lines are incident with at most one point.

Two general references on geometric and combinatorial configurations are [7, 6].

In the following we will suppose that $v \leq b$. This can be done without loss of generality, since if $v > b$ we can take the dual configuration.

Proposition 3 *The conditions $vr = bk$ and $v \geq r(k-1)+1$ are necessary for a non-trivial configuration (v, b, r, k) to exist* [6].

For some values of r and k, more is known.

Theorem 4 *For $k = 3$ the necessary conditions of Proposition 3 are sufficient* [5].

There has not been found any example on parameters v, b, r, such that a $(v, b, r, 4)-$configuration fails to exist as long as the parameters satisfy the necessary conditions. Regarding symmetric configurations, that is, v_k-configurations, for which $r = k$ and $v = b$, it is known that for $r = k = 4$ they all exist for $v \geq 13$.

The necessary conditions are not always sufficient. One example is $k = 5$, since there is no configuration 22_5.

For symmetric configurations, existence for some parameters are listed in Table 1, also from [6] and [4]. We see there that also for small values of k and v the existence of v_k-configurations is sometimes unknown, for example it is not known whether or not there exists a 33_6-configuration.

Results on non-symmetric configurations, generalizing the symmetric configurations, are more sparse, at least for large parameters. The state of the art can be found in [7] which actually treats geometric configurations, but also covers results on combinatorial configurations.

One interesting result in our context is the next theorem by Gropp. It guarantees the existence of large configurations and, in fact, the existence of any configuration satisfying the necessary conditions with sufficiently large v (and so b). Its limitation is the restriction on the choice of the parameters r, k.

Theorem 5 *For given k and r with $r = tk$ there is a v_0 depending on k, t such that there is a (v, b, r, k)-configuration for all $v \geq v_0$ satisfying the necessary conditions from Proposition* 3.

$k=5$	21_5	$-$	23_5	24_5	25_5	26_5	27_5	28_5	29_5	30_5	31_5
6	31_6	$-$	?	?	35_6	36_6	37_6	38_6	39_6	40_6	41_6
7	$-$	$-$	45_7	?	?	48_7	49_7	50_7	51_7	52_7	53_7

Table 1: Existence of configurations v_k for $5 \leq k \leq 7$ and $d \leq 10$. v_k means configuration exists, $-$ means configuration does not exist, ? means existence is unknown. The notation v_k-configuration is used to denote a $(v, v, k, k)-$configuration.

2.2 The set of $(r, k)-$configurable tuples

Definition 6 We say that the tuple (v, b, r, k) is *configurable if a* (v, b, r, k)*-configuration exists.*

As we saw in Proposition 3, if (v, b, r, k) is configurable then $vr = bk$ and consequently there exists d such that $v = d\frac{k}{\gcd(r,k)}$ and $b = d\frac{r}{\gcd(r,k)}$. So, to each configurable tuple (v, b, r, k) we can assign an integer d. Two different configurable tuples (v, b, r, k) will have different integers d. Let us call $D_{r,k}$ the set of all possible integers d corresponding to configurable tuples (v, b, r, k). That is,

$$D_{r,k} = \left\{ d \in \mathbb{N}_0 : \left(d\frac{k}{\gcd(r,k)}, d\frac{r}{\gcd(r,k)}, r, k \right) \text{ is configurable} \right\}.$$

Our aim is to study $D_{r,k}$. We will consider the empty graph to be also a configuration and consequently $0 \in D_{r,k}$ for all pair r, k. Obviously $D_{r,k} = D_{k,r}$ and $D_{1,k} = \{0, k\}$. First we will give a complete description of $D_{2,k}$ and a complete description of $D_{3,k}$ and then we will study the general case.

2.3 The case $r = 2$

There is a natural bijection between $(v, b, 2, k)$-configurations and k-regular connected graphs with b vertices and v edges. Two vertices in the graph share an edge if and only if the corresponding nodes in the configuration share a neighbor and viceversa. The following well-known lemma is the key result for describing $D_{2,k}$. We include the proof in order to make the article more self-contained.

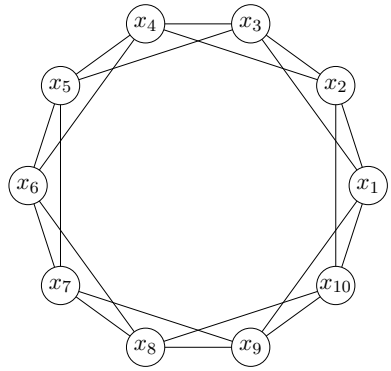

Figure 1: Construction of a connected 4-regular graph with 10 vertices

Lemma 7 *Let k be an even positive integer. A connected k-regular graph with b vertices exists if and only if $b \geq k+1$.*

Proof: By definition, any k-regular graph must have a number of vertices at least $k+1$.

Conversely, suppose $b \geq k+1$. Consider a set of vertices $x_1, \ldots, x_b$. Put an edge between x_i and x_j, with $i \leq j$, if $j - i \leq k/2$ or $i + b - j \leq k/2$. This gives a connected k-regular graph with b vertices. □

The construction in this last proof is illustrated in Figure 1.

From the natural bijection between $(v, b, 2, k)$-configurations and k-regular connected graphs with b vertices and v edges, we get the following corollary. We write $\langle a_1, \ldots, a_n \rangle$ to denote the numerical semigroup generated by $a_1, \ldots, a_n$.

Corollary 8 *If k is an even positive integer then*

$$D_{2,k} = \langle k+1, k+2, \ldots, 2k+1 \rangle .$$

Lemma 9 *Let k be an odd positive integer. A connected k-regular graph with b vertices exists if and only if b is even and $b \geq k+1$.*

Proof: By definition, any k-regular graph must have a number of vertices at least $k+1$. Now, since the number of edges is $kb/2$ this means that kb

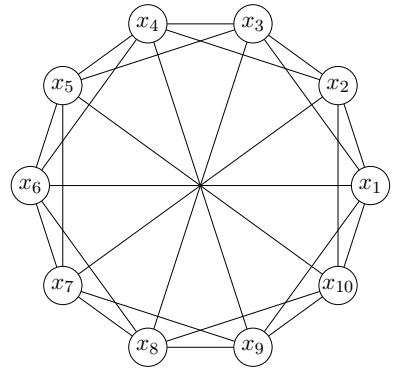

Figure 2: Construction of a connected 5-regular graph with 10 vertices

must be even and since k is odd b must be even. Conversely, suppose b is even and $b \geq k+1$. Consider a set of vertices $x_1, \ldots, x_b$. Put an edge between x_i and x_j, with $i \leq j$, if $j - i \leq (k-1)/2$ or $i + b - j \leq (k-1)/2$. Put also edges between x_i and $x_{i+b/2}$ for i from 1 to $b/2$. This gives a connected k-regular graph with b vertices. □

The construction in this last proof is illustrated in Figure 2.

From the natural bijection between $(v, b, 2, k)$-configurations and k-regular connected graphs with b vertices and v edges, we now get the following corollary.

Corollary 10 *If k is an odd positive integer then*

$$D_{2,k} = \left\langle \frac{k+1}{2}, \frac{k+1}{2} + 1, \frac{k+1}{2} + 2, \ldots, k \right\rangle.$$

2.4 The case $r = 3$

Because of Theorem 4, the case $r = 3$ is much simpler. It is stated in the next theorem.

Theorem 11 *Suppose $k > 1$ then*

$$D_{3,k} = \begin{cases} \{0, 2k+1, 2k+2, \dots\} & \text{if } k \equiv 0 \bmod 3 \\ \{0, \frac{2k+1}{3}, \frac{2k+1}{3}+1, \frac{2k+1}{3}+2, \dots\} & \text{if } k \equiv 1 \bmod 3 \\ \{0, \frac{2k+2}{3}, \frac{2k+2}{3}+1, \frac{2k+2}{3}+2, \dots\} & \text{if } k \equiv 2 \bmod 3 \end{cases}$$

Proof: By Theorem 4 (by swapping the role of b and v) we know that any tuple $(v, b, 3, k)$ with $b \neq 0$ is configurable if and only if $3v = bk$ and $b \geq k(3-1)+1 = 2k+1$. In particular, the non-zero values b for which there exists a configurable tuple $(v, b, 3, k)$ are exactly those integers $b \geq 2k+1$ such that $\frac{bk}{3}$ is an integer.

If $k \equiv 0 \bmod 3$ then the only condition is $b \geq 2k+1$ which results in

$$d = \frac{b \gcd(3,k)}{3} = \frac{3b}{3} = b \geq 2k+1$$

and this proves the result in this case.

Otherwise, we need $b \geq 2k+1$ and b be a multiple of 3. If $k \equiv 1 \bmod 3$ this is equivalent to $b \in \{2k+1, 2k+4, 2k+7, \dots\}$ and so $d = \frac{b \gcd(3,k)}{3} = \frac{b}{3}$ is in

$$\left\{ \frac{2k+1}{3}, \frac{2k+1}{3}+1, \frac{2k+1}{3}+2, \dots \right\}.$$

If $k \equiv 2 \bmod 3$ this is equivalent to $b \in \{2k+2, 2k+5, 2k+8, \dots\}$ and so $d = \frac{b \gcd(3,k)}{3} = \frac{b}{3}$ is in

$$\left\{ \frac{2k+2}{3}, \frac{2k+2}{3}+1, \frac{2k+2}{3}+2, \dots \right\}. \quad \square$$

2.5 The general case

We want to prove that $D_{r,k} \subset \mathbb{N}_0$ is a numerical semigroup. The following results on semigroups will be helpful.

Proposition 12 *A set of integers generate a numerical semigroup if and only if they are coprime.*

The proof of this proposition can be found in [13].

Proposition 12 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. This means that we need to prove that

- $0 \in D_{r,k}$,
- $D_{r,k}$ is closed under addition,
- at least two elements (and therefore all of the elements) of $D_{r,k}$ are coprime.

The two first conditions ensure that the subset $D_{r,k}$ of the natural numbers is a monoid. The operation of the monoid is addition. The last condition ensures that the monoid is a numerical semigroup. Since the case $r \leq 3$ has been proved earlier, in this section we will suppose that $r, k > 3$.

The set of configurable tuples is a submonoid of the natural numbers

We first observe that since we consider the empty configuration a configuration, $0 \in D_{r,k}$.

We will now prove that the set $D_{r,k}$ is closed under addition.

Lemma 13 *If (v, b, r, k) and (v', b', r, k) are configurable tuples, so is $(v + v', b + b', r, k)$.*

Proof: Suppose we have a (v, b, r, k)-configuration with vertices $\{x_1, \ldots, x_v\}$, $\{y_1, \ldots, y_b\}$ and a (v', b', r, k)-configuration with vertices $\{x'_1, \ldots, x'_{v'}\}$ and $\{y'_1, \ldots, y'_{b'}\}$. Consider the graph with vertices $\{x_1, \ldots, x_v\} \cup \{x'_1, \ldots, x'_{v'}\}$, $\{y_1, \ldots, y_b\} \cup \{y'_1, \ldots, y'_{b'}\}$ and all the edges in the original configurations. We can assume without loss of generality that the edges x_1y_1, x_vy_b,$x'_1y'_1$, $x'_{v'}y'_{b'}$ belong to the original configurations.

Swap the edges x_vy_b and $x'_1y'_1$ for $x_vy'_1$ and x'_1y_b. This gives a $(v+v', b+b', r, k)$ configuration [3]. An example of this construction is illustrated in Figure 3. □

Since

$$d = v \gcd(r, k)/k = b \gcd(r, k)/r$$

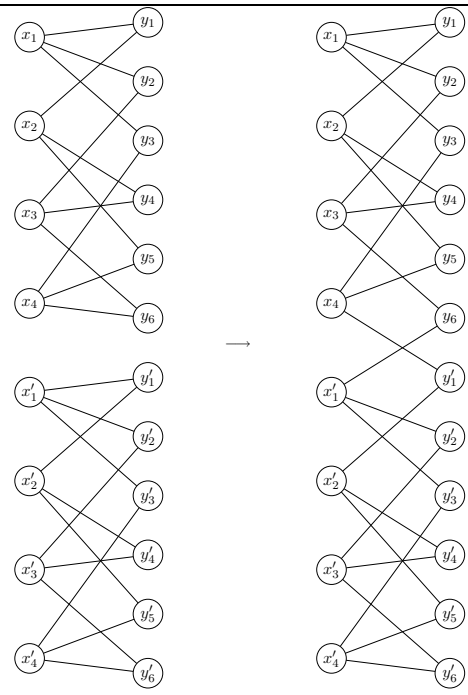

Figure 3: Construction of a $(v+v', b+b', r, k)$ configuration from a (v, b, r, k) configuration and a (v', b', r, k) configuration.

and

$$d' = v' \gcd(r,k)/k = b' \gcd(r,k)/r$$

there exists a

$$d'' = (v+v') \gcd(r,k)/k = (b+b') \gcd(r,k)/r = d + d'.$$

Hence if $d, d' \in D_{r,k}$, then $d + d' \in D_{r,k}$, or in other words $D_{r,k} \subset \mathbb{N}_0$ is closed under addition. Together with the fact that $0 \in D_{r,k}$ we get the result we were looking for.

Proposition 14 *$D_{r,k}$ is a submonoid of the natural numbers.*

The submonoid contains two coprime elements

We start by proving that given any pair of natural numbers (r, k), there exists at least one element in $D_{r,k}$. We do this by constructing a (v, b, r, k)-configuration.

For the construction we need a graph of girth at least 5. In [10] a family of small graphs of girth 5 is constructed, which can be used for our purposes. The existence of this graph is given in the following theorem.

Theorem 15 *Let $q \geq 13$ be an odd prime power and let $n \leq q + 3$. Then there exists a n regular graph with girth 5 and with $2(n-2)(q-1)$ vertices* [10, Theorem 17].

There are other constructions of small graphs for other (larger) girths, such as the ones in [1]. For our purposes taking girth at least 5 is enough.

Now we can construct the connected, r, k biregular graph of girth at least 5 which gives us the (v, b, r, k) configuration we are looking for.

Proposition 16 *For any pair of integers $r > 1, k > 1$, there exists at least one non-zero integer in $D_{r,k}$.*

Proof: The cases in which $r \leq 3$ or $k \leq 3$ have already been proved. We can therefore suppose that $r > 3$ and $k > 3$.

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 vertex set V, but edge set $E' \subset E$ with $|E'| = r + k - 1$.

The number of edges in $K_{r,k}$ outside $T_{r,k}$, that is in $E - E'$, is $n = rk - r - k + 1$. Since $r, k > 3$ we have $n \geq 3$.

From Theorem 15 we know that there exists (at least) a n-regular graph of girth (at least) 5. We take one of these graphs and call it G.

Now we will construct a bipartite $(r, k)-$biregular graph of girth at least 5, using 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 $x_A y_A$ in A, but not in T_A and one edge $x_B y_B$ in B, but not in T_B and swap them so that we instead get two edges $x_A y_B$ and $x_B y_A$. 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 $x_A y_A$ and $x_B y_B$ for every edge in G.

In this way we get a bipartite, $(r,k)-$biregular graph of girth at least 5, from a $n-$regular graph of girth at least 5, with $n = rk - r - k + 1$.

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 configuration we want to construct. If we choose the smallest connected subgraph, then we minimize the size of the smallest known (v,b,r,k)-configuration proved to exist in this manner;
- We can use the 'addition' law from Lemma 13 to connect all the connected subgraphs.

In any case we get a connected, bipartite, $(r,k)-$biregular graph of girth at least 6, hence the incidence graph of a (v,b,r,k)-configuration. □

We will now construct a second element of $D_{r,k}$, also different from 0, such that the element we already have and the new one are coprime. In order to do so we need the following lemma.

Lemma 17 *Suppose we have a (v,b,r,k)-configuration with $r \geq 3$. There exist three edges in the configuration such that the six ends are all different.*

Proof: It is easy to prove, by the property that no cycle of length 4 exists, that there exists a path with four edges with the five ends being different. Three of these ends will be in one partition of the graph while the other two will be in the other partition. Take the vertex at the end of the path. It must be one of the three in the same partition. Since its degree is at least 3, then it will have one neighbor not in the path. So, by adding the edge from the end of the path to this additional vertex, we obtain a new path with 5 edges with all its vertices being different. By taking the first, third, and fifth edges of this new path we obtain the result. □

This lemma tells us that the vertices $\{x_1,\ldots,x_v\}$, $\{y_1,\ldots,y_b\}$ in a (v,b,r,k)-configuration with $r \geq 3$ can be arranged in a way such that the edges x_1y_1, x_2y_2 and x_vy_b belong to the configuration.

We are now ready to prove the existence of two coprime elements of $D_{r,k}$.

Proposition 18 *$D_{r,k}$ contains two elements $m \neq 0$ and $sm+1$, with $s = rk/\gcd(r,k)$, so that the two are coprime.*

Proof: Because of the results in the previous sections we can assume that r and k are larger than 3. By Proposition 16 and since $D_{r,k} \subseteq \mathbb{N}_0$, there is a minimal non-zero element m in $D_{r,k}$. Let us call

$$v = mk/\gcd(r,k)$$

and

$$b = mr/\gcd(r,k).$$

Select a (v,b,r,k) configuration. Take

$$s = rk/\gcd(r,k)$$

copies of this configuration. Let us call the vertices of the ith copy

$$x_1^{(i)}, \ldots, x_v^{(i)}, y_1^{(i)}, \ldots, y_b^{(i)}.$$

By Lemma 17 we can assume that

$$x_1^{(i)}y_1^{(i)},\ x_2^{(i)}y_2^{(i)} \text{ and } x_v^{(i)}y_b^{(i)}$$

belong to the ith copy. Consider $k/\gcd(r,k)$ further vertices

$$x'_1, \ldots, x'_{k/\gcd(r,k)}$$

and $r/\gcd(r,k)$ further vertices

$$y'_1, \ldots, y'_{r/\gcd(r,k)}.$$

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 4. In the figure the edges to be removed are dashed, while the edges to add are thick lines.

- For all $2 \leq i \leq s$ replace the edges

$$x_v^{(i)}y_b^{(i)} \text{ and } x_1^{(i-1)}y_1^{(i-1)}$$

by

$$x_v^{(i)} y_1^{(i-1)} \text{ and } x_1^{(i-1)} y_b^{(i)}.$$

- Also, remove the edges $x_2^{(i)} y_2^{(i)}$ for all $2 \leq i \leq s$.
- Add the edges

$$x'_1 y_2^{(1)}, x'_1 y_2^{(2)}, \ldots, x'_1 y_2^{(r)},$$
$$x'_2 y_2^{(r+1)}, x'_2 y_2^{(r+2)}, \ldots, x'_2 y_2^{(2r)},$$
$$\vdots$$
$$x'_{k/\gcd(r,k)} y_2^{(s-r+1)}, \ldots, x'_{k/\gcd(r,k)} y_2^{(s)}$$

and

$$x_2^{(1)} y'_1, x_2^{(2)} y'_1, \ldots, x_2^{(k)} y'_1,$$
$$x_2^{(k+1)} y'_2, x_2^{(k+2)} y'_2, \ldots, x_2^{(2k)} y'_2,$$
$$\vdots$$
$$x_2^{(s-k+1)} y'_{r/\gcd(r,k)}, \ldots, x_2^{(s)} y'_{r/\gcd(r,k)}.$$

As can be verified, the construction gives a new configuration with parameters

$$\begin{aligned}(v', b', r, k) &= (sv + k/\gcd(r,k),\ sb + r/\gcd(r,k), r, k)\\ &= (smk/\gcd(r,k) + k/\gcd(r,k),\\ &\qquad smr/\gcd(r,k) + r/\gcd(r,k),\ r,\ k)\\ &= ((sm+1)k/\gcd(r,k),\ (sm+1)r/\gcd(r,k),\ r,\ k)\end{aligned}$$

and so $sm + 1 \in D_{r,k}$. □

From Proposition 18 we deduce that $D_{r,k}$ contains two coprime elements, so that they generate a numerical semigroup and this semigroup is contained in $D_{r,k}$. So the complement of $D_{r,k}$ in $\mathbb{N}_0$ is finite and $D_{r,k}$ is a numerical semigroup.

Theorem 19 *For every pair of integers $r, k \geq 2$, $D_{r,k}$ is a numerical semigroup.*

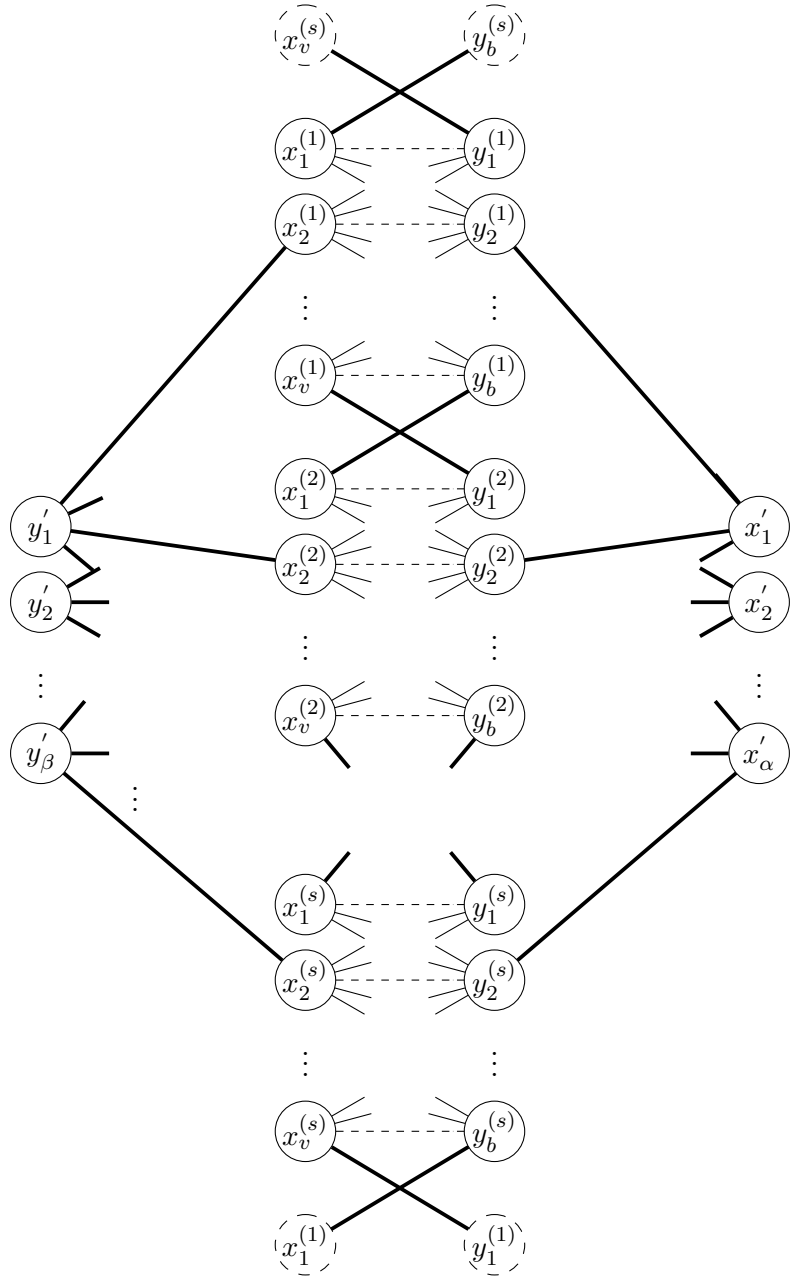

Figure 4: Construction of a $(sv + k/\gcd(r,k), sb + r/\gcd(r,k), r, k)$-configuration from s (v, b, r, k) configurations and $\alpha + \beta = k/\gcd(r,k) + r/\gcd(r,k)$ extra vertices.

We call an element of the complement of a numerical semigroup a gap. Observe that $D_{2,k}$ as well as $D_{3,k}$ for $k > 1$ are ordinary, that is, all their gaps are in a row. However, there are pairs r, k for which $D_{r,k}$ is not ordinary. For example the multiplicity of $D_{5,5}$ is 21, but 22 is a gap, as can be deduced from Table 1. Also, while the multiplicity of $D_{6,6}$ is 31, we have that $33 \notin D_{6,6}$ (see [11]).

3 Bounds on configurable tuples

3.1 A lower bound on the multiplicity of the numerical semigroup $D_{r,k}$

The multiplicity of a numerical semigroup is its smallest non-zero element. Observe that bounds on the multiplicity are bounds regarding the size of the smallest configuration for a given pair of r and k.

For the cases $r = 2$ and $r = 3$, since we know the actual structure of the semigroup we can precise the multiplicity exactly.

Proposition 20 *For $k > 1$ the multiplicity of $D_{2,k}$ is*

$$\begin{cases} k+1 & \text{if } k \text{ is even} \\ \frac{k+1}{2} & \text{if } k \text{ is odd} \end{cases}$$

For $k > 1$ the multiplicity of $D_{3,k}$ is

$$\begin{cases} 2k+1 & \text{if } k \equiv 0 \bmod 3 \\ \frac{2k+1}{3} & \text{if } k \equiv 1 \bmod 3 \\ \frac{2k+2}{3} & \text{if } k \equiv 2 \bmod 3 \end{cases}$$

The proof follows from Corollary 8, Corollary 10, and Theorem 11.

In the next lemma we give a lower bound for the multiplicity of $D_{r,k}$. It is a consequence of Proposition 3.

Lemma 21 *If $d \in D_{r,k}$ and $d \neq 0$ then $d \geq (rk - r + 1)\frac{\gcd(r,k)}{k}$ and, by symmetry, $d \geq (rk - k + 1)\frac{\gcd(r,k)}{r}$.*

For certain $r = k$, the bound is tight. An example is seen in the next proposition.

Proposition 22 *For $r = k = q + 1$ with q a power of a prime, the multiplicity of the numerical semigroup $D_{r,k}$ is $r^2 - r + 1$.*

Proof: There exists a finite projective plane for every power of a prime q. The projective plane is a $(q^2+q+1, q^2+q+1, q+1, q+1)-$configuration. We have that

$$q^2 + q + 1 = (r-1)^2 + r - 1 + 1 = r^2 - r + 1. \quad \square$$

3.2 An upper bound on the multiplicity of the numerical semigroup $D_{r,k}$

In Proposition 16 we proved that $D_{r,k}$ contains at least one element for every pair (r, k). Counting the points and lines of the configuration constructed in the proof of Proposition 16 we get an upper bound on the multiplicity of $D_{r,k}$.

The graph G from the proof of Proposition 16 has $2(n-2)(q-1)$ vertices, for an odd prime power $q \geq n-3$, $q \geq 13$ and $n = rk-r-k+1$. In the final graph, constructed from G, every vertex of G is replaced by the vertices of the $r, k-$complete graph. Therefore in the final graph, the total number of vertices is $2(n-2)(q-1)(r+k)$ and the numbers of points and lines in the corresponding configuration are $2(n-2)(q-1)r$ and $2(n-2)(q-1)k$ respectively.

A bound on the existence of a prime power

In order to get an exact bound we need a bound on the existence of the prime power q. However, we will not care about prime powers of higher exponents and instead use a famous bound on the existence of primes. The density of prime powers of exponent greater than 1 is small compared with the density of primes.

Proposition 23 *The number of squares, cubes, ... of primes up to x does not exceed*

$$x^{\frac{1}{2}} + x^{\frac{1}{3}} + x^{\frac{1}{4}} + \cdots = O(x^{\frac{1}{2}} \ln x).$$

When it comes to prime numbers, their density is described in the 'Prime number theorem'.

Theorem 24 *Prime number theorem Let $\pi(x)$ be the function counting the number of prime numbers up to x. Then we have*

$$\pi(x) \sim \frac{x}{\ln x}$$

The function $x^{\frac{1}{2}} \ln x$ grows much slower than a function containing x like the latter, so that the function counting all prime powers, including those of exponent 1, behaves asymptotically like the prime counting function. For more details on this see [9].

Therefore, when we look for a power of a prime $\geq n-3$, we are more likely to find a prime p than a power of a prime p^m, and it is enough to apply the Bertrand's Postulate in order to get a good bound.

Theorem 25 *Bertrand's Postulate*

If $m > 3$ is an integer, then there always exists at least one prime number p with $m < p < 2m-2$.

Using this, since we want our prime to be greater or equal to $n-3$, we get that there exists at least one prime number in the interval

$$[n-3, 2(n-4)-3] = [n-3, 2n-11].$$

Therefore we get the following upper bound on the multiplicity of $D_{r,k}$.

Proposition 26 *For $r, k > 3$ the multiplicity m of $D_{r,k}$ satisfies*

$$m \leq 2(rk-r-k-1)(2(rk-r-k)-10)\gcd(r,k).$$

Proof: Since $r, k > 3$, we have $n = rk-r-k+1 > 7$ and so $n-4 > 3$. Because of the construction of the configuration in Proposition 16 and Bertrand's postulate, we get the following bound on the number of points in the configuration.

$$\begin{aligned} v &= 2(n-2)(q-1)k \\ &\leq 2(n-2)(2n-11-1)k \\ &= 2(rk-r-k-1)(2(rk-r-k)-10)k \end{aligned}$$

We have

$$v = d\frac{k}{\gcd(r,k)}$$

and therefore

$$d = \frac{v\gcd(r,k)}{k}.$$

This means that in this particular configuration

$$\begin{aligned} d &= \tfrac{v\gcd(r,k)}{k} \\ &\leq 2(rk-r-k-1)(2(rk-r-k)-10)\gcd(r,k) \end{aligned}$$

If we had used the bound on the number of lines in the configuration instead, we would have arrived at the same conclusion, simply replacing k by r. □

3.3 An upper bound on the conductor of the numerical semigroup $D_{r,k}$

The largest gap of a numerical semigroup S is called the Frobenius number of S. To Proposition 12 we have associated the following result.

Proposition 27 *The numerical semigroup generated by two coprime positive integers a, b has Frobenius number $(a-1)(b-1)-1$ [15].*

Definition 28 The *conductor* of a numerical semigroup is the smallest element such that all subsequent natural numbers belong to the semigroup.

Hence if the Frobenius number is f, then $c = f + 1$. By bounding the conductor upwards, we get a value from which all subsequent integers give configurable tuples. This is equivalent to giving values v_0 and b_0 such that all tuples (v, b, r, k) with $vr = bk$, $v \geq b_0$ and $b \geq b_0$ are configurable.

As before, for the cases $r = 2$ and $r = 3$ we know exactly the conductor of $D_{r,k}$. Indeed, in these semigroups the conductor is equal to the multiplicity (see Corollary 8, Corollary 10, and Theorem 11) and the multiplicity is given in Proposition 20.

Proposition 29 *Suppose $r, k > 1$ and let $t = rk-r-k-1$. The conductor c of the numerical semigroup $D_{r,k}$ satisfies*

$$c \leq rk((4t^2-16t)^2\gcd(r,k) - 4t^2 + 16t).$$

Proof: By Proposition 26 the multiplicity of $D_{r,k}$ satisfies $m \leq 2(rk - r - k - 1)(2(rk - r - k) - 10)gcd(r,k)$. Now, because of Proposition 18, $sm + 1 \in D_{r,k}$, with $s = rk/gcd(r,k)$, and $sm + 1$ and m are coprime. Therefore Proposition 27 says that $(m-1)sm-1$ is the Frobenius element of a numerical semigroup contained in $D_{r,k}$. We have

$$(m-1)sm-1 \leq (2(rk-r-k-1)(2(rk-r-k)-10)\gcd(r,k)-1)2(rk-r-k-1)(2(rk-r-k)-10)rk-1$$

and therefore the conductor is bounded by

$$c \leq (2(rk-r-k-1)(2(rk-r-k)-10)\gcd(r,k)-1)2(rk-r-k-1)(2(rk-r-k)-10)rk.$$

With $t = rk - r - k - 1$ we get

$$c \leq (2t(2t-8)\gcd(r,k)-1)2t(2t-8)rk = rk((4t^2-16t)^2\gcd(r,k)-4t^2+16t).$$

□

	$k=4$	5	6	7	8
$r=4$	13	17/5	7	25/7	29/2
5		21	13/3	31/7	9/2
6			31	37/7	43/4
7				43	25/4
8					57

Table 2: Lower bounds for the multiplicity of the numerical semigroup $D_{r,k}$

	$k=4$	5	6	7	8
$r=4$	336	240	936	768	4560
5		2800	1008	1584	2288
6			10488	2688	7656
7				28560	5760
8					64672

Table 3: Upper bounds for the multiplicity of the numerical semigroup $D_{r,k}$

	$k=4$	5	6	7	8
$r=4$	450240	1147200	10501920	16493568	166312320
5		39186000	30451680	87761520	209306240
6			659925936	303351552	1406560320
7				5709515280	1857623040
8					33459223296

Table 4: Upper bounds for the conductor of the numerical semigroup $D_{r,k}$

3.4 Results

The upper bounds on the multiplicity and the conductor of $D_{r,k}$ are both huge, while the lower bound on the multiplicity is quite small. In Table 2, Table 3 and Table 4 one can see some examples of the values the bounds take for some r and k. We leave it as an open problem to find better bounds.

3.5 Concluding results

We are ready to collect our results in a final theorem.

Theorem 30 *For any pair of integers r, k, both larger than 1,*

(i) *there exist infinitely many configurable tuples (v, b, r, k);*

(ii) *there exists at least one configurable tuple (v, b, r, k) with*

$$v \leq 2(rk - r - k - 1)(2(rk - r - k) - 10)k$$

and

$$b \leq 2(rk - r - k - 1)(2(rk - r - k) - 10)r;$$

(iii) *all tuples (v, b, r, k) with $vr = bk$,*

- *$v \geq d_0 k / \gcd(r, k)$, and*
- *$b \geq d_0 r / \gcd(r, k)$,*

are configurable for a certain d_0;

(iv) *if $r = 2$ then*

$$d_0 = \begin{cases} k+1 & \text{if } k \text{ is even} \\ \frac{k+1}{2} & \text{if } k \text{ is odd} \end{cases}$$

if $r = 3$ then

$$d_0 = \begin{cases} 2k+1 & \text{if } k \equiv 0 \bmod 3 \\ \frac{2k+1}{3} & \text{if } k \equiv 1 \bmod 3 \\ \frac{2k+2}{3} & \text{if } k \equiv 2 \bmod 3 \end{cases}$$

(v) *if $r, k > 3$ then $d_0 \geq rk((4t^2 - 16t)^2 \gcd(r,k) - 4t^2 + 16t)$, where $t = rk - r - k - 1$.*

Proof:

(i) This is a result of the fact that for any (r, k), $D_{r,k}$ is a numerical semigroup,

(ii) This was proven in Proposition 26.

(iii) This is because a numerical semigroup has a conductor d_0, so that every element greater or equal to d_0 pertains to $D_{r,k}$.

(iv) This is a consequence of Proposition 20 and the fact that for the semigroups $D_{2,k}$ and $D_{3,k}$ the multiplicity equals the conductor.

(v) This is the bound on the conductor from Proposition 29. □

Acknowledgement

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

References

[1] G. Araujo-Pardo, C. Balbuena b and T. Héger. Finding small regular graphs of girths 6, 8 and 12 as subgraphs of cages. *Discrete Mathematics*, volume 310, pages 1301-1306, 2010.

[2] J. Domingo-Ferrer and M. Bras-Amorós. Peer-to-peer private information retrieval. In J. Domingo-Ferrer and Y. Saygin, editors, *Privacy in Statistical Databases*, volume 5262 of *Lecture Notes in Computer Science*, pages 315–323. Springer, 2008.

[3] J. Domingo-Ferrer, M. Bras-Amorós, Q. Wu, and J. Manjón. User-private information retrieval based on a peer-to-peer community. *Data and Knowledge Engineering*, 68(11):1237-1252, 2009.

[4] H. Gropp. Nonsymmetric configurations with deficiencies 1 and 2. In *Combinatorics '90 (Gaeta, 1990)*, volume 52 of *Ann. Discrete Math.*, pages 227–239. North-Holland, Amsterdam, 1992.

[5] H. Gropp. Non-symmetric configurations with natural index. *Discrete Mathematics*, 124:87–98, 1994.

[6] H. Gropp. *Handbook Of Combinatorial Designs (Charles J. Colbourn and Jeffrey H. Dinitz ed.)*, chapter Configurations, pages 353–355. Chapman and Hall/CRC, Kenneth H. Rosen, 2007.

[7] B. Grünbaum. *Configurations of Points and Lines*, volume 103 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009.

[8] M. Hall, Jr. *The theory of groups*. The Macmillan Co., New York, N.Y., 1959.

[9] G.H. Hardy. *Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work*. 1999.

[10] L. K. Jørgensen. Girth 5 graphs from relative difference sets. *Discrete Mathematics*, 293(1-3):177–184, 2005.

[11] P. R. J. Östergård. There exists no symmetric configuration with 33 points and line size 6. *Australas. J. Combin.*, 38:273–277, 2007.

[12] J. Lee and D. R. Stinson. A combinatorial approach to key predistribution for distributed sensor networks. In *Wireless Communications and Networking Conference-WCNC 2005*, volume 2, pages 1200–1205, 2005.

[13] J. C. Rosales and P. A. García-Sánchez. *Numerical semigrops*, volume 20 of *Developments in Mathematics*. Springer, New York, 2009.

[14] K. Stokes and M. Bras-Amorós. Optimal configurations for peer-to-peer private information retrieval. Computers and Mathematics with Applications, volume 59 (4), pages 1568 - 1577, 2010.

[15] J.J. Sylvester. On subvariants, i.e. semi-invariants to binary quantics of an unlimited order. *American Journal of Mathematics*, volume 5 (1-4) pages 79-136, 1882.