

# INSIDE FACTORIAL MONOIDS AND THE CALE MONOID OF A SINGLE DIOPHANTINE EQUATION

PEDRO A. GARCÍA-SÁNCHEZ, ULRICH KRAUSE, AND DAVID LLENA

**ABSTRACT.** We give a structure theorem for inside factorial domains. As an example we study the monoid of nonnegative integer solutions of equations of the form  $a_1x_1 + \cdots + a_{r-1}x_{r-1} = a_rx_r$ , with  $a_1, \dots, a_r$  positive integers. This set is isomorphic to a simplicial full affine semigroup, and thus it can be described in terms of its extremal rays and the Apéry sets with respect to the extremal rays.

## 1. INTRODUCTION

The motivation of this manuscript was essentially the extension of Elliott’s results on the sets of nonnegative integer solutions of equations of the form  $ax + by = cz$ , with  $a, b, c$  positive integers. Elliott was able to give parametric solutions to these equations for  $c$  up to 10. The set of solutions of these equations are full affine semigroups, and consequently they can be “parametrized” in terms of the Apéry sets of the extremal rays. Simplicial full affine semigroups are a particular instance of Cale monoids, which are always inside factorial. Also every full affine semigroup is isomorphic to a normal affine semigroup. The normal condition is known as root-closed in multiplicative notation.

We see that for root-closed inside factorial monoids, elements can be expressed uniquely as a linear combination of the elements in a basis plus an element in the Apéry set of this basis. Thus basis for inside factorial monoids play the same role as extremal rays in simplicial full affine semigroups. This motivates the extension of the structure theorem for simplicial full affine semigroups to inside factorial monoids. It turns out that root-closed inside factorial monoids are of the form  $G \times F$  with  $G$  a torsion Abelian group and  $F$  a free monoid, endowed with an operation that has a “carry” on the first component.

Cale monoids are a particular case of inside factorial monoids with special bases known as tame bases. For these monoids we are able to determine the class group and the inner class group. We see that the inner class group coincides with the Apéry set of the monoid with respect to a tame base, and actually the Apéry set can be endowed with an operation that makes it isomorphic to the inner class group.

Going back to the original problem of studying the monoid of nonnegative integer solutions of  $a_1x_1 + \cdots + a_{r-1}x_{r-1} = a_rx_r$ , with all  $a_i$  positive integers, we particularize the results obtained above and recover some known results for simplicial affine semigroups. For the particular case of  $r = 3$ , we see that the inner class group is cyclic, and we are able to compute it together with the class group. We discuss with some examples the uniqueness achieved by Elliott in the description of the set of solutions for the case  $r = 3$ .

---

*Date:* August 1, 2018.

*2010 Mathematics Subject Classification.* 20M14, 20M13, 11D04.

*Key words and phrases.* Cale monoid, atomic monoid, root-closed monoid, inside factorial, Diophantine equation, class group, inner class group, Hilbert basis.

The first and third authors are supported by the project MTM2017-84890-P, which is funded by Ministerio de Economía, Industria y Competitividad and Fondo Europeo de Desarrollo Regional FEDER, and by the Junta de Andalucía Grant Number FQM-343. Part of this work was done while the second author visited the Universities of Almería and Granada supported by the project MTM2014-55367-P.

## 2. INSIDE FACTORIAL MONOIDS

Let  $M$  be a cancellative and commutative monoid, and let  $Q$  be a set of nonunit elements of  $M$ . We say that  $M$  is *inside factorial with base  $Q$*  if

- for each element  $x \in M$ , there exists a positive integer  $n(x)$  and  $u$  a unit in  $M$  such that  $n(x)x \in u + \langle Q \rangle$ ,
- if  $n(x)x = u + \sum_{q \in Q} \lambda_q q = v + \sum_{q \in Q} \mu_q q$ , for some  $u, v$  units of  $M$  and  $\lambda_q, \mu_q \in \mathbb{N}$  (only a finite number of them is nonzero;  $\mathbb{N}$  stands for the set of nonnegative integers), then we have  $\lambda_q = \mu_q$  for all  $q \in Q$ .

The set  $Q$  is known as a *Cale basis* for  $M$ .

If we assume that  $M$  is unit free (reduced), then  $M$  is an inside factorial monoid with base  $Q$  if and only if for every  $x \in M$ , there exist nonnegative integers  $n(x), x(q), q \in Q$ , such that

$$n(x)x = \sum_{q \in Q} x(q)q,$$

with all  $x(q)$  equal to zero except for finitely many  $q \in Q$ , and the elements in  $Q$  are  $\mathbb{Q}$ -linearly independent.

For a cancellative monoid  $M$  we can define the divisibility relation as follows:

$$a \leq_M b \text{ if there exists } c \in M \text{ such that } a + c = b.$$

Given a reduced inside factorial monoid  $M$ , we say that  $q \in M$  is a *strong atom* if the only nontrivial divisors of multiples of  $q$  are multiples of  $q$ . That is, if for some  $n \in \mathbb{Z}^+$  and  $x \in M$  with  $x \leq_M nq$ , then  $x = mq$  for some  $m \in \mathbb{Z}^+$ . The set of all strong atoms of  $M$  is a Cale base for  $M$  (this is a consequence of [3, Lemma 3.3 (4)]).

Let  $M$  be an inside factorial monoid with base  $Q$ , we define the *Apéry set* of  $M$  with respect to  $Q$  as follows

$$\text{Ap}(M, Q) = M \setminus (Q + M).$$

**Lemma 1.** *Let  $M$  be a reduced inside factorial monoid with basis  $Q$ . Then*

$$\{x \in M \mid \lambda(q, x) < 1 \text{ for all } q \in Q\} \subseteq \text{Ap}(M, Q),$$

where for  $x, y \in M$ ,  $\lambda(x, y) = \sup\{\frac{m}{n} \mid mx \leq_M ny\}$ .

*Proof.* Assume that  $\lambda(q, x) < 1$  for all  $q \in Q$  and suppose that  $x = q + y$  for some  $y \in M$ . Then  $q \leq_M x$ , and consequently  $\lambda(q, x) \geq 1$ , a contradiction. Thus,  $x \in \text{Ap}(M, Q)$ .  $\square$

Let  $M$  be a cancellative monoid. Then  $M$  can be embedded naturally in its quotient group  $G(M)$ . We say that  $M$  is *root closed* if whenever  $nz \in M$  for some positive integer  $n$  and some  $z \in G(M)$ , then  $z \in M$ .

We see next that if we add the root-closed condition to Lemma 1, then we get an equality. Clearly (as was already used in Lemma 1), if  $q \leq_M x$ , then  $\lambda(q, x) \geq 1$ . The converse holds under the root-closed condition.

**Lemma 2.** *Let  $M$  be a reduced root-closed inside factorial monoid with base  $Q$ . For  $x \in M$  and  $q \in Q$ ,  $\lambda(q, x) \geq 1$  if and only if  $q \leq_M x$ .*

*Proof.* By hypothesis, there exists two positive integers  $m$  and  $n$  such that  $mq \leq_M nx$ , with  $m \geq n$ . Then  $nq \leq_M mq \leq_M nx$ , which yields  $nx - nq \in M$ . Hence  $n(x - q) \in M$  and as  $M$  is root closed,  $x - q \in M$ , equivalently,  $q \leq_M x$ .

Now assume that  $q \leq_M x$ . Then  $\lambda(q, x) \geq \frac{1}{1} = 1$ .  $\square$

**Lemma 3.** *Let  $M$  be a reduced and root-closed inside factorial monoid with basis  $Q$ . Then*

$$\text{Ap}(M, Q) = \{x \in M \mid \lambda(q, x) < 1 \text{ for all } q \in Q\}.$$

*Proof.* Let  $x \in \text{Ap}(M, Q)$ . Then  $x \notin q + M$  for all  $q \in Q$ . Assume that  $\lambda(q, x) \geq 1$  for some  $q \in Q$ . By Lemma 2,  $x - q \in M$ . But this means that  $x \in q + M$ , contradicting that  $x \in \text{Ap}(M, Q)$ .

The other inclusion was shown in Lemma 1.  $\square$

Given  $x \in M$ , we can define

$$\nu(x) = \sup\{\lambda(q, x) \mid q \in Q\}.$$

Notice that the above supremum in our case is a maximum, since for every  $x$  only for finitely many  $q$ ,  $\lambda(q, x)$  will be nonzero (by [2, Lemma 2 (a)],  $\lambda(q, x) = n(x)/x(q)$ ).

Lemma 3 can be restated as follows in terms of  $\nu$ .

**Corollary 1.** *Let  $M$  be a reduced and root-closed inside factorial monoid with basis  $Q$ . Then*

$$\text{Ap}(M, Q) = \nu^{-1}([0, 1]).$$

With this machinery we can decompose  $M$  in terms of  $\text{Ap}(M, Q)$  and  $F = \langle Q \rangle$ . With this decomposition, every element in  $M$  can be expressed uniquely as  $a + \sum_{q \in Q} \lambda_q q$ , with  $a \in \text{Ap}(M, Q)$ . Something similar occurs for simplicial Cohen-Macaulay affine semigroups, if we choose  $Q$  to be the extremal rays of the semigroup, [9, Theorem 1.5]. In contrast, our monoids do not have to be finitely generated. In the finitely generated case, root-closed forces the Cohen-Macaulay property [7], so it is not surprising that both families of monoids share this decomposition.

**Theorem 1.** *Let  $M$  be a reduced root-closed inside factorial monoid with base  $Q$ . Then*

$$M = \dot{\bigcup}_{a \in \text{Ap}(M, Q)} a + \langle Q \rangle.$$

*Proof.* Let  $x \in M$ . Then  $n(x)x = \sum_{q \in Q} x(q)q$ . If  $\lambda(q, x) < 1$  for all  $q \in Q$ , using Lemma 1 we have  $x \in \text{Ap}(M, Q)$ , and we are done.

If  $\lambda(q, x) \geq 1$  for some  $q$ , then for all  $(m, n)$  such that  $mq \leq_M nx$ , we have that  $m \geq n$ . Also  $q \leq_M x$  by Lemma 2. Thus, the map  $(m, n) \mapsto (m - n, n)$  is a bijection between the sets  $\{(m, n) \mid mq \leq_M nx\}$  and  $\{(m, n) \mid mq \leq_M n(x - q)\}$ . This implies that  $\lambda(q, x - q) = \lambda(q, x) - 1$ . If  $\lambda(q, x - q) \geq 1$ , then we repeat the argument and subtract  $q$  to  $x - q$ . In this way we obtain a chain of strictly decreasing nonnegative real numbers, which at some point will reach an element in the interval  $[0, 1)$ . Thus, there exists  $k \in \mathbb{N}$  such that  $x - kq \in M$  and  $x - (k + 1)q \notin M$ . Set  $y = x - kq$ , then  $x = kq + y$ , with  $y - q \notin M$ , or equivalently  $\lambda(q, y) < 1$ . We easily deduce that  $k = \lfloor \lambda(q, x) \rfloor$ , as  $1 > \lambda(q, y) = \lambda(q, x - kq) = \lambda(x, q) - k > 0$ .

By [2, Lemma 2 (a)],  $\lambda(q, x) = x(q)/n(x)$ . Hence there are only finitely many  $q \in Q$  such that  $\lambda(q, x) \neq 0$ . This lemma also states that for every  $q' \in Q$ ,  $\lambda(q', x) = \lambda(q', kq + y) = k\lambda(q', q) + \lambda(q', y)$ . As a consequence of the definition of inside factorial monoid and [2, Lemma 2], one gets that for  $q \neq q'$ ,  $q(q') = 0 = q'(q)$  and thus  $\lambda(q, q') = 0$ . It follows that  $\lambda(q', y) \neq 0$  only for finitely many  $q' \in Q$ . By repeating the argument with  $y$ , we end up writing  $x$  in the form  $x = \sum_{q \in Q} \lfloor \lambda(x, q) \rfloor q + w$ , with  $w \in \text{Ap}(M, Q)$  (notice that  $\lfloor \lambda(x, q) \rfloor$  are all zero except a finite number of them).  $\square$

Compare also the decomposition in Theorem 1 with the Stanley decomposition described in [8, Section 4.6]. This decomposition can also be stated in terms of the group spanned by the monoid, as the following corollary shows.

**Corollary 2.** *Let  $M$  be a reduced root-closed inside factorial monoid with base  $Q$ . Then*

$$\text{G}(M) = \dot{\bigcup}_{a \in \text{Ap}(M, Q)} a + \text{G}(Q).$$

*Moreover,  $a + f \in M$  with  $a \in \text{Ap}(M, Q)$  and  $f \in \text{G}(Q)$  if and only if  $f \in \langle Q \rangle$ .*

*Proof.* Let  $z \in \text{G}(M)$ . Then  $z = u - v$  for some  $u, v \in M$ . By Theorem 1, there exist  $a, b \in \text{Ap}(M, Q)$  and  $f, g \in \langle Q \rangle$  such that  $u = a + f$  and  $v = b + g$ . Thus  $z = (a - b) + (f - g)$ . But  $-b = (n(b) - 1)b - \sum b(q)q$ . Hence  $z = (a + (n(b) - 1)b) + (f - g - \sum b(q)q)$ . Observe

that  $a + (n(b) - 1)b \in M$ , and consequently there exists  $c \in \text{Ap}(M, Q)$  and  $h \in \langle Q \rangle$  such that  $a + (n(b) - 1)b = c + h$  (Theorem 1). It follows that  $z = c + (f - g + h - \sum b(q)q) \in c + G(Q)$ . This proves one inclusion, and the other is trivial.

Now assume that  $a \in \text{Ap}(M, Q)$  and  $f \in G(Q)$  are such that  $a + f \in M$ . Then by Theorem 1, there exists  $b \in \text{Ap}(M, Q)$  and  $g \in \langle Q \rangle$  such that  $a + f = b + g$ . Write  $f = f' - f''$  with  $f', f'' \in \langle Q \rangle$ . Then  $a + f' = b + (g + f'')$ , and by Theorem 1 this implies that  $a = b$  and  $f' = g + f''$ . In particular,  $f = f' - f'' = g \in \langle Q \rangle$ .  $\square$

**Corollary 3.** *Let  $M$  be a reduced root-closed inside factorial monoid with base  $Q$ . Assume that  $M$  has beside the strong atoms in  $Q$  two more atoms, say  $u$  and  $v$ . Then each  $x \in M$  has a unique parametrized representation*

$$x = \sum_{q \in Q} \lambda_q q + mu + nv,$$

with  $\lambda_q \in \mathbb{N}$  and parameters  $m, n \in \mathbb{N}$  restricted by

$$m\lambda(q, u) + n\lambda(q, v) < 1,$$

for all  $q \in Q$ .

*Proof.* From Theorem 1, we have that  $x$  has a unique representation  $x = \sum_{q \in Q} \lambda_q q + y$ , with  $y \in \text{Ap}(M, Q)$ .

First, we show that  $y = mu + nv$ , where  $m, n \in \mathbb{N}$  are uniquely determined. That  $y$  is written in this way follows from the fact that the only atoms that are not in  $Q$  are  $u$  and  $v$ . For uniqueness, suppose that  $mu + nv = m'u + n'v$  for some  $m', n' \in \mathbb{N}$ . Assume without loss of generality that  $m \geq m'$ . Therefore  $(m - m')u = (n' - n)v$ . If  $m - m' \geq n' - n$ , then  $((m - m') - (n' - n))u = (n' - n)(v - u) \in M$ . But  $M$  is root-closed, and consequently  $v - u \in M$ , contradicting that  $u$  and  $v$  are atoms. If  $n' - n \geq m - m'$ , we argue in the same way.

By Lemma 3,  $\lambda(q, y) < 1$ , and we already know that  $\lambda$  is additive on the second argument. Thus  $m\lambda(q, u) + n\lambda(q, v) < 1$ .  $\square$

On  $\text{Ap}(M, Q)$  we can define the following binary operation. For  $a, b \in \text{Ap}(M, Q)$ ,  $a + b = c + f$ , with  $c \in \text{Ap}(M, Q)$  and  $f \in \langle Q \rangle$  ( $c$  and  $f$  are unique; Theorem 1). Since  $f$  is unique we will denote it by  $I(a, b)$  (following [10]). We set  $a \oplus b = c$ . The same construction can be performed when  $M$  is a Cohen-Macaulay simplicial affine semigroup, [10, Proposition 4].

Thus, with the above notation

$$a + b = a \oplus b + I(a, b).$$

Let  $a \in \text{Ap}(M, Q)$  and let  $n$  be a nonnegative integer. We denote  $\overline{n}a$  as the unique element in  $\text{Ap}(M, Q)$  such that  $na \in \overline{n}a + \langle Q \rangle$ . The existence of such element is once more guaranteed by Theorem 1. Observe that

$$na = \overline{n}a + \sum_{i=1}^{n-1} I(a, \overline{i}a),$$

and that  $\overline{n}a = a \oplus \cdots \oplus a$ . This notation is motivated by the fact that  $\oplus$  is just  $+$  modulo  $\langle Q \rangle$ .

Also notice that the inverse of  $a$  with respect to  $\oplus$  is  $(n(a) - 1)a$ , since from the definition of Cale monoid  $n(a)a \in \langle Q \rangle$ .

Let us see some of the basic properties  $I$  has. They are very similar to those for the case of Cohen-Macaulay simplicial affine semigroups [10]; and those were abstracted from the concept of Tamura's  $\mathcal{N}$ -semigroups [12].

**Proposition 1.** *Let  $M$  be a reduced root-closed with Cale basis  $Q$ , and let  $I$  be defined as above.*

- (1) For all  $a, b \in \text{Ap}(M, Q)$ ,  $I(a, b) = I(b, a)$ .
- (2) For all  $a \in \text{Ap}(M, Q)$ ,  $I(a, 0) = 0$ .
- (3) For every  $a, b, c \in \text{Ap}(M, Q)$ ,  $I(a, b) + I(a \oplus b, c) = I(b, c) + I(a, b \oplus c)$ .

- (4) If  $a, b \in \text{Ap}(M, Q)$ ,  $a \neq 0$  and  $a \oplus b = 0$ , then  $I(a, b) \notin Q \cup \{0\}$ .  
(5) For all  $a \in \text{Ap}(M, Q) \setminus \{0\}$ ,  $\sum_{i=1}^{n(a)-1} I(a, \overline{ia}) \neq n(a)f$  for any  $f \in \langle Q \rangle$ .  
(6) For every positive integer  $n$ , every  $a \in \text{Ap}(M, Q)$  and every  $f \in G(Q)$ ,  $\sum_{i=1}^{n-1} I(a, \overline{ia}) + nf \in \langle Q \rangle$  implies  $f \in \langle Q \rangle$ .

*Proof.* The first and second assertions follow easily from the definition. The third reflects the fact that  $\oplus$  is associative.

$$a + (b + c) = a + (b \oplus c + I(b, c)) = a \oplus (b \oplus c) + I(a, b \oplus c) + I(b, c)$$

and

$$(a + b) + c = (a \oplus b + I(a, b)) + c = (a \oplus b) \oplus c + I(a \oplus b, c) + I(a, b).$$

By Theorem 1,  $a \oplus (b \oplus c) = (a \oplus b) \oplus c$  and  $I(a, b \oplus c) + I(b, c) = I(a \oplus b, c) + I(a, b)$ .

Now assume that  $a \oplus b = 0$  for some  $a, b \in \text{Ap}(M, Q)$ . This implies that  $a + b = I(a, b)$ . If  $I(a, b) = 0$ , then  $a + b = 0$ , and as  $M$  is reduced, we obtain  $a = b = 0$ , a contradiction. If  $I(a, b) = q' \in Q$ , then  $q' = a + b$ . We have  $n(a)n(b)q' = n(a)n(b)(a + b) = \sum_{q \in Q} (n(a)b(q) + n(b)a(q))q$  thus  $a(q) = 0 = b(q)$  for all  $q \in Q \setminus \{q'\}$ , and  $n(a)n(b) = n(a)b(q') + n(b)a(q')$ .

Recall that  $\lambda(q', a) = n(a)/a(q') < 1$  and  $\lambda(q', b) = n(b)/b(q') < 1$  since  $a, b \in \text{Ap}(M, Q)$  (Lemma 3). Hence  $n(a)n(b) > 2n(a)n(b)$ , a contradiction. This proves the fourth assertion.

Let  $a \in \text{Ap}(M, Q)$ . Assume that there exists  $f \in \langle Q \rangle$  such that  $n(a)f = \sum_{i=1}^{n(a)-1} I(a, \overline{ia})$ . As  $\overline{n(a)a} = 0$ ,  $n(a)a = \sum_{i=1}^{n(a)-1} I(a, \overline{ia}) = n(a)f$ . Hence  $a = f$ , as  $M$  is root closed. This can only be the case if  $a = 0 = f$ . The fifth assertion now follows easily.

Finally, suppose that we have  $n, a, f$  under the hypothesis of the last statement. Then  $a + f \in G(M)$ , and  $n(a + f) = na + nf = \overline{na} + \sum_{i=1}^{n-1} I(a, \overline{ia}) + nf \in M$ . As  $M$  is root closed,  $a + f \in M$ , which means that  $f \in \langle Q \rangle$  (Corollary 2).  $\square$

This inspires the following structure theorem for reduced inside factorial monoids.

**Theorem 2.** *Let  $G$  be a torsion Abelian group and let  $F$  be the free monoid on a set  $Q$ . Let  $I$  be a map  $I : G \times G \rightarrow F$  fulfilling the following conditions:*

- (1) for all  $a, b \in G$ ,  $I(a, b) = I(b, a)$ ,
- (2) for all  $a \in G$ ,  $I(a, 0) = 0$ ,
- (3) for every  $a, b, c \in G$ ,  $I(a, b) + I(a + b, c) = I(b, c) + I(a, b + c)$ ,
- (4) if  $a \in G \setminus \{0\}$ , then  $I(a, -a) \notin Q \cup \{0\}$ .

*On  $G \times F$  define the operation  $(a, f) +_I (b, g) = (a + b, f + g + I(a, b))$ . Then  $G \times F$  with this binary operation is a reduced inside factorial monoid with basis  $\{0\} \times Q$ . Moreover, all elements in  $\{0\} \times Q$  are irreducible, and  $\text{Ap}(G \times F, \{0\} \times Q) = G \times \{0\}$ .*

*If in addition,*

- (5) for every positive integer  $n$ , every  $a \in G$  and every  $f \in G(F)$ ,  $\sum_{i=1}^{n-1} I(a, ia) + nf \in F$  implies  $f \in F$ ,

*then  $G \times F$  is root-closed.*

*Proof.* The first three assertions are telling us that  $G \times F$  with this binary operation is a monoid with identity element  $(0, 0)$ .

Assume that  $(a, f) +_I (c, h) = (b, g) +_I (c, h)$ . Then  $a + c = b + c$  and  $f + h + I(a, c) = g + h + I(b, c)$ . As  $G$  is a group, we get  $a = b$ , and thus  $f + h + I(a, c) = g + h + I(a, c)$ . Now, by using that  $F$  is a free monoid, we deduce that  $f = g$ . Thus,  $G \times F$  is cancellative.

Let us see now that  $G \times F$  is reduced. If  $(a, f) +_I (b, g) = (0, 0)$ , then  $b = -a$  and  $f + g + I(a, b) = 0$ . But  $F$  is free, whence  $f = g = I(a, -a) = 0$ . Property (4) of  $I$  ensures that  $a = 0$ . Hence  $(a, f) = (0, 0) = (b, g)$ .

Now take any  $(a, f) \in G \times F$ . Then  $\text{ord}(a)(a, f) = (0, \text{ord}(a)f + \sum_{i=1}^{\text{ord}(a)-1} I(a, ia)) \in \{0\} \times Q$ . If  $(0, \sum_{q \in Q} \lambda_q q) = (0, \sum_{q \in Q} \mu_q q)$  with  $\lambda_q, \mu_q \in \mathbb{N}$  and all zero except finitely many of them, then

as  $F$  is free over  $Q$ , this implies that  $\lambda_q = \mu_q$  for all  $q \in Q$ . This proves that  $G \times F$  is an inside factorial monoid with basis  $Q$ .

Let  $(a, f), (b, g) \in G \times F$  such that  $(a, f) +_I (b, g) = (0, q)$  with  $q \in Q$ . Then  $a + b = 0$  and  $f + g + I(a, b) = q$ . By (4),  $I(a, b) \neq q$ , and as  $F$  is free over  $Q$ , this implies that  $I(a, b) = 0$  and that either  $f = 0$  and  $g = q$ , or  $f = q$  and  $g = 0$ . In any case, by (4) again,  $a = 0 = b$ , and  $(0, q)$  is an atom.

Now let  $(a, 0) \in G \times \{0\}$ . If  $(a, 0) = (0, q) +_I (b, f)$  for some  $(0, q) \in \{0\} \times Q$  and  $(b, f) \in G \times F$ , then  $a = b$  and  $0 = q + f$ , which is impossible. Thus,  $G \times \{0\} \subseteq \text{Ap}(G \times F, \{0\} \times Q)$ . For the other inclusion, let  $(a, f) \in \text{Ap}(G \times F, \{0\} \times Q)$ . If  $f \neq 0$ , then  $f - q \in F$  for some  $q \in Q$ . Hence  $(a, f) = (0, q) +_I (a, f - q) \in G \times F$ , contradicting that  $(a, f) \in \text{Ap}(G \times F, \{0\} \times Q)$ .

Finally assume that (5) holds. We first show that  $\text{G}(G \times F) = G \times \text{G}(F)$  with the operation  $(a, f) +_I (b, g) = (a + b, f + g + I(a, b))$ . The inverse of  $(a, f)$  is  $(-a, -f - I(a, -a))$ . If  $(a, f) \in G \times \text{G}(F)$ , then  $f = g - h$  for some  $g, h \in F$ , and  $(a, f) = (a, g) +_I (-h, h)$ . Hence  $(a, f) \in \text{G}(G \times F)$ . For the other inclusion, take  $(a, f) \in \text{G}(G \times F)$ . Then  $(a, f) = (b, g) +_I (-c, h)$  for some  $(b, g), (c, h) \in G \times F$ , that is,  $a + c = b$  and  $g = f + h + I(a, c)$ . Consequently  $(a, f) = (a, g - h - I(a, c)) \in G \times \text{G}(F)$ .

If for some positive integer  $n$  and some  $(a, f) \in G \times \text{G}(F)$  we have  $n(a, f) \in G \times F$ , then  $(na, nf + \sum_{i=1}^{n-1} I(a, ia)) \in G \times F$ . In particular, this implies that  $nf + \sum_{i=1}^{n-1} I(a, ia) \in \text{G}(F)$ , and by (5), this yields  $f \in F$ . Thus,  $(a, f) \in G \times F$ , and  $G \times F$  is root-closed.  $\square$

### 3. THE INNER CLASS GROUP OF A CALE MONOID

Let  $M$  be a reduced inside factorial monoid with Cale base  $Q$ . We say that  $Q$  is a *tame base* if for every  $q \in Q$ , there exists a positive integer  $\ell(q)$  such that  $\ell(q)\lambda(q, x) \in \mathbb{N}$  for all  $x \in M$  (see [3]; we take  $\ell(q)$  to be the least positive integer fulfilling this condition). We say that  $M$  is a *Cale monoid* if it is inside factorial with a tame base.

By [2, Lemma 2 (b)] (and with our additive notation), we know that  $\lambda(q, x+y) = \lambda(q, x) + \lambda(q, y)$  for all  $x, y \in M$ . For each  $q \in Q$ , the map  $f_q(x) = \ell(q)\lambda(q, x)$  defines a monoid morphism of  $M$  into  $(\mathbb{N}, +)$ . Recall that by [3, Lemma 2.1 (i)],  $f_q(x) = \ell(q)x(q)/n(x)$ .

Let  $\varphi : M \rightarrow \mathbb{N}^{(Q)}$  defined as  $\varphi(x)(q) = f_q(x)$ . Then  $\varphi$  is injective. If  $x, y \in M$  are such that  $f_q(x) = f_q(y)$  for all  $q \in Q$ , then  $x(q)/n(x) = y(q)/n(y)$  for all  $q \in Q$ . Hence  $x = \sum_{q \in Q} \frac{x(q)}{n(x)} q = \sum_{q \in Q} \frac{y(q)}{n(y)} q = y$ .

Let  $\text{G}(M)$  be the quotient group of  $M$ . Then  $\varphi$  extends to the group morphism  $\varphi : \text{G}(M) \rightarrow \mathbb{Z}^{(Q)}$ , by defining  $\varphi(a - b) = \varphi(a) - \varphi(b)$ .

For a cancellative monoid  $S$  and a submonoid  $T$  of  $S$ , we can define the following binary relation:  $a \sim_T b$ ,  $a, b \in S$  if  $b - a \in \text{G}(T)$ . This relation is a congruence, and thus  $S / \sim_T$ , denoted as  $S/T$ , is a monoid, called the quotient of  $S$  modulo  $T$ . It follows that  $S/T$  is isomorphic to  $\text{G}(S)/\text{G}(T)$ .

The quotient  $\text{Cl}(M) = \mathbb{N}^{(Q)}/\varphi(M)$  is the (*outer*) *class group* of  $M$ . The *inner class group* of  $M$  is defined as  $\text{inCl}(M) = \varphi(M)/\varphi(F)$ , with  $F = \langle Q \rangle$ .

Hence,

$$\text{Cl}(M) = \frac{\mathbb{Z}^{(Q)}}{\varphi(\text{G}(M))}, \quad \text{inCl}(M) = \frac{\varphi(\text{G}(M))}{\varphi(\text{G}(F))} \cong \frac{M}{F}.$$

Thus, by the third isomorphism theorem,

$$(1) \quad \text{Cl}(M) = \frac{\mathbb{Z}^{(Q)}/\varphi(\text{G}(F))}{\text{inCl}(M)}.$$

From  $\varphi(q) = \ell(q)\mathbf{e}_q$ , for  $q \in Q$  (where  $\mathbf{e}_q$  is the function that maps everything to 0 except  $q$  which is sent to 1), one obtains

$$(2) \quad \frac{\mathbb{Z}^{(Q)}}{\varphi(\text{G}(F))} = \bigoplus_{q \in Q} \mathbb{Z}_{\ell(q)}.$$

As a consequence of this we obtain the following corollary.

**Corollary 4.** *Let  $M$  be a reduced root-closed Cale monoid with (finite) Cale basis  $Q$ . Then*

$$\prod_{q \in Q} \ell(q) = |\text{Cl}(M)| \cdot |\text{inCl}(M)|.$$

From Theorem 1, we obtain another interesting consequence.

**Corollary 5.** *Let  $M$  be a reduced root-closed Cale monoid with Cale basis  $Q$ . Then*

$$\text{inCl}(M) \cong (\text{Ap}(M, Q), \oplus)$$

Also Theorem 1 and the last corollary offer a new way to see  $M$ . We can define on the cartesian product  $\text{Ap}(M, Q) \times F$  the following binary operation:  $(a, f) + (b, g) = (a \oplus b, f + g + \text{I}(a, b))$ . With this operation  $\text{Ap}(M, Q) \times F$  is a monoid isomorphic to  $M$ .

**Theorem 3.** *Let  $M$  be a reduced root-closed Cale monoid with basis  $Q$ . Then  $M$  is isomorphic to  $\text{Ap}(M, Q) \times \langle Q \rangle$  endowed with the operation  $(a, f) + (b, g) = (a \oplus b, f + g + \text{I}(a, b))$ .*

*Remark 1.* Let  $q \in Q$  and  $x \in M$ . Then by Theorem 1, there exist unique  $a \in \text{Ap}(M, Q)$  and  $f \in \langle Q \rangle$  such that  $x = a + f$ . We know that  $\lambda$  is additive in the second argument, and so  $\lambda(q, x) = \lambda(q, a) + \lambda(q, f)$ . It also follows that  $\lambda(q, f) \in \mathbb{N}$  (it is actually  $f(q)$ ), and by Lemma 3,  $\lambda(q, a) < 1$ . Thus if we want to compute  $\ell(q)$  we only have to deal with  $\lambda(q, a)$  for all  $a \in \text{Ap}(M, Q)$ . As a consequence of Corollary 5, we only have to look for least integer  $k$  such  $k\lambda(q, a) \in \mathbb{N}$  for all  $a$  in a minimal generating set of  $(\text{Ap}(M, Q), \oplus)$ . This integer will be  $\ell(q)$ .

#### 4. THE EQUATION

Let  $a_1, \dots, a_r$  be positive integers. Let  $N = \{(x_1, \dots, x_r) \in \mathbb{N}^r \mid a_1x_1 + \dots + a_{r-1}x_{r-1} = a_rx_r\}$ . In light of [3, Proposition 5.6],  $N$  is a Cale monoid.

Instead of considering  $N = \{x \in \mathbb{N}^r \mid a_1x_1 + \dots + a_{r-1}x_{r-1} = a_rx_r\}$ , we will consider  $M = \{x \in \mathbb{N}^{r-1} \mid a_1x_1 + \dots + a_{r-1}x_{r-1} \equiv 0 \pmod{a_r}\}$ , which as we see next is isomorphic to  $N$ . With this rephrasing we can apply the results in [11].

**Lemma 4.** *The semigroups  $N$  and  $M$  are isomorphic.*

*Proof.* Let  $\pi : N \rightarrow M$  be projection on the first  $r - 1$  coordinates. Clearly  $\pi$  is a monoid epimorphism. If  $\pi(x) = \pi(x')$ , with  $x, x' \in N$ , we get  $a_rx_r = a_1x_1 + \dots + a_{r-1}x_{r-1} = a_1x'_1 + \dots + a_{r-1}x'_{r-1} = a_rx'_r$ . Hence  $a_rx_r = a_rx'_r$  and consequently  $x_r = x'_r$ . Thus  $\pi$  is a monoid isomorphism.  $\square$

The inverse of  $\pi$  is  $\pi^{-1}(x_1, \dots, x_{r-1}) = \left(x_1, \dots, x_{r-1}, \frac{1}{a_r} \sum_{i=1}^{r-1} x_i\right)$ .

One of the side effects of this lemma is that  $M$  is simplicial, with extremal rays  $\{q_1, \dots, q_{r-1}\}$ , with  $q_i = \frac{a_r}{\gcd(a_i, a_r)} \mathbf{e}_i$  for all  $i \in \{1, \dots, r - 1\}$  (in this context,  $\mathbf{e}_i$  denotes the  $i$ th row of the  $(r - 1) \times (r - 1)$  identity matrix).

Now [7] can be used in combination with [9]. It also follows easily that  $M$  is a Cale monoid with basis  $Q = \{q_1, \dots, q_{r-1}\}$ . This has also another advantage. We may consider now the  $a_i$  modulo  $a_r$ .

The monoid  $M$  is a full affine semigroup, and it is generated by the set of minimal nonzero elements in  $M$  with respect to the usual partial ordering in  $\mathbb{N}^{r-1}$ . This set is known in the literature as a *Hilbert basis* of  $M$ .

The following result implicitly appears in [11, Theorem 10].

**Lemma 5.** *Under the standing hypothesis,*

$$\text{Ap}(M, Q) = M \cap \prod_{i=1}^{r-1} [0, a_r / \gcd(a_i, a_r)].$$

*Proof.* Let  $x \in \text{Ap}(M, Q)$ , and assume that for some  $i$ ,  $x_i \geq a_r / \gcd(a_i, a_r)$ . Then  $x - q_i \in \mathbb{N}^{r-1}$ , but this means that  $x - q_i \in M$ , contradicting that  $x \in \text{Ap}(M, q_i)$ .

The other inclusion is clear, since for every  $x \in M$  with  $x_i < a_r / \gcd(a_i, a_r)$  for all  $i$  one cannot have  $x - q_i \in M$ .  $\square$

As a consequence of the above lemma and Theorem 1, we obtain the following consequence.

**Corollary 6.** *Let  $a_1, \dots, a_r$  be positive integers, with  $r > 2$ . Let  $M$  be the set of nonnegative integer solutions of  $a_1x_1 + \dots + a_{r-1}x_{r-1} \equiv 0 \pmod{a_r}$ . Set  $F = \langle \frac{a_r}{\gcd(a_1, a_r)}\mathbf{e}_1, \dots, \frac{a_r}{\gcd(a_{r-1}, a_r)}\mathbf{e}_{r-1} \rangle$ , and let  $A = \text{Ap}(M, Q)$ . Then*

$$M = \bigcup_{a \in A} a + F,$$

and this union is disjoint.

**Corollary 7.** *Let  $a_1, \dots, a_r$  be positive integers, with  $r > 2$ . Let  $M$  be the set of nonnegative integer solutions of  $a_1x_1 + \dots + a_{r-1}x_{r-1} \equiv 0 \pmod{a_r}$ . Assume that the Hilbert basis of  $M$  is of the form  $\{\frac{a_r}{\gcd(a_1, a_r)}\mathbf{e}_1, \dots, \frac{a_r}{\gcd(a_{r-1}, a_r)}\mathbf{e}_{r-1}, u, v\}$ , for some  $u, v$ . Then each  $x \in M$  has a unique parametrized representation*

$$x = \sum_{i=1}^{r-1} \lambda_i \frac{a_r}{\gcd(a_i, a_r)} \mathbf{e}_i + mu + nv,$$

with  $\lambda_i \in \mathbb{N}$  and parameters  $m, n \in \mathbb{N}$  restricted to

$$mu_i + nv_i < \frac{a_r}{\gcd(a_i, a_r)},$$

for all  $i \in \{1, \dots, r-1\}$ .

*Proof.* Apply Corollary 3 and the particular shape of  $A = \text{Ap}(M, Q)$  in Corollary 6.  $\square$

*Remark 2.* Notice that both Corollaries 3 and 7 hold if the Hilbert basis consists in the extreme rays plus an extra element, say  $u$ . The decomposition and restrictions of the parameters will be the same suppressing the terms in  $v$ .

*Example 1.* Let  $N$  be the set of nonnegative integer solutions of  $4x + 5y = 7z$ . Then we know that  $M$  is the set of nonnegative integer solutions of  $4x + 5y \equiv 0 \pmod{7}$ . The extremal rays of  $M$  are  $(7, 0)$  and  $(0, 7)$ , that is, the Gale base of  $M$  is  $Q = \{(7, 0), (0, 7)\}$ . Since  $M$  is also a full affine semigroup,  $\text{Ap}(M, Q) = M \cap [0, 6]^2$ . The elements in this set are

$$\{(0, 0), (1, 2), (2, 4), (3, 6), (4, 1), (5, 3), (6, 5)\}.$$

In order to obtain the Hilbert basis of  $M$  it suffices to take  $(7, 0)$ ,  $(0, 7)$  and the minimal nonzero elements of  $M \cap [0, 6]^2$ :  $(1, 2)$  and  $(4, 1)$ . Thus  $H = \{(7, 0), (0, 7), (1, 2), (4, 1)\}$  is a Hilbert basis of  $M$ .

By Corollary 7, with  $u = (1, 2)$  and  $v = (4, 1)$ , the unique representation of any element  $x \in M$  is

$$x = \lambda_1(7, 0) + \lambda_2(0, 7) + m(1, 2) + n(4, 1),$$

with  $\lambda_1, \lambda_2 \in \mathbb{N}$  and parameters  $m, n \in \mathbb{N}$  restricted by

$$m + 4n < 7 \text{ and } 2m + n < 7.$$

The latter restrictions are equivalent to  $(m, n) \in \{0, 1, 2\} \times \{0, 1\} \cup \{(3, 0)\}$ , and the integers  $\lambda_1, \lambda_2, n, m$  are unique (compare with [5], page 368). If we do not put restrictions on  $n$  and  $m$ , then we lose uniqueness.

Set  $q_1 = (7, 0)$  and  $q_2 = (0, 7)$ . As  $7(1, 2) = (7, 0) + 2(0, 7)$ , we obtain  $\lambda(q_1, (1, 2)) = \frac{1}{7}$  and  $\lambda(q_2, (1, 2)) = \frac{2}{7}$ . In a similar way we can compute  $\lambda(q_i, a)$  for  $i \in \{1, 2\}$  and  $a \in \text{Ap}(M, Q)$ . It



follows that  $\ell(q_1) = \ell(q_2) = 7$ . By Corollary 5,  $\text{inCl}(M)$  is isomorphic to  $\text{Ap}(M, Q)$  endowed with the operation  $\oplus$ . This group is isomorphic to  $\mathbb{Z}_7$ .

In our setting  $\mathbb{Z}^{(Q)} = \mathbb{Z}^2$  and  $\varphi : M \rightarrow \mathbb{Z}^2$ ,  $\varphi(x) = (7\lambda(q_1, x), 7\lambda(q_2, x))$ . Also  $\varphi(G(M)) = G(\varphi(M)) = G(\varphi(H))$ , so we can describe  $\varphi(G(M))$  by computing the images of the elements in  $H$  via  $\varphi$  and then taking the group spanned by them. A quick calculation shows that  $\varphi((7, 0)) = (7, 0)$ ,  $\varphi((0, 7)) = (0, 7)$ ,  $\varphi((1, 2)) = (1, 2)$ ,  $\varphi((4, 1)) = (4, 1)$ , and consequently  $\varphi$  is just the inclusion of  $M$  inside  $\mathbb{N}^2$ . The group spanned by  $\{(7, 0), (0, 7), (1, 2), (4, 1)\}$  equals the group  $G((1, 2), (3, -1))$  with invariant factors 1, 7. Thus  $\text{Cl}(M) \cong \mathbb{Z}_7$ .

## 5. THE TWO DIMENSIONAL CASE

In this section we focus in the case  $ax + by = cz$ , or equivalently,  $ax + by \equiv 0 \pmod{c}$ . We may assume that  $\text{gcd}(a, b, c) = 1$  (if not, we divide the equation by this amount).

**Lemma 6.** *Let  $c$  be a positive integer and let  $a, b \in \{1, \dots, c-1\}$  with  $\text{gcd}(a, b, c) = 1$ . Let  $M$  be the set of nonnegative integer solutions of  $ax + by \equiv 0 \pmod{c}$ . Let  $Q = \{(\frac{c}{\text{gcd}(a, c)}, 0), (0, \frac{c}{\text{gcd}(b, c)})\}$ . Then*

$$\text{Ap}(M, Q) = \left\{ \left( \text{gcd}(b, c)i, -ida \pmod{\left(\frac{c}{\text{gcd}(b, c)}\right)} \right) \mid i \in \left\{ 0, \dots, \frac{c}{\text{gcd}(a, c)\text{gcd}(b, c)} - 1 \right\} \right\},$$

where  $d = (b/\text{gcd}(b, c))^{-1} \pmod{c/\text{gcd}(b, c)}$ .

*Proof.* We already know by Lemma 5 that

$$\text{Ap}(M, \{(c/\text{gcd}(a, c), 0), (0, c/\text{gcd}(b, c))\}) = M \cap [0, c/\text{gcd}(a, c)] \times [0, c/\text{gcd}(b, c)].$$

We are going to prove that

$$\text{Ap}(M, \{(c/\text{gcd}(a, c), 0), (0, c/\text{gcd}(b, c))\}) = \left\{ (i, j) \mid \begin{array}{l} i \in \{0, \dots, c/\text{gcd}(a, c) - 1\} \cap \text{gcd}(b, c)\mathbb{N}, \\ j = -da(i/\text{gcd}(b, c)) \pmod{c/\text{gcd}(b, c)} \end{array} \right\},$$

and then the rest of the proof follows by a change of indices.

Observe that if  $(i, j), (k, l) \in M \cap [0, c/\text{gcd}(a, c)] \times [0, c/\text{gcd}(b, c)]$ , with  $(i, j) \neq (k, l)$ , then  $i \neq k$  and  $j \neq l$ . Assume to the contrary and without loss of generality that  $i = k$  and  $j > l$ . Then  $(0, j - l) \in M$ , or equivalently  $(j - l)b \equiv 0 \pmod{c}$ . But then  $j - l$  is a multiple of  $c/\text{gcd}(b, c)$  in  $[0, c/\text{gcd}(b, c)]$ , which implies  $j - l = 0$ , a contradiction.

Let us see for which  $i \in \{0, \dots, c/\text{gcd}(a, c) - 1\}$  there is  $j \in \{0, \dots, c/\text{gcd}(b, c) - 1\}$  such that  $ai + bj \equiv 0 \pmod{c}$ . The equation in  $j$ ,  $bj \equiv -ai \pmod{c}$ , has a solution if and only if  $\text{gcd}(b, c)$  divides  $-ai$ , but  $\text{gcd}(\text{gcd}(b, c), a) = \text{gcd}(a, b, c) = 1$ , and so this occurs if and only if  $\text{gcd}(b, c) \mid i$ .

Thus, for each  $i \in \{0, \dots, c/\text{gcd}(a, c) - 1\} \cap \text{gcd}(b, c)\mathbb{N}$  there exists a unique  $j \in \{0, \dots, c/\text{gcd}(b, c) - 1\}$  such that  $(i, j) \in M$ .

If  $(i, j) \in M$ , we already know that  $\text{gcd}(b, c) \mid i$ . Also there must exist  $r \in \mathbb{N}$  such that  $ai + bj = rc$ . Dividing by  $\text{gcd}(b, c)$ , we have  $ai/\text{gcd}(b, c) + b/\text{gcd}(b, c)j = rc/\text{gcd}(b, c)$ , or equivalently  $ai/\text{gcd}(b, c) + b/\text{gcd}(b, c)j \equiv 0 \pmod{c/\text{gcd}(b, c)}$ . From here, we obtain that  $j$  can be expressed as  $j = -(b/\text{gcd}(b, c))^{-1}ai/\text{gcd}(b, c) \pmod{c/\text{gcd}(b, c)}$ .  $\square$

**Theorem 4.** *Let  $c$  be a positive integer and let  $a, b \in \{1, \dots, c-1\}$  with  $\text{gcd}(a, b, c) = 1$ . Let  $M$  be the set of nonnegative integer solutions of  $ax + by \equiv 0 \pmod{c}$ . Then*

$$\text{inCl}(M) \cong \text{Cl}(M) \cong \mathbb{Z}_{\frac{c}{\text{gcd}(a, c)\text{gcd}(b, c)}}.$$

*Proof.* The equality  $\text{Cl}(M) \cong \mathbb{Z}_{\frac{c}{\text{gcd}(a, c)\text{gcd}(b, c)}}$  is a consequence of [1, Theorem 1.3]. By Corollary 5 and Lemma 6, we get that  $\text{inCl}(M)$  is a cyclic group of size  $c/(\text{gcd}(a, c)\text{gcd}(b, c))$  and thus it is isomorphic to  $\text{Cl}(M)$ .  $\square$

*Remark 3.* For  $a, b, c$  positive integers with  $\gcd(a, b, c) = 1$  we have that the set of solutions of  $ax + by \equiv 0 \pmod{c}$  is a Cale monoid with tame basis  $\{q_1 = (c/\gcd(a, c), 0), q_2 = (0, c/\gcd(b, c))\}$ . Also by Lemma 6, the group  $\text{Ap}(M, Q)$  (with the operation  $\oplus$ ) is generated by an element of the form  $(\gcd(b, c), k)$  with  $k$  a positive integer less than  $c/\gcd(b, c)$ . By Remark 1, in order to compute  $\ell(q_1)$  and  $\ell(q_2)$  we only have to look at the denominators of the rational number  $\lambda(q_1, (\gcd(b, c), k))$  and  $\lambda(q_2, (1, k))$ . From  $\frac{c}{\gcd(b, c)}(1, k) = \gcd(a, c)q_1 + kq_2$ ,  $\lambda(q_1, (1, k)) = \gcd(a, c)\gcd(b, c)/c = 1/(c/\gcd(a, c)\gcd(b, c))$ , and thus  $\ell(q_1) = c/(\gcd(a, c)\gcd(b, c))$ . But now Corollary 4 states that  $\ell(q_1)\ell(q_2) = |\text{Cl}(M)|/|\text{inCl}(M)|$  and we know by Theorem 4 that the equalities  $|\text{Cl}(M)| = |\text{inCl}(M)| = c/(\gcd(a, c)\gcd(b, c))$  hold. Therefore  $\ell(q_2) = c/(\gcd(a, c)\gcd(b, c))$ .

*Example 2.* Let us go back to Example 1, now applying Lemma 6. We have  $a = 4$ ,  $b = 5$  and  $c = 7$ . Then  $b^{-1} \pmod{c} = 3$ . Thus by Lemma 6, the elements in  $\text{Ap}(M, \{(c, 0), (0, c)\})$  are of the form

$$(i, -3 \times 4 \times i \pmod{7})$$

for  $i \in \{0, \dots, c-1\}$ . For  $i = 0$ , we get  $(0, 0)$ , for  $i = 1$ , we obtain  $(1, -12 \pmod{7}) = (1, 2)$ , and so on.

Then to obtain a Hilbert basis we filtered the set obtained, looking for the second coordinate less than the last second coordinate obtained, i.e. as the set obtained using the algorithm is

$$\{(0, 7), (1, 2), (2, 4), (3, 6), (4, 1), (5, 3), (6, 5), (7, 0)\}.$$

We construct the Hilbert basis starting with  $\{(0, 7), (1, 2)\}$ , the point  $(2, 4)$  has second coordinate bigger than 2 (the second coordinate of the last point added, then we do not need it, as well  $(3, 6)$ ). However  $(4, 1)$  has the second coordinate less than 2, so we add it. Finally  $(5, 3)$  and  $(6, 5)$  have second coordinate bigger than 1 so we ignore them. Adding  $(7, 0)$  we construct the Hilbert basis  $H = \{(0, 7), (1, 2), (4, 1), (7, 0)\}$ .

Note that multiplying by  $2 \equiv 4^{-1} \pmod{7}$  both  $a$  and  $b$  we obtain the same Apéry set and the same conclusions, that is, the equation  $x + 3y \equiv 0 \pmod{7}$  is equivalent to the above.

Observe that Corollary 6 and Lemma 6 provide a way to express any solution of  $ax + by = cz$  (equivalently  $ax + by \equiv 0 \pmod{c}$ ) in a unique way as  $a + \lambda q_1 + \mu q_2$ , with  $a$  in the Apéry set of  $\{q_1, q_2\}$ , and  $\lambda, \mu \in \mathbb{N}$ . However this is not the approach given by Elliott; he was looking for a (unique) description of the solutions of the form  $\gamma_1 a_1 + \dots + \gamma_t a_t + \lambda q_1 + \mu q_2$ , with  $\lambda, \mu \in \mathbb{N}$  and  $\gamma_i \in J_i$ , with  $J_i$  an interval of nonnegative integers. We gave such a description in Example 1. Next we present a family of equations where we can provide a “unique” description of the solutions in Elliott’s sense.

*Example 3.* Consider the equation  $ax + y \equiv 0 \pmod{2a+1}$  with  $a \in \mathbb{Z}^+$ . We have  $\gcd(a, 2a+1) = 1$ . It is no difficult to see that the Hilbert basis is  $H = \{(0, 2a+1), (1, a+1), (2, 1), (2a+1, 0)\}$ , and also

$$\begin{aligned} \text{Ap}(M, \{(2a+1, 0), (0, 2a+1)\}) = & \{(2i, i) \mid i \in \{0, \dots, a-1\}\} \\ & \cup \{(2i+1, a+i+1) \mid i \in \{0, \dots, a-1\}\}. \end{aligned}$$

We apply Corollary 7 with  $u = (1, a+1)$  and  $v = (2, 1)$ . It follows that any solution of  $ax + y \equiv 0 \pmod{2a+1}$  is expressed (uniquely) as  $\lambda_1(0, 2a+1) + \lambda_2(2a+1, 0) + m(1, a+1) + n(2, 1)$ , with  $\lambda_i \in \mathbb{N}$  and  $m, n \in \mathbb{N}$  parameters restricted to  $m + 2a < 2a+1$  and  $m(a+1) + n < 2a+1$ . These restrictions are equivalent to  $(m, n) \in \{0\} \times [0, a] \cup \{1\} \times [0, a-1]$ .

Recall that Example 2 corresponds to the equation  $x + by \equiv 0 \pmod{2b+1}$  by taking  $b = 3$ ; this case is dual to the above example and can be worked out in a similar way.

Another useful algorithm to find the set of minimal solution, or Hilbert basis, for this type of equations can be found in [6, Figure 3], which computes all minimal solutions by means of geometrical tools. The authors called it *slopes algorithm* because it calculates the slopes of the lines containing the minimal solutions.

## REFERENCES

- [1] S. T. Chapman, U. Krause, E. Oeljeklaus, Monoids determined by a homogeneous linear Diophantine equation and the half-factorial property. *J. Pure Appl. Algebra* **151** (2000), no. 2, 107–133.
- [2] S. T. Chapman, F. Halter-Koch, U. Krause, Inside factorial monoids and integral domains. *J. Algebra* **252** (2002), 350–375.
- [3] S. T. Chapman, U. Krause, Cale monoids, cale domains, and cale varieties. *Arithmetical properties of commutative rings and monoids*, 142–171, *Lect. Notes Pure Appl. Math.*, **241**, Chapman & Hall/CRC, Boca Raton, FL, 2005.
- [4] E. Domenjoud, Solving systems of linear Diophantine equations: an algebraic approach. *Mathematical foundations of computer science, 1991* (Kazimierz Dolny, 1991), 141–150, *Lecture Notes in Comput. Sci.*, **520**, Springer, Berlin, 1991.
- [5] E. B. Elliott, On linear homogeneous Diophantine equations, *Quart. J. Pure Appl. Math.* **34** (1903), 348–377.
- [6] M. Filgueiras, A.P. Tomás, A Fast Method for Finding the basis of Non-negative Solutions to a Linear Diophantine Equation. *J.Symbolic Computation* **19** (1995), 507–526.
- [7] M. Hochster, Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes. *Ann. of Math.* **96** (1972), 318–337.
- [8] R. Stanley, *Enumerative Combinatorics*, Vol.1, CUP,1997.
- [9] J. C. Rosales and P. A. García-Sánchez, On Cohen-Macaulay and Gorenstein simplicial affine semigroups, *Proc. Edinburgh Math. Soc.* **41** (1998), no. 3, 517–53.
- [10] J. C. Rosales and P. A. García-Sánchez, On the structure of Cohen-Macaulay simplicial affine semigroups, *Comm. Algebra* **27** (1999), no. 2, 511–518.
- [11] J. C. Rosales and P. A. García-Sánchez, On full affine semigroups, *J. Pure Appl. Algebra* **149** (2000), 295–303.
- [12] T. Tamura. Commutative nonpotent Archimedean semigroup with cancellation law, *J.Gakugei Tickushima Univ.* **8** (1957) 5-11.

DEPARTAMENTO DE ÁLGEBRA AND IEMATH-GR, UNIVERSIDAD DE GRANADA, E-18071 GRANADA, ESPAÑA  
*E-mail address:* `pedro@ugr.es`

UNIVERSITÄT BREMEN, FACHBERICH MATHEMATIK/INFORMATIK, D-28359 BREMEN, GERMANY  
*E-mail address:* `ukrause@uni-bremen.de`

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE ALMERIA, E-04120 ALMERIA, ESPAÑA  
*E-mail address:* `dllena@ual.es`