FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Bc. Lucien Šíma

Finitely generated semirings and semifields

Department of Algebra

Supervisor of the master thesis: Mgr. Vítězslav Kala, Ph.D.
Study programme: Mathematics
Study branch: Mathematical Structures

Prague 2021

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In . . . . date . . . .
                                                      Author's signature

Title: Finitely generated semirings and semifields

Author: Bc. Lucien Šíma

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: We investigate commutative semirings, which are formed by a ground set equipped with two binary associative and commutative operations such that one distributes over the other. We narrow down our interest to ideal-simple semirings, that is, semirings without proper ideals. We present the classification of ideal-simple semirings and deal with some classes of ideal-simple semirings, namely semifields and parasemifields. The main result of this thesis is giving tight bounds on the minimal number of generators needed to generate a parasemifield as a semiring. We also study how the semifields that are finitely generated as a semiring look like. Last, but not least, we show that every finitely generated ideal-simple semiring is finitely-generated as a multiplicative semigroup.

Keywords: ideal-simple semirings, finitely generated semirings, parasemifields, semifields

Contents

Introduction

Commutative semirings are formed by a ground set equipped with two binary associative and commutative operations such that one distributes over the other. They are a generalization of commutative rings and can be found in many various areas of mathematics, such as tropical geometry, number theory and algebra.

The most fundamental examples of semirings are natural numbers, positive rational integers or real functions together with addition and point-wise maximum. We narrow down our interest to the class of *ideal-simple* semirings, i.e., semirings without proper ideals.

The thesis is organized as follows. In Chapter 2, we introduce the key definition of an ideal-simple semiring and define a couple of fundamental classes of ideal-simple semirings, namely *parasemifields* and *semifields*. We present the classification of ideal-simple semirings (Theorem 2.8), which was introduced by [Bashir et al., 2001]. For the comfort of the reader, we give more detailed proofs. Moreover, we add one new class of ideal-simple semirings (formed by a multiplicative abelian group with an added zero element and with zero addition), which was not mentioned in the classification by [Bashir et al., 2001].

In Chapter 3, we state the classification of parasemifields that are finitely generated as the semiring (Theorem 3.5) from the article [Kala, 2017]. The author shows that every finitely-generated parasemifield can be associated with a rooted forest containing an additive group of integers in each of its vertices. The second semiring operation is defined as a lexicographic maximum with respect to the forest structure.

The aim of Chapter 4 is to determine the minimal number of generators needed to generate a given parasemifield using the semiring operations. We show that this number is indeed linear in the depth of the rooted forest that represents it (Theorem 4.15). We also give the precise minimal number of generators for the parasemifields corresponding to $\mathbb{Z}^n$ equipped with a coordinate-wise addition and maximum (Theorem 4.7).

Chapter 5 is devoted to study semifields that are finitely generated as a semiring. We combine the classifications from previous chapters together with a couple of known results regrading finitely-generated groups to give a detailed description of how the finitely-generated semifields look like (Theorem 5.1, Theorem 5.6 and Theorem 5.8). We also show an intriguing fact that every finitely-generated ideal-simple semiring is finitely-generated as a multiplicative semigroup (Corollary 5.2).

Let us comment on the original contribution of the author. In Chapter 2, we present a detailed classification of ideal-simple semirings, as self-contained as possible. All results contained in Chapter 4 and Chapter 5 are original and due to the author. We intend to submit them to a scientific journal.

1. Preliminaries

1.1 Semigroups

We are going to present a couple of observations from group theory, which are going to be useful in the study of semirings. We assume that every semigroup is commutative.

Definition 1.1. *By a* (commutative) semigroup*, we mean a ground set S equipped with one binary operation (usually denoted by $*$) that is associative and commutative.*

Definition 1.2. *Let $S(*)$ be a semigroup and $a \in S$ its element. We say that a is* an absorbing element *if $a * s = a$ for every $s \in S$. We say that a is* a neutral element *if $a * s = s$ for every $s \in S$.*

For $k \in \mathbb{N}$, we denote by a^k the element we obtain by applying the operation $*$ on a with itself k times. By a cyclic subsemigroup generated by a, *we mean $\{a^k \mid k \in \mathbb{N}\}$, usually denoted by $\langle a \rangle$.*

Claim 1.3. *Let S be a finite semigroup and $a \in S$ its arbitrary element. Then $\langle a \rangle$ contains an idempotent element.*

Proof. We let $A = \{a^{2^i} \mid i \in \mathbb{N}\}$ be the subsemigroup of $\langle a \rangle$. Since S is finite, we are able to find $i, j \in \mathbb{N}, i < j$ such that $a^{2^i} = a^{2^j}$. Letting $b = a^{2^i}$ and $k = 2^{j-i} \geq 2$, we have that $b^k = b$. We obtain the following equation:

$$b^{k-1} * b^{k-1} = b^k * b^{k-2} = b * b^{k-2} = b^{k-1}$$

which shows that b^{k-1} (which clearly lies in $\langle a \rangle$) is an idempotent element. □

Claim 1.4. *Let S be a semigroup and let us suppose that $a * S \overset{\text{def}}{=} \{a * s \mid s \in S\} = S$ for each $a \in S$. Then S is a group.*

Proof. Take any $x \in S$. Since $x * S = S$, we can find $y \in S$ such that $x * y = x$. Similarly, we can find $z \in S$ such that $x * z = y$. Multiplying the first equation by z and the second one by y, we obtain that $x * y * z = x * z = y$ and $x * y * z = y * y$. Altogether, we have that $y * y = y$.

We will show that y is a neutral element in S. For that, we take an arbitrary element a from S. Since $y * S = S$, we can find $b \in S$ such that $y * b = a$. We obtain that $y * a = y * (y * b) = (y * y) * b = y * b = a$. It follows that S is a group. □

1.2 Rooted trees and forests

Definition 1.5. *By a* tree*, we mean a (finite, non-oriented) connected graph $T = (V(T), E(T))$ without cycles. We call its vertices of degree one* leaves*, the rest of them are called* internal vertices*. We say that a tree is* rooted *if one of its vertices has been designated to be the root, usually denoted by v.*

A forest *is a disjoint union of trees. A forest consisting of k trees $T_1 \cup \cdots \cup T_k$ is* rooted *if we can specify a root $v_i \in V(T_i)$ in each of its tree components. We usually denote the union of trees $T_1 \cup \cdots \cup T_k$ by F and by R the set of roots $\{v_1, \ldots, v_k\}$.*

Since trees are connected and acyclic, we always have a unique path connecting two arbitrary vertices. Let us develop a couple more notions.

Definition 1.6. *Let (T, v) be a rooted tree and $w \neq v$ its vertex. A* parent *of a vertex w is the vertex connected to w on the path from w to the root v. Every vertex has a unique parent except for the root, which has no parent. We say that a vertex x is a* child *of a vertex w if w is a parent of x.*

Definition 1.7. *For an arbitrary vertex $w \in V(T)$, we define its depth as the number of vertices on a unique path from v to w. Note that the depth of the root equals 1. By the* depth *of a tree T, we mean the maximal depth of a vertex among all vertices from T. We can extend these notions to forests naturally.*

Definition 1.8. *Let n be a natural number. We say that a rooted tree (T, v) is n-ary if each vertex of T has at most n children. We say that a rooted forest (F, R) is n-ary if $|R| \leq n$ and each of its tree components is n-ary. We sometimes write* binary *instead of 2-ary.*

1.3 Vectors

Notation 1.9. *Let n be a natural number. We denote the set $\{1, 2, \ldots, n\}$ by $[n]$.*

Notation 1.10. *Throughout the thesis, we are going to work with integer-valued vectors. To distinguish vectors from scalar numbers, we use either a tuple of integers or we write a vector's name in bold (for example $\mathbf{v}$).*

If $\mathbf{v}$ is a vector of dimension n, we denote by v_i its i-th coordinate for any $i \in [n]$. For a natural number k and a vector $\mathbf{v}$ we will denote by $k \cdot \mathbf{v}$ the vector obtained by applying addition on $\mathbf{v}$ with itself k times.

Furthermore, for any $i \in [n]$, we denote by $\mathbf{e_i}$ the vector, which has i-th coordinate equal to one and all the other coordinates equal to zero. We sometimes refer to $\mathbf{e_i}$ as the i-th canonical *vector.*

Finally, the vector $(c, \ldots, c)$ is sometimes denoted by $\mathbf{c}$ for an integer c. The dimension of $\mathbf{c}$ should be clear from the context.

Definition 1.11. *We say that a vector is* positive (negative)*, if all its coordinates are.*

1.4 Finitely generated abelian groups

In this section, we define a free abelian group and a finitely generated group. We also present a couple of fundamental results from group theory.

Notation 1.12. *Let $G(+, -, 0)$ be an additive group and $a \in G$ its element. For a natural number n, we denote by na the element obtained by applying addition on a with itself n times. By $(-n)a$, we mean the element $n(-a)$.*

Notation 1.13. *Let G and H be two groups. By $G \times H$, we mean the Cartesian product of ground sets G and H. We denote the direct product of groups G and H by $G \oplus H$.*

Definition 1.14. *Let $G(+)$ be a group and $H \subseteq G$ its subset. We say that H generates G if for every $g \in G$, we can find $n \in \mathbb{N}$, $h_1, \ldots, h_n \in H$ and $k_1, \ldots, k_n \in \mathbb{Z}$ such that $g = k_1 h_1 + \cdots + h_n k_n$. If such H can be chosen finite, we say that G is* finitely generated.

Observation 1.15. *Let $G(+)$ be an abelian group and H its subgroup. If H and G/H are finitely generated groups, then G is also finitely generated.*

Proof. We suppose that the set $B = \{[b_1], \ldots, [b_m]\}$ generates G/H and that the set $C = \{c_1, \ldots, c_n\}$ generates H. We will show that G is generated by the set $\{b_1, \ldots, b_m, c_1, \ldots, c_n\}$. Let us take an arbitrary $g \in G$. Since G/H is generated by B, we can find $k_1, \ldots, k_m \in \mathbb{Z}$ and $h \in H$ such that:

$$[g] = [\sum_{i=1}^{m}(k_i b_i)] \Rightarrow g = h + \sum_{i=1}^{m}(k_i b_i). \tag{1.1}$$

Because H is generated by C, we can find $l_1, \ldots, l_n \in \mathbb{Z}$ such that:

$$h = \sum_{j=1}^{n}(l_j c_j). \tag{1.2}$$

We plug Equation 1.2 into the Equation 1.1 to obtain that:

$$g = \sum_{j=1}^{n}(l_j c_j) + \sum_{i=1}^{m}(k_i b_i),$$

as desired. $\qquad\qquad\square$

Definition 1.16. *An abelian group $G(+)$ is called* free *if we can find a* basis *$B = \{b_1, \ldots, b_n\} \subseteq G$ such that every element $g \in G$ can be uniquely expressed as $g = k_1 b_1 + \cdots + k_n b_n$ for some integer coefficients $k_1, \ldots, k_n$. We denote this fact by $G = \langle b_1, \ldots, b_n \rangle$. The number n is called the* rank *of G.*

Let us recall the well-known classification of finitely generated abelian groups and mention how the subgroups of a free group look like.

Theorem 1.17 ([Rotman, 1999, Theorem 10.20.]). *Let G be a finitely generated abelian group. Then we can find $n, m \in \mathbb{N}_0$, natural numbers $k_1, \ldots, k_m$ and primes $p_1, \ldots, p_m$ such that $G \simeq \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{k_m}}$.*

Notation 1.18. *Let m, n be integers such that m divides n. We denote this fact by $m \mid n$.*

Theorem 1.19 ([Dummit and Foote, 1999, Theorem 12.4.]). *Let H be a subgroup of $\mathbb{Z}^n$. Then we can find a basis $\{\mathbf{a_1}, \ldots, \mathbf{a_n}\}$ of $\mathbb{Z}^n$, a natural number $m \leq n$ and natural numbers $d_1 \mid d_2 \mid \cdots \mid d_m$ such that $H = \langle d_1 \cdot \mathbf{a_1}, \ldots, d_m \cdot \mathbf{a_m} \rangle$. Consequently, H is free of rank m.*

2. The classification of ideal-simple semirings

In this chapter, we introduce the key definition of an ideal-simple semiring. We present the classification of ideal-simple semirings from [Bashir et al., 2001] and we give more detailed proofs.

2.1 Ideal-simple semirings

Definition 2.1. *By a* (commutative) semiring*, we mean a ground set S equipped with two binary associative and commutative operations (denoted by $+$ and $\cdot$) such that multiplication distributes over addition, i.e., for every $a, b, c \in S$, we have that $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$.*

Throughout the thesis, we will be working with commutative semirings only, and hence the word semiring will always mean a commutative semiring.

Definition 2.2. *Let S be a semiring. We say that S is* additively idempotent *if $a + a = a$ for every $a \in S$. S is called* additively cancellative *if $a + c = b + c$ implies $a = b$ for every $a, b, c \in S$. The same notions (*multiplicative idempotency *and* multiplicative cancellativity*) are defined for multiplication.*

Definition 2.3. *Let S be a semiring and $I \subseteq S$ its subset. We say that I is* an ideal *if following two conditions are met:*

1. $\forall a, b \in I : a + b \in I$

2. $\forall a \in I, \forall s \in S : a \cdot s \in I$

An ideal I is called proper *if and only if $|I| \geq 2$ and $I \neq S$. S is said to be* ideal-simple *if it does not contain any proper ideals.*

Observation 2.4. *Let S be a semiring and $a \in S$. Then $aS \overset{\text{def}}{=} \{a \cdot s \mid s \in S\}$ is an ideal.*

Proof. It suffices to verify the axioms of an ideal. Let us take two arbitrary elements as, at from aS. Then $as + at = a(s + t)$ also lies in aS. For any $r \in S$, we have $(as)r = a(sr)$, which is also an element of aS. $\qquad\square$

Every semiring S, which has at most two elements, clearly has to be ideal-simple. We present the list of all eight two-element semirings from [Bashir et al., 2001, Section 2].

S_1

+	0	1		·	0	1
0	0	0		0	0	0
1	0	0		1	0	0

S_2

+	0	1		·	0	1
0	0	0		0	0	0
1	0	0		1	0	1

S_3

+	0	1		·	0	1
0	0	0		0	0	0
1	0	1		1	0	0

S_4

+	0	1		·	0	1
0	0	0		0	1	1
1	0	1		1	1	1

S_5

+	0	1		·	0	1
0	0	0		0	0	1
1	0	1		1	1	1

S_6

+	0	1		·	0	1
0	0	0		0	0	0
1	0	1		1	0	1

S_7

+	0	1		·	0	1
0	0	1		0	0	0
1	1	0		1	0	0

S_8

+	0	1		·	0	1
0	0	1		0	0	0
1	1	0		1	0	1

Figure 2.1: Two-element commutative semirings.

From now on, let us suppose that $|S| \geq 3$. We will start with definitions of a semifield and a parasemifield, which are going to be two typical examples of ideal-simple semirings.

Definition 2.5. *Let S be a semiring. If $S(\cdot)$ forms a group, we say that S is a* parasemifield. *S is a* semifield, *if we can find an element $0 \in S$ such that $0S = \{0\}$ and $(S \setminus \{0\}, \cdot)$ is a group. We usually denote the neutral element of the multiplicative group by 1.*

Observation 2.6. *Parasemifields and semifields are ideal-simple.*

Proof. Let S be a semifield. Let I be an ideal such that $|I| \geq 2$. We can thus take $a \in I, a \neq 0$. For an arbitrary $s \in S$, we have that $s = a(a^{-1}s)$ lies in I, implying that $I = S$. The proof for parasemifields is almost identical. $\square$

Before giving the first classification of ideal-simple semirings, we need an auxiliary claim regarding multiplicatively absorbing elements.

Claim 2.7. *Let S be an ideal-simple semiring and $w \in S$ absorbing with respect to multiplication, i.e., $sw = w$ for every $s \in S$. Then:*

(a) $w + w = w$

(b) w is either absorbing or neutral with respect to addition

Proof. We have that $sw = w$ for every $s \in S$, in particular, for $s = w + w$, we obtain that: $w = sw = (w + w)w = (ww) + (ww) = w + w$ and we are done with the first part.

For the second part, we will observe that the set $S + w \overset{\text{def}}{=} \{s + w \mid s \in S\}$ is an ideal. For that, we take arbitrary $s, t \in S$ and obtain that:

$$(s + w) + (t + w) = (s + t) + (w + w) = (s + t) + w \in S + w$$
$$t(s + w) = ts + tw = ts + w \in S + w.$$

Since s and t were chosen arbitrarily, it follows that $S + w$ is an ideal.

From the part (a) of this observation, we have that $w = w + w$, implying that $w \in S + w$. Since $S + w$ is an ideal in an ideal-simple semiring S, we have that either $S + w = \{w\}$ (exactly that w is absorbing) or $S + w = S$.

In the second case, we take any element $s \in S$. Since $S + w = S$, we can find $t \in S$ such that $t + w = s$. Adding w to both sides of this equation, we obtain:

$$s + w = (t + w) + w = t + (w + w) = t + w = s$$

which shows neutrality of w, since s was chosen arbitrarily. $\square$

Theorem 2.8 ([Bashir et al., 2001, Theorem 11.2])**.** *Let S be a semiring, $|S| \geq 3$. Then S is ideal-simple if and only if one of the following cases takes place:*

(1) S is isomorphic to $\mathbb{Z}_p$ with zero-multiplication, p odd prime

(2) S is a semifield

(3) S is a parasemifield

Proof. We shall start with showing that semirings of all three listed types are ideal-simple. Parasemifields and semifields are ideal-simple from Observation 2.6.

In the remaining case (1), let $I \subseteq \mathbb{Z}_p, |I| \geq 2$ be an ideal. Let us take $a \in I$, $a \neq 0$ and we will observe that $a\mathbb{Z}_p = \mathbb{Z}_p$. It suffices to show that the set $\{0, a, 2a, \ldots, (p-1)a\}$ consists of p distinct elements (in $\mathbb{Z}_p$). For contradiction, suppose $0 \leq i < j \leq p - 1$ such that $ia = ja$, implying that p divides $(j - i)a$. Since p is a prime number, then either $p \mid a$ or $p \mid (j - i)$, which is not possible, as both numbers lie in $[p - 1]$. We have that $a\mathbb{Z}_p = \mathbb{Z}_p$ which clearly implies that $I = \mathbb{Z}_p$. We are done with the first implication.

For the converse, let us assume that S is ideal-simple. From Observation 2.4, we have that aS is an ideal for every $a \in S$. Because S is an ideal-simple semiring, we have that either $|aS| = 1$ or $aS = S$. Let $A = \{a \in S \mid |aS| = 1\}$ be a subset of S.

If $A = \emptyset$, we have that $aS = S$ for every element $a \in S$. It follows from Claim 1.4 that $S(\cdot)$ is a group. Consequently, S is a parasemifield.

From now on, we assume that A is non-empty. First, let us observe that $|AS| = 1$. For contradiction, suppose that we can find $a, b \in A$ and $s \neq t \in S$, such that $aS = \{s\}, bS = \{t\}$. But $ab \in (aS \cap bS) = (\{s\} \cap \{t\}) = \emptyset$, contradiction. Let us denote by 0 the only element of AS. We have that $A = \{a \in S \mid aS = \{0\}\}$.

We are going to show that $0 \in A$. We have assumed that A is non-empty, so we are able to take $a \in A$. From the definition of A, we have, for every $s \in S$,

that $a0 = 0$ and $0s = (a0)s = a(0s) = 0$. Since s was chosen arbitrarily, it follows that $0S = \{0\}$, implying that $0 \in A$.

Furthermore, let us observe that the set A forms an ideal. Recall that $0S = \{0\}$ and Claim 2.7 gives us that $0 + 0 = 0$. Take any $a, b \in A$ and any $t \in S$. The following equations hold for any $s \in S$:

$$(a + b)s = as + bs = 0 + 0 = 0$$
$$(ta)s = t(as) = t0 = 0,$$

implying that $a + b, ta \in A$ and that A is an ideal. Since $0 \in A$ and S is ideal-simple, we can distinguish two cases depending on whether $A = S$ or $A = \{0\}$.

Case 1)
We assume that $A = S$ and consequently $SS = \{0\}$. We shall start with an auxiliary observation.

Observation 2.9. *Let S be a semiring such that $SS = \{0\}$. If R is an additively closed subset of S, then $I = R \cup \{0\}$ is an ideal.*

Proof. Since $SS = \{0\}$, I is closed under multiplication by any element of S. We have assumed that R is closed under addition and Claim 2.7 gives us that $0+0 = 0$ and that $r+0 \in \{0, r\}$. Thus, I is closed under addition, the observation follows. $\square$

Now, let us fix an arbitrary $a \neq 0$ and let $P = \langle a \rangle = \{na \mid n \in \mathbb{N}\}$. If P is infinite, then $R = \{(2n)a \mid n \in \mathbb{N}\}$ is closed under addition and it follows from Observation 2.9 that $R \cup \{0\}$ is a proper ideal, so S is not ideal-simple.

On the other hand, if P is finite, then Claim 1.3 guarantees that P has to contain an idempotent element e. If $e \neq 0$, then it follows from Observation 2.9 that $\{e, 0\}$ is a proper ideal (we assumed that $|S| \geq 3$), so S is not ideal-simple.

Therefore, 0 has to be the only idempotent element in P. Observe that P is an ideal (see Observation 2.9) containing two distinct elements 0 and a, which implies that $P = S$. Since $0 \in P$, we can take the smallest natural number $p \geq 2$ such that $pa = 0$. If $p = 2$, then $|S| = |P| = 2$ which contradicts the assumption that $|S| \geq 3$. We can thus assume that $p \geq 3$.

It follows from Claim 2.7(b) that 0 is either absorbing or neutral with respect to addition. Let us distinguish two subcases based on that.

Case 1a)
We assume that 0 is an absorbing element with respect to addition. Let us look at the element $b = (p - 1)a \neq 0$. It follows that:

$$b + b = (p - 1)a + (p - 1)a = pa + (p - 2)a = 0 + (p - 2)a = 0.$$

Therefore, $\{b, 0\}$ is a proper ideal, contradiction.

Case 1b)
We assume that 0 is a neutral element with respect to addition. If p is a composite number, then p has a non-trivial divisor d and the set $I = \{nd(a) \mid n \in \mathbb{N}\}$ forms a proper ideal, contradiction. Therefore, p has to be an odd prime number.

We are going to show that $S = P = \{a, 2a, \ldots, pa\} \simeq \mathbb{Z}_p$. Let us suppose $ka \in P$ for a natural number $k > p$. We take $n \in \mathbb{N}$ and $r \in \{1, \ldots, p\}$ such that

9

$k = np + r$ and we observe that $ka = (np + r)a = n(pa) + ra = 0 + ra = ra \in \{a, 2a, \ldots, pa\}$.

We will show that $\{a, 2a, \ldots, pa\}$ consists of p distinct elements. For contradiction, suppose $1 \leq i < j \leq p$ such that $ia = ja$. Adding $(p - i)a$ to both sides of the equation, we obtain that $pa = pa + (j - i)a \Rightarrow 0 = (j - i)a$, contradiction with the minimality of p.

Since $(ia) + (p - i)a = pa = 0$ for every $i \in [p]$, we have that 0 is a unit element in the group $S(+)$. It follows that S is isomorphic to the additive group $\mathbb{Z}_p$ with zero-multiplication.

Case 2)

In the second case, we have that $A = \{0\}$ and we let $T = S \setminus \{0\}$. Recall that $A = \{0\}$ implies that $0S = \{0\}$ and that for every $t \in T$, we have $|tS| \neq 1$ and therefore $tS = S$. Let us take an arbitrary $t \in T$ and define the set $I_t = \{s \in S \mid ts = 0\}$.

Let us take any $a, b \in I_t$. Since following equations are satisfied for every $s \in S$:

$$t(a + b) = ta + tb = 0 + 0 = 0$$
$$t(as) = (ta)s = 0s = 0,$$

we have that the set I_t forms an ideal.

Clearly $0 \in I_t$ and we have that $I_t \neq S$ (since $tS = S$) and thus $I_t = \{0\}$. It follows from the definition of I_t that $tT = T$. Claim 1.4 gives us that $T(\cdot)$ is a group and consequently S is a semifield. $\square$

The theorem above gives us that ideal-simple semirings are either zero-multiplication rings with prime cardinality (which are not that interesting for further study) or semifields and parasemifields. Let us continue by looking more closely at the structure of semifields.

2.2 Semifields

The goal of this section will be to classify semifields. We will show that they are either fields, groups with an added zero element or they arise from a parasemifields. Throughout this section, we will denote by T the set $S \setminus \{0\}$, which forms a multiplicative group. We have to deal with four distinct type of semifields, as the following theorem proposes.

Theorem 2.10. *Let S be a semifield. Then one of the following cases occurs:*

(1) S is a field

(2) T is a parasemifield and $s + 0 = s$ for every $s \in S$

(3) $S + S = \{0\}$

(4) $a + S \neq \{0\}$ for each $a \in T$ and $s + 0 = 0$ for every $s \in S$

Proof. We apply Claim 2.7 on zero element to see that it is either neutral or absorbing element with respect to addition. We will distinguish two cases based on that.

First, we assume that 0 is neutral with respect to addition. Let $U = \{a \in T \mid 0 \notin a + S\}$. If $U = \emptyset$, we have that each element of S has an additive inverse, consequently $S(+)$ is a group and S is a field.

If $U \neq \emptyset$, we take $a \in U$ and we are going to show that $U = T$. For contradiction, suppose that $b \in T$ does not belong to U. From the definition of U, we can find $s \in S$ such that $b + s = 0$. Multiplying both sides of this equation by ab^{-1}, we obtain $a + ab^{-1}s = 0$, which is a contradiction with the fact that $a \in U$. We have shown that $U = T$. It follows that T is additively closed, T is a parasemifield and that S is a semifield of type (2).

On the other hand, we assume that 0 is an absorbing element with respect to addition. Let us suppose that S is not of type (4) and we will show that S has to be of type (3). We can thus find $a \neq 0$ such that for every $s \in S$ we have $a + s = 0$. Let b, c be two arbitrary elements from T. We can multiply the equation by ba^{-1} to obtain that $b + sba^{-1} = 0$. Since the equation holds for any $s \in S$, we can let $s = cab^{-1}$ to get that $0 = b + cab^{-1}ba = b + c$, as we wanted to show. $\qquad\square$

We are now going to concentrate on semifields of type (4). In order to classify semifields of this type completely, we have to develop the theory of congruence-simple semirings.

Notation 2.11. *Let S be a set and $R \subseteq S \times S$ a relation. If an ordered pair of elements (a, b) belongs to R, we write either $(a, b) \in R$ or aRb.*

Definition 2.12. *Let S be a semiring and let $R \subseteq S \times S$ be a relation. We say that R is a* congruence *if it is an equivalence and it is compatible with semiring operations, i.e., for every $a, b, c \in S$ satisfying that aRb, it holds that $(a+c)R(b+c)$ and $(ac)R(bc)$.*

We say that S is congruence-simple *(or cg-simple for brevity) when it has no non-trivial congruences. In other words, the only congruences on S are $id_S = \{(s, s) \mid s \in S\}$ and $S \times S$.*

The complete classification of congruence-simple semirings is contained in the article [Bashir et al., 2001]. We will only mention one theorem, which will be useful for classifying semifields.

Theorem 2.13 ([Bashir et al., 2001, Theorem 3.1. and Theorem 3.3])**.** *Let S be a cg-simple semiring and $|S| \geq 3$. Then one of the following cases occurs:*

1. *S is additively cancellative*

2. *S is additively idempotent and multiplicatively cancellative*

3. *S contains exactly one element a such that $|aS| = 1$. Then $S \setminus \{a\}$ is a multiplicative group and $S = V(S \setminus \{a\})$, which is defined below.*

Definition 2.14. *Let $G(\cdot)$ be a multiplicative abelian group and $0 \notin G$. We let $V(G) \stackrel{\text{def}}{=} G \cup \{0\}$ and we define the semiring operations on $V(G)$ as follows. For every $x, y \in V(G)$, $x \neq y$, we let $x + x = x$ and $x + y = 0$. The multiplication is inherited from $G(\cdot)$ and we set $0 \cdot x = 0$ for each $x \in V(G)$.*

We can now get back to semifields and move towards the classification of semifields of type (4).

Definition 2.15. *Let S be a semiring and $a \in S$ its arbitrary element. The* annihilator *of a is defined to be $Ann(a) = \{s \in S \mid a + s = 0\}$. We define the relation $\sim \subseteq S \times S$ as follows: $a \sim b$ if and only if $Ann(a) = Ann(b)$.*

Observation 2.16. *Let S be a semifield of type (4) and let $\sim$ be the relation from Definition 2.15. It has following properties.*

1. *$\sim$ is a congruence on S*

2. *$P \stackrel{\text{def}}{=} [1]_\sim$ is a multiplicative subgroup of $T(\cdot)$*

3. *$[0]_\sim = \{0\}$*

Proof. Since $\sim$ is defined by the certain equality of sets, it is clear that it is an equivalence. We need to show that it preserves both binary operations. Let a, b, c, d be arbitrary elements from S such that $a \sim b$. We use $Ann(a) = Ann(b)$ to show that $Ann(a + c) = Ann(b + c)$:

$$d \in Ann(a + c) \iff a + c + d = 0 \iff c + d \in Ann(a) \iff$$
$$\iff c + d \in Ann(b) \iff b + c + d = 0 \iff d \in Ann(b + c).$$

If $c = 0$, then $Ann(ac) = Ann(bc)$ is obvious. Otherwise, we obtain $Ann(ac) = Ann(bc)$ as follows:

$$d \in Ann(ac) \iff ac + d = 0 \iff a + dc^{-1} = 0 \iff$$
$$\iff b + dc^{-1} = 0 \iff bc + d = 0 \iff d \in Ann(bc).$$

The second part is easy to show. It is clear that $1 \in P$. If $a \in P$, we can multiply both sides of $a \sim 1$ by a^{-1} to obtain $1 \sim a^{-1}$ and $a^{-1} \in P$. If $a, b \in P$, we multiply both sides of $a \sim 1$ by b to obtain $ab \sim b$. Together with $b \sim 1$, we get $ab \sim 1$ and $ab \in P$.

We show that $[0]_\sim = \{0\}$ by contradiction. Let us suppose that there is $a \in T$ such that $a \sim 0$. From the definition of semifields of type (4) (see Theorem 2.10), we can find $b \in T$ such that $a + b \neq 0$, hence $Ann(a) \neq S = Ann(0)$, contradiction. $\square$

Claim 2.17 ([Bashir et al., 2001, Proposition 12.2.])**.** *Let S be a semifield of type (4) and let $\sim$ be the congruence from Definition 2.15. We claim that the factor-semiring $R = S/\sim$ is congruence-simple and that R is isomorphic to an additively idempotent semifield $V(T/P)$, where $P = [1]_\sim$.*

Proof. From Observation 2.16(b), we have that $P(\cdot)$ is a multiplicative subgroup of an abelian group $T(\cdot)$, so the factor-group T/P is well-defined.

We will begin with showing that R is congruence-simple. Let $C \subseteq R \times R$ be a congruence, $C \neq id_R$. We can thus find $x, y \in R, x \neq y$ such that $(x, y) \in C$. Since $Ann(x) \neq Ann(y)$, we can without loss of generality assume that we can find $z \in Ann(x) \setminus Ann(y)$. From the definition of annihilators, we have that $x + z = 0$ and $y + z \neq 0$. Since $(x, y) \in C$, we have that $(x + z = 0, y + z) \in C$.

Let $I = \{z \in R \mid (z, 0) \in C\}$ and observe that it is an ideal. We have shown that I contains a non-zero element $y + z$. Therefore, we have that $I = R$, provided that the factor-semiring R of ideal-simple semifield S is also ideal-simple. It follows that $C = R \times R$ and that R is cg-simple.

Let us assume that $|R| = 2$. From Observation 2.16(c), we have that $[0]_\sim = \{0\}$. It follows that $R = \{[0], [1]\}$, where $P = [1]_\sim = T$. In order to show that $R \simeq V(T/P) = V(P/P) = V([1])$, it suffices to observe that $[1] + [1] = [1]$. Let us take $a \in T$. From the definition of semifields of type (4) (see Theorem 2.10), we can find $b \in T$ such that $a + b \in T$ and thus $[1] + [1] = [1]$.

If R is additively or multiplicatively cancellative, then let us take any element $a \in R, a \neq 0$. We have that $a+0 = 0 = 0+0$ and $a \cdot 0 = 0 = 0 \cdot 0$. The cancellativity would imply $a = 0$, contradiction.

If $|R| \geq 3$ and R is not additively nor multiplicatively cancellative, then Theorem 2.13 gives us that the only possible option is that $R \simeq V(R \setminus [0]_\sim)$, provided that $|0R| = |\{0\}| = 1$. From the fact $[0]_\sim = \{0\}$ (Observation 2.16(c)) and from the definition of P, it follows that $R \simeq V(R \setminus [0]_\sim) = V(R \setminus \{0\}) = V((S/\sim) \setminus \{0\}) = V(T/\sim) = V(T/P)$, as required. $\qquad\square$

Let us summarize and state the complete classification of semifields.

Theorem 2.18. *Let S be a semifield. Then one of the following cases occurs:*

(1) S is a field.

(2) S is constructed from a parasemifield T by adding an element 0 and letting $0 + s = s$ and $0s = 0$ for every $s \in S$.

(3) S is constructed from a multiplicative abelian group $A(\cdot)$ by adding an element 0 and letting $s + t = 0$ and $0s = 0$ for every $s, t \in S$.

(4) S is constructed from a parasemifield $P(+, \cdot)$ as follows. Let $P(\cdot)$ be a multiplicative subgroup of an abelian group $T(\cdot)$ and let $S = T \cup \{0\}$ and $S0 = \{0\}$. We define the addition for any $x, y \in S$ as follows:

$$x + 0 = 0$$
$$x^{-1}y \notin P : x + y = 0$$
$$x^{-1}y \in P : x + y = (x^{-1}y + 1) \cdot x.$$

The classification above tells us that semifields arise either from well-known structures (fields and groups) or from parasemifields. It is not much to be known about parasemifields in general, but when we confine ourselves to the class of parasemifields that are finitely generated as a semiring, there is a nice classification by [Kala, 2017] that will be presented in the following chapter.

3. The classification of finitely generated parasemifields

In this chapter, we would like to present the striking classification of parasemifields, which are finitely generated as a semiring, introduced by [Kala, 2017]. Let us begin with the definition of being finitely generated as a semiring.

Definition 3.1. *Let S be a semiring and $A \subseteq S$ its subset. We let $g(A) \subseteq S$ to be the smallest additively and multiplicatively closed subset of S containing A. We say that A generates S if $g(A) = S$. Moreover, we say that S is finitely generated as a semiring if S contains a finite subset A generating S. For brevity, we sometimes write fg-(para)semifield, meaning that the (para)semifield is finitely generated as a semiring.*

The classification by [Kala, 2017] is stated only for additively idempotent fg-parasemifields, but [Kala and Korbelář, 2018] proved the following conjecture a few months after publishing the classification.

Theorem 3.2 ([Kala and Korbelář, 2018, Theorem 4.5.])**.** *Let S be a fg-parasemifield. Then S is additively idempotent.*

As a result, the classification is now complete and we can state Theorem 3.5 and Corollary 3.6 for a general fg-parasemifield.

We are now going to associate a parasemifield $G(T, v)$ to a rooted tree (T, v) and extend this notion to rooted forests afterwards. We will use a couple of notions from graph theory (regarding rooted trees and forests) described in preliminaries.

Definition 3.3. *Let (T, v) be a rooted tree and n the size of its vertex set. We attach a copy of integers $\mathbb{Z}_w$ to each vertex $w \in V(T)$ forming the ground set of our parasemifield $G(T, v)$. We refer to elements of $G(T, v)$ as integer-valued vectors from $\mathbb{Z}^n$, each coordinate belongs to a certain vertex in (T, v).*

We shall define semiring operations on $G(T, v)$. The multiplication is defined to be the coordinate-wise addition from the group $\mathbb{Z}^n(+)$, which does not depend on structure of the tree (T, v).

The addition will be denoted by $\vee$ and is defined as follows. Let $\mathbf{g}, \mathbf{h}$ be two arbitrary elements from $G(T, v)$. For a vertex $w \in V(T)$, we define $(\mathbf{g} \vee \mathbf{h})_w$ as follows. Let $v = v_1, v_2, \ldots, v_k = w$ be vertices on the unique path from the root v to the vertex w. If $\mathbf{g}_{v_i} = \mathbf{h}_{v_i}$ for all $i \in [k]$ (vertices among the path), we set $(\mathbf{g} \vee \mathbf{h})_w = \mathbf{g}_w = \mathbf{h}_w$. Otherwise, we find the least i such that $\mathbf{g}_{v_i} \neq \mathbf{h}_{v_i}$. We can without loss of generality assume that $\mathbf{g}_{v_i} > \mathbf{h}_{v_i}$ and let $(\mathbf{g} \vee \mathbf{h})_w = \mathbf{g}_w$.

We define the same structure for rooted forests.

Definition 3.4. *Let (F, R) be a rooted forest, $F = T_1 \cup \cdots \cup T_k$ and $R = \{v_1, \ldots, v_k\}$ be the set of roots. We define the associated parasemifield $G(F, R)$ as the direct product of parasemifields $G(T_i, v_i)$.*

It turns out that every fg-parasemifield arises from a rooted forest in that way, as the following theorem proposes.

Theorem 3.5 ([Kala, 2017, Theorem 4.1]). *Let S be a fg-parasemifield. Then we are able to find a rooted forest (F, R) such that $(S, +, \cdot, ^{-1}) \simeq (G(F, R), \vee, +, -)$ and this forest is unique up to isomorphism.*

Corollary 3.6 ([Kala, 2017, Corollary 4.12.]). *Let S be a fg-parasemifield. Then S is finitely generated as a multiplicative semigroup.*

Proof. Theorem 3.5 gives us that $S \simeq G(F, R) = \mathbb{Z}^n$ for some rooted forest (F, R) and $n = |V(F)|$. The multiplicative group $S(\cdot)$ corresponds to $\mathbb{Z}^n(+)$. The corollary follows from the fact that $\mathbb{Z}^n$ is clearly generated as an additive semigroup (see Claim 4.3 in the next chapter). $\square$

4. The minimal number of generators of a parasemifield

We have discussed (in the previous chapter) that every fg-parasemifield S corresponds to a rooted forest (F, R) (in a sense that $S \simeq G(F, R)$). We turn our interest to finding the minimal number of generators needed to generate S as a semiring.

In this chapter, we are going to show that the minimal number of semiring generators of a fg-parasemifield S is indeed linear in the depth of the corresponding rooted forest (F, R). Let us briefly introduce some notation and show a couple of elementary results.

Notation 4.1. *Let $S \simeq G(F, R)$ be a fg-parasemifield. We will denote by $m(F, R)$ the minimal number of semiring generators of S.*

The multiplicative group of a parasemifield $G(F, R)$ is $\mathbb{Z}^n(+)$. Thus, it is quite useful to determine the minimal number of vectors needed to generate $\mathbb{Z}^n$ as an additive semigroup.

Observation 4.2. *Let n be a natural number and $\mathbf{u} \in \mathbb{Z}^n$ a negative vector. Then the set $\{\mathbf{e_1}, \ldots \mathbf{e_n}, \mathbf{u}\}$ together with coordinate-wise addition generates $\mathbb{Z}^n$.*

Proof. Let us take any vector $\mathbf{v} \in \mathbb{Z}^n$. Since $\mathbf{u}$ is a negative vector, we can find a natural k such that $\mathbf{w} = \mathbf{v} - k \cdot \mathbf{u}$ is a positive vector. Then $\mathbf{v} = \mathbf{w} + k \cdot \mathbf{u} = w_1 \cdot \mathbf{e_1} + \cdots + w_n \cdot \mathbf{e_n} + k \cdot \mathbf{u}$ for positive integers $k, w_1, \ldots, w_n$, as we wanted to show. $\square$

Claim 4.3. *The minimal number of semigroup generators of $\mathbb{Z}^n(+)$ is $n + 1$.*

Proof. The observation above gives us the set of $n + 1$ generators. It suffices to show that any n vectors do not generate $\mathbb{Z}^n$. For contradiction, suppose that the set $V = \{\mathbf{v_1}, \ldots, \mathbf{v_n}\}$ generates $\mathbb{Z}^n$. Thus, we can find non-negative integers $a_1, \ldots, a_n$ such that:

$$a_1 \cdot \mathbf{v_1} + \cdots + a_n \cdot \mathbf{v_n} = \mathbf{0}. \tag{4.1}$$

It is easy to see that V generates the vector field $\mathbb{Q}^n$ over $\mathbb{Q}$. Because V consists of n vectors and the dimension of $\mathbb{Q}^n$ over $\mathbb{Q}$ is n, it follows that V is a basis of $\mathbb{Q}^n$. But we have found a non-trivial linear combination of the zero vector (Equation 4.1) showing that V is not linearly independent, contradiction. $\square$

4.1 Isolated vertices

In order to bound $m(F, R)$, one needs to start with a base case, when the depth of F equals 1. We thus consider rooted forests (F, R), which are formed by n isolated vertices (and clearly $R = F$, because each tree component consists of exactly one vertex). We will denote such forests by Z_n and give the exact value of $m(Z_n)$ in this section.

In other words, we are looking for the minimal set G of vectors from $\mathbb{Z}^n$ such that G generates the whole $\mathbb{Z}^n$ together with addition and maximum (both applied coordinate-wise). We will start with an easier case, when $n \leq 2$.

Claim 4.4. *Let $n \in \{1, 2\}$. Then $m(Z_n) = 2$.*

Proof. It is clear that one generator can not be sufficient, as the sign is preserved under both operations, i.e., every coordinate would stay either positive or negative and the whole $\mathbb{Z}^n$ could not be generated.

We finish the proof by finding the generating set G of size two. If $n = 1$, we let $G = \{(1), (-1)\}$ and we simply generate $\mathbb{Z}^1$ (addition suffices).

For $n = 2$, we define G to be $\{(1, -2), (-2, 1)\}$. It suffices to generate the following three vectors $\{(1, 0), (0, 1), (-1, -1)\}$ since they generate the whole $\mathbb{Z}^n$ with coordinate-wise addition (Observation 4.2). We obtain the first one of them as follows:

$$(5, -2) = (1, -2) \vee (5 \cdot (1, -2))$$
$$(1, 0) = (5, -2) + 2 \cdot (-2, 1),$$

the second one is obtained in a similar manner:

$$(-2, 5) = (-2, 1) \vee (5 \cdot (-2, 1))$$
$$(0, 1) = (-2, 5) + 2 \cdot (1, -2)$$

and we get the last one by adding $(1, -2)$ and $(-2, 1)$. $\qquad\square$

Let us now consider the case when $n \geq 3$. Surprisingly, it turns out that $m(Z_n) = 3$, regardless on the value of n. In order to show that two generators do not suffice, we need to state an auxiliary observation.

Observation 4.5. *Let $1 \leq j \neq k \leq n$ be natural numbers and let us take two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^n$ satisfying that $u_j \geq a \cdot u_k$ and $v_j \geq a \cdot v_k$ for some positive real number a. Then the same inequality holds for vectors $\mathbf{u} + \mathbf{v}$ and $\mathbf{u} \vee \mathbf{v}$.*

Proof. The inequality for $\mathbf{u} + \mathbf{v}$ is verified by an easy computation:

$$(u + v)_j = u_j + v_j \geq a \cdot u_k + a \cdot v_k = a \cdot (u + v)_k.$$

Let $\mathbf{m} = \mathbf{u} \vee \mathbf{v}$. It holds that $m_j \geq u_j \geq a \cdot u_k$ and that $m_j \geq v_j \geq a \cdot v_k$. Since $m_k = u_k$ or $m_k = v_k$, the observation follows. $\qquad\square$

Corollary 4.6. *Let $G = \{\mathbf{g_1}, \ldots, \mathbf{g_m}\}$ be a set of vectors in $\mathbb{Z}^n$. Let $1 \leq j \neq k \leq n$ be natural numbers and let $a \in \mathbb{R}^+$ such that $g_{i,j} \geq a \cdot g_{i,k}$ for every $\mathbf{g_i} \in G$. Then G does not generate $\mathbb{Z}^n$.*

Proof. As a result of the observation above, the inequality holds for all generated vectors, the corollary follows. $\qquad\square$

We are now ready to prove the following theorem.

Theorem 4.7. *Let $n \in \mathbb{N}$, $n \geq 3$. Then $m(Z_n) = 3$.*

Proof. Let n be fixed. We will start with showing that two generators do not suffice. For contradiction, suppose that the set $G = \{\mathbf{u}, \mathbf{v}\}$ generates $\mathbb{Z}^n$.

We are going to distinguish two cases. First, let us suppose that we can find a coordinate i such that $u_i, v_i \geq 0$. Both operations preserve the sign, thus we can not generate any vector that has negative i-th coordinate. Similarly for $u_i, v_i \leq 0$.

Let us suppose the opposite, i.e., for every $i \in [n]$ we have either $u_i > 0, v_i < 0$ or $u_i < 0, v_i > 0$. Since $n \geq 3$, we can use pigeonhole principle to find two coordinates $j \neq k$ such that u_j has the same sign as u_k and v_j has also the same sign as v_k (because there are only two possible combinations of signs).

Without loss of generality, we assume that $u_j, u_k > 0, v_j, v_k < 0$. Let us denote the positive real number u_j/u_k by a. If $v_j/v_k \leq a$, then both inequalities $u_j \geq a \cdot u_k$ and $v_j \geq a \cdot v_k$ are satisfied. On the other hand, if $v_j/v_k \geq a$, then both $u_k \geq (1/a) \cdot u_j$ and $v_k \geq (1/a) \cdot v_j$ are satisfied. In either case, we have found an inequality satisfied by both vectors from G, contradiction with Corollary 4.6.

We finish the proof by finding the set of three generators of $\mathbb{Z}^n$. We let $k = n^2 + 1$ and we define $G = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ by setting $a_i = i, b_i = k - i^2, c_i = -1$. Note that k was chosen such that $\mathbf{b}$ is a positive vector.

We will start by generating n positive vectors $\mathbf{u_1}, \ldots, \mathbf{u_n}$ such that i-th coordinate of $\mathbf{u_i}$ is strictly maximal. We define $\mathbf{u_i}$ to be $2i \cdot \mathbf{a} + \mathbf{b}$. Then the j-th coordinate of $\mathbf{u_i}$ is $u_{i,j} = 2i \cdot a_j + b_j = 2ij + k - j^2 = k + j(2i - j)$. It is easy to see that this expression attains maximum for $j = i$, which gives us that i-th coordinate of $\mathbf{u_i}$ is indeed maximal, i.e., $u_{i,i} > u_{i,j}$ for all $j \neq i$.

For every $i \in [n]$, let us generate $\mathbf{v_i} = \mathbf{u_i} + ((u_{i,i}) - 1) \cdot \mathbf{c}$. Note that i-th coordinate of $\mathbf{v_i}$ equals 1 and all the other coordinates are non-positive.

Now it is the time to apply our second operation, which is coordinate-wise maximum (denoted by $\vee$). We obtain the zero vector as $\mathbf{0} = (\mathbf{v_1} \vee \mathbf{v_2} \vee \cdots \vee \mathbf{v_n}) + \mathbf{c}$. Finally, we get $\mathbf{e_i}$ as $\mathbf{v_i} \vee \mathbf{0}$.

As a result of Observation 4.2, all canonical vectors $\mathbf{e_i}$ together with the negative vector $\mathbf{c}$ generate the whole $\mathbb{Z}^n$ (with coordinate-wise addition). $\qquad\square$

4.2 Ordering

We introduce a partial ordering $\preceq$ on the set of rooted forests, which is compatible with the function m, in a sense that $(F, R) \preceq (E, S)$ implies $m(F, R) \leq m(E, S)$.

Definition 4.8. *We define a relation $\preceq$ on the set of rooted forests. Let (F, R) and (E, S) be two rooted forests. We say that $(F, R) \preceq (E, S)$ if and only if (F, R) can be obtained from (E, S) by deleting leaves from the forest E one by one. Note that $R \subseteq S$ is the set of roots from S, which were not deleted.*

Observation 4.9. *Let $\preceq$ be the relation on the set of rooted forests defined as above. Then:*

(a) the relation $\preceq$ is a partial ordering

(b) $(F, R) \preceq (E, S)$ implies that $m(F, R) \leq m(E, S)$

Proof. The reflexivity and the transitivity of $\preceq$ is obvious. For anti-symmetry, we suppose that $(F, R) \preceq (E, S)$ and $(E, S) \preceq (F, R)$. From the definition of $\preceq$ we have that $V(F) \subseteq V(G)$ and $V(G) \subseteq V(F)$ and it follows that $(F, R) = (E, S)$.

For the part (b), it suffices to observe that deleting a leaf l from (E, S) does not increase the minimal number of generators. If $G = \{\mathbf{g_1}, \ldots, \mathbf{g_k}\}$ is the minimal generating set of $G(E, S)$, then we can obtain the generating set of size k for $G((E, S) \setminus \{l\})$ by simply deleting the coordinate, which corresponds to the leaf l, from all generators in G. $\square$

4.3 Paths

This short section is devoted to determine the minimal number of semiring generators for parasemifields, which correspond to rooted paths.

Claim 4.10. *Let $P_n \overset{\text{def}}{=} v_1, \ldots, v_n$ be a rooted path with the root v_1. Then $m(P_n) = n + 1$.*

Proof. It follows from the definition of the operation $\vee$ that we have either $\mathbf{v} \vee \mathbf{w} = \mathbf{v}$ or $\mathbf{v} \vee \mathbf{w} = \mathbf{w}$ for any $\mathbf{v}, \mathbf{w} \in G(P_n)$. Therefore, the minimal number of semiring generators of $G(P_n)$ equals the minimal number of semigroup generators of $\mathbb{Z}^n$, which is $n + 1$ (see Claim 4.3). $\square$

Corollary 4.11. *Let (F, R) be a rooted forest of depth l. Then $m(F, R) \geq l + 1$.*

Proof. From the definition of the depth, we can find $w \in V(F)$ and $v \in R$ such that there is a path P from v to w consisting of l vertices. It follows that $(F, R) \succeq (P, v)$. Combining Observation 4.9(b) and Claim 4.10, we obtain that $m(F, R) \geq m(P, v) = l + 1$. $\square$

4.4 General forests

Let (F, R) be a general rooted forest. The aim of this section is to give bounds on $m(F, R)$, as tight as possible.

We have two parameters how to measure the size of (F, R), namely its depth and its arity. As we have seen in the previous sections, $m(F, R)$ grows at least linearly with the depth of (F, R) (see Corollary 4.11) but, on the other hand, rooted forests of arbitrary large arity can still have constant $m(F, R)$ (for example $m(Z_n) = 3$ for any $n \geq 3$, see Theorem 4.7). These thoughts led us to define a 'universal' rooted forest of arity k and depth l.

Definition 4.12. *Let k, l be natural numbers. We define T_{kl} to be a unique rooted forest satisfying that it has k roots, every internal vertex has exactly k children and every leaf has depth exactly l.*

For better understanding of the definition above, we give the following picture containing two examples of how T_{kl} looks like.
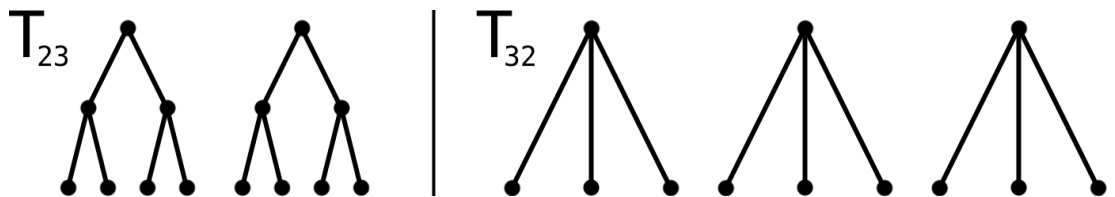

Figure 4.1: Rooted forests T_{23} and T_{32}

Observe that $G(F, R) \preceq T_{kl}$ for every k-ary rooted forest (F, R) of depth l, which implies that $m(F, R) \leq m(T_{kl})$ (Observation 4.9(b)). In order to give the upper bound on $m(F, R)$, we would like to estimate $m(T_{kl})$ from above. The first step is the following quite powerful theorem.

Theorem 4.13. *Let (F, R) be a rooted forest and let us construct a rooted forest (E, S) by a union of $m \geq 2$ disjoint copies of (F, R). Furthermore, let $k = m(F, R)$.*

(a) If $m = 2$, we have that $m(E, S) \leq k + 1$.

(b) For $m \geq 3$, we have that $m(E, S) \leq k + 2$.

Proof. Let $n = |V(F)|$ and $G = \{\mathbf{g_1}, \ldots, \mathbf{g_k}\} \in \mathbb{Z}^n$ be the minimal set of generators of $G(F, R)$. Throughout the proof, we are going to work with vectors from $(\mathbb{Z}^n)^m$ and we will denote $\mathbf{v} \in (\mathbb{Z}^n)^m$ by $(v_1, \ldots, v_n \mid v_{n+1}, \ldots, v_{2n} \mid \cdots \mid v_{(m-1)n+1}, \ldots, v_{mn})$.

We shall start with the part (a), when $m = 2$. Let us take a natural constant C such that $C > |g_{i,j}|$ for all $i \in [k], j \in [n]$. We are now ready to define the set $H = \{\mathbf{h_1}, \ldots, \mathbf{h_{k+1}}\}$ consisting of $k + 1$ vectors from $\mathbb{Z}^{2n}$. The first k of them are defined as $\mathbf{h_i} = (\mathbf{g_i} + 2\mathbf{C} \mid \mathbf{g_i} - 4\mathbf{C})$ and we let $\mathbf{h_{k+1}} = (-\mathbf{C} \mid 2\mathbf{C})$.

Our goal will be to show that we are able to generate any vector from $\mathbb{Z}^{2n}$ from the set H. By adding $2 \cdot \mathbf{h_{k+1}}$ to each $\mathbf{h_i}$, we obtain $(\mathbf{g_i} \mid \mathbf{g_i})$. Since G generates $G(F, R)$, we are able to obtain all vectors of the form $(\mathbf{v} \mid \mathbf{v})$ for any $\mathbf{v} \in \mathbb{Z}^n$, especially the vector $(-2\mathbf{C} \mid -2\mathbf{C})$.

Since C is large enough, we have that $\mathbf{h_i} \vee \mathbf{h_{k+1}} = (\mathbf{g_i} + 2\mathbf{C} \mid 2\mathbf{C})$. Adding $(-2\mathbf{C} \mid -2\mathbf{C})$ to $(\mathbf{g_i} + 2\mathbf{C} \mid 2\mathbf{C})$, we obtain $(\mathbf{g_i} \mid \mathbf{0})$ for each $i \in [k]$, which suffices to generate $(\mathbf{v} \mid \mathbf{0})$ for each $\mathbf{v} \in \mathbb{Z}^n$.

Any vector $(\mathbf{v} \mid \mathbf{w}) \in \mathbb{Z}^{2n}$ can be constructed by adding $(\mathbf{v} - \mathbf{w} \mid \mathbf{0})$ to $(\mathbf{w} \mid \mathbf{w})$, we are done with the first part.

For the part (b), we define the set $H = \{\mathbf{h_1}, \ldots, \mathbf{h_{k+2}}\}$ of $k + 2$ vectors from $(\mathbb{Z}^n)^m$ as follows:

$$\mathbf{h_i} = (\mathbf{g_i} \mid \mathbf{g_i} \mid \mathbf{g_i} \mid \cdots \mid \mathbf{g_i}), i \in [k]$$
$$\mathbf{h_{k+1}} = (\mathbf{1} \mid \mathbf{2} \mid \mathbf{3} \mid \cdots \mid \mathbf{m})$$
$$\mathbf{h_{k+2}} = (\mathbf{m^2 + 1 - 1^2} \mid \mathbf{m^2 + 1 - 2^2} \mid \mathbf{m^2 + 1 - 3^2} \mid \cdots \mid \mathbf{m^2 + 1 - m^2})$$
$$= (\mathbf{m^2} \mid \mathbf{m^2 - 3} \mid \mathbf{m^2 - 8} \mid \ldots \mid \mathbf{1}).$$

Our goal will be to prove that H is a generating set of $(\mathbb{Z}^n)^m$. As in the first part, we can use vectors $\mathbf{h_1}, \ldots, \mathbf{h_k}$ to generate $(\mathbf{v} \mid \cdots \mid \mathbf{v})$ for any $\mathbf{v} \in \mathbb{Z}^n$, especially the vector $\mathbf{c} = (-\mathbf{1} \mid \cdots \mid -\mathbf{1})$.

Since vectors $\{(1, 2, \ldots, m), (m^2, m^2 - 3, m^2 - 8, \ldots, 1), (-1, -1, \ldots, -1)\}$ were used to generate $\mathbb{Z}^m$ (see the proof of Theorem 4.7), we are able to use vectors $\mathbf{h_{k+1}}, \mathbf{h_{k+2}}, \mathbf{c}$ to generate $(\mathbf{c_1} \mid \mathbf{c_2} \mid \cdots \mid \mathbf{c_m})$ for any integers $c_1, \ldots, c_m$.

We finish the proof by generating any canonical vector $\mathbf{e_{ni+j}}$ for $i \in \{0, \ldots, m-1\}, j \in [n]$ and applying Observation 4.2. Let us take such arbitrary i and j. We generate a vector $\mathbf{t_i} = (-\mathbf{1} \mid \cdots \mid -\mathbf{1} \mid \mathbf{0} \mid -\mathbf{1} \mid \cdots \mid -\mathbf{1})$ such that $\mathbf{0}$ lies in the i-th copy of $G(F, R)$. We obtain the vector $\mathbf{u_{i,j}} = \mathbf{t_i} + (\mathbf{e_j} \mid \cdots \mid \mathbf{e_j})$ that has all n-tuples non-positive except for i-th tuple, which contains $\mathbf{e_j}$. We obtain $\mathbf{e_{ni+j}}$ as $\mathbf{u_{i,j}} \vee \mathbf{0}$. $\square$

Theorem 4.13 plays an important role in constructing the upper bound for $m(T_{kl})$ in the following theorem.

Theorem 4.14. *Let k, l be natural numbers. Then:*

(a) $m(T_{1l}) = l + 1$

(b) $l + 1 \leq m(T_{2l}) \leq 2l$

(c) $l + 1 \leq m(T_{kl}) \leq 3l$ for $k \geq 3$

Proof. For the part (a), it is enough to observe that T_{1l} is actually a path of length l and we know that $m(T_{1l}) = m(P_l) = l + 1$ (Claim 4.10).

Let us proof parts (b) and (c) together. The lower bound follows from Corollary 4.11, provided that the depth of T_{kl} is defined to be l.

We are going to proof the upper bound by an induction on l. If $l = 1$, then T_{k1} is formed by k isolated vertices (Z_k). We have already argued (Claim 4.4 and Theorem 4.7) that $m(Z_2) = 2$ and $m(Z_k) = 3$ for $k \geq 3$, which gives the upper bound for the base case, when $l = 1$.

We proof the inductive step only for the case (c), the other case (b) is proven in a similar manner. Let us suppose that $m(T_{kl}) \leq 3l$ and we want to show that $m(T_{k(l+1)}) \leq 3l + 3$.

As you can see on the following picture, we can construct $T_{k(l+1)}$ from T_{kl} in two simple steps. First, we connect all roots of T_{kl} to a new single root r creating the rooted tree U_{kl} and we obtain $T_{k(l+1)}$ as k disjoint copies of U_{kl}.
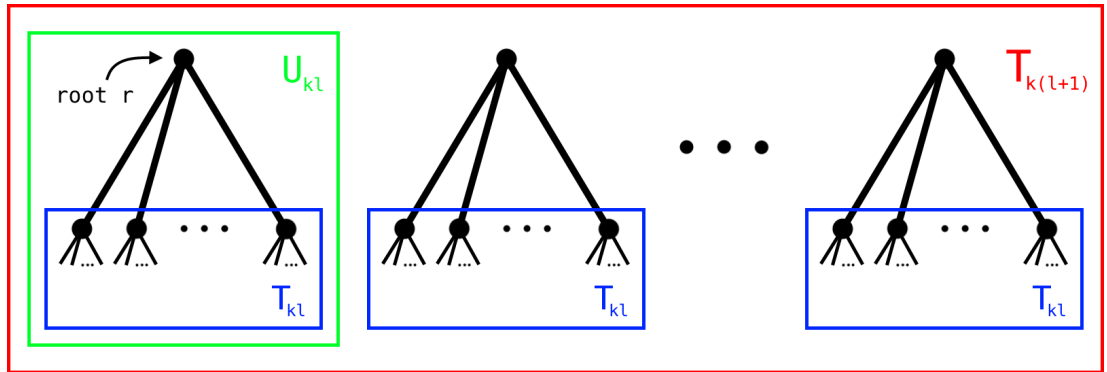

Figure 4.2: Construction of $T_{k(l+1)}$ from T_{kl}.

Let $n = |V(T_{kl})|$. We use the assumption $m(T_{kl}) \leq 3l$ to find a set $G = \{\mathbf{g_1}, \ldots, \mathbf{g_{3l}}\} \subseteq \mathbb{Z}^n$ that generates $G(T_{kl})$ as a semiring. We are going to show that $m(U_{kl}) \leq 3l + 1$ by finding its generating set $H = \{\mathbf{h_1}, \ldots, \mathbf{h_{3l+1}}\} \subseteq \mathbb{Z}^{n+1}$ consisting of $3l + 1$ vectors. We can assume that the first coordinate of these vectors corresponds to the root r of U_{kl}.

For any $i \in [3l]$, we let $\mathbf{h_i} = (-1, \mathbf{g_i})$ and we let $\mathbf{h_{3l+1}} = \mathbf{e_1}$. Adding the vector $\mathbf{h_{3l+1}}$ to each $\mathbf{h_i}$, we obtain $(0, \mathbf{g_i})$, which we can be used to generate $(0, \mathbf{w})$ for any $\mathbf{w} \in \mathbb{Z}^n$ (since G generates $G(T_{kl})$).

Let $(c, \mathbf{v}) \in \mathbb{Z}^{n+1}$ be an arbitrary vector, $c \in \mathbb{Z}, \mathbf{v} \in \mathbb{Z}^n$. If $c \geq 0$, we can obtain $(c, \mathbf{v})$ as $c \cdot \mathbf{h_{3l+1}} + (0, \mathbf{v})$. On the other hand, if $c < 0$, then we generate $(c, \mathbf{v})$ as $(-c) \cdot \mathbf{h_1} + (0, \mathbf{v} - c \cdot \mathbf{g_1})$, which finishes the proof that $m(U_{kl}) \leq 3l + 1$.

Since $T_{k(l+1)}$ is constructed by k disjoint copies of U_{kl}, the desired bound $m(T_{k(l+1)}) \leq 3l+3$ follows from Theorem 4.13 and already proven bound $m(U_{kl}) \leq 3l + 1$. $\qquad \square$

Now it only takes one last step to give bounds on $m(F, R)$ for a general rooted forest (F, R). We obtain a tighter upper bound for binary forests.

Theorem 4.15. *Let (F, R) be a rooted forest of depth l.*

(a) $l + 1 \leq m(F, R) \leq 3l$

(b) If (F, R) is a binary forest, we even have $l + 1 \leq m(F, R) \leq 2l$.

Proof. We proof both parts together. The lower bound follows from Corollary 4.11. Let us denote the arity of (F, R) by k. It is easy to see that $(F, R) \preceq T_{kl}$ and Observation 4.9(b) gives us that $m(F, R) \leq m(T_{kl})$. Combining that with the bounds on T_{kl} from Theorem 4.14, we obtain the result. $\qquad \square$

4.5 Remarks

We are aware of a simpler proof of the upper bound in Theorem 4.15(a) from Theorem 4.7. We are going to sketch the construction of a set G generating $G(F, R)$ such that $|G| \leq 3l$, where l is the depth of (F, R).

We split vertices of (F, R) into l disjoint subsets $V_1, \ldots, V_l$, where $V_i = \{v \in V(F) \mid$ depth of v is exactly $i\}$. For each V_i, we take (at most) three generators of $G(Z_{n_i})$, where $n_i = |V_i|$ (see Claim 4.4 and Theorem 4.7). We set the other coordinates (corresponding to vertices that do not belong to V_i) of those generators to zero and add them to G. It can be shown that such G generates $G(F, R)$.

However, we think that Theorem 4.13 is interesting on its own, so we have chosen (possibly) more complicated approach of proving Theorem 4.15 via bounding $m(T_{kl})$. Moreover, we have obtained the tighter bound for binary forests.

Unfortunately, we were not able to obtain the precise value of $m(F, R)$ for all rooted forests (F, R). The following question remains open for further studies.

Question 4.16. *Let $(F, R) \neq Z_n$ be a rooted forest of depth l. Does $m(F, R)$ equal $l + 1$?*

Note that $m(F, R) \geq l + 1$ follows from Corollary 4.11. For Question 4.16 to hold, it suffices to find a generating set of $G(F, R)$ of size $l + 1$. We were able to do so for several classes of rooted forests. We end this chapter by presenting these partial results.

We give a table of generating sets of parasemifields $G(F, R)$ such that (F, R) contains less than 5 vertices and $(F, R) \neq Z_n$.
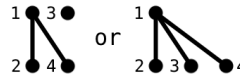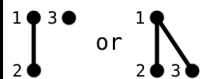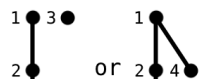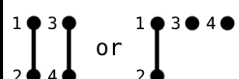
G(F,R)	depth	gen.set	G(F,R)	depth	gen.set
1• 2•	2	(1,0) (0,1) (-1,-1)	1•3• 2•4• or 1• 2•3•4•	2	(1,0,0,2) (-1,1,-2,-1) (-1,-2,1,-5)
1•3• 2• or 1• 2•3•	2	(1,0,0) (-1,1,-2) (-1,-2,1)	1•3• 2• 3• or 1• 2•4• 3•	3	(1,0,0,0) (-1,1,0,0) (-1,-1,1,-2) (-1,-1,-2,1)
1• 2• 3•	3	(1,0,0) (0,1,0) (0,0,1) (-1,-1,-1)	1• 2• 3• 4•	4	(1,0,0,0) (0,1,0,0) (0,0,1,0) (0,0,0,1) (-1,-1,-1,-1)
1•3• 2•4• or 1•3•4• 2•	2	(-1,0,-2,-2) (0,1,1,0) (-2,-2,0,1)			

Figure 4.3: Generators of $G(F,R)$ for $(F,R) \neq Z_n$, $|V(F)| < 5$.

We have shown that Question 4.16 holds for small rooted forests. We are going to look at rooted forests that are formed by a couple of rooted paths and we will answer Question 4.16 for some of them.

Notation 4.17. *For natural numbers k, n, let us denote by kP_n the rooted forest formed by k disjoint copies of a rooted path P_n.*

Theorem 4.18. *Let k, n be natural numbers and $k \leq (n+1)$. Then there exists a set of $n+1$ generators of $G(kP_n)$. Consequently, $m(kP_n) = n+1$.*

Proof. It suffices to proof the theorem for $k = n+1$. Elements from $G((n+1)P_n)$ are vectors from $(\mathbb{Z}^n)^{n+1}$ which will be denoted as $\mathbf{v} = (v_1, \ldots, v_n \mid v_{n+1} \ldots v_{2n} \mid \cdots \mid v_{n^2+1} \ldots v_{n^2+n})$.

We define the set $G = \{\mathbf{g_1}, \ldots, \mathbf{g_{n+1}}\}$ of $n+1$ vectors from $(\mathbb{Z}^n)^{n+1}$ as follows:

$$\mathbf{g_1} = (-\mathbf{2} \mid \mathbf{e_1} \mid \mathbf{e_1} \mid \cdots \mid \mathbf{e_1} \mid \mathbf{e_1})$$
$$\mathbf{g_2} = (\mathbf{e_2} \mid -\mathbf{2} \mid \mathbf{e_2} \mid \cdots \mid \mathbf{e_2} \mid \mathbf{e_2})$$
$$\vdots \qquad\qquad \ddots$$
$$\mathbf{g_n} = (\mathbf{e_n} \mid \mathbf{e_n} \mid \mathbf{e_n} \mid \cdots \mid -\mathbf{2} \mid \mathbf{e_n})$$
$$\mathbf{g_{n+1}} = (\mathbf{e_1} \mid \mathbf{e_2} \mid \mathbf{e_3} \mid \cdots \mid \mathbf{e_n} \mid -\mathbf{2}).$$

We are going to show that G generates $G((n+1)P_n)$. Let us start with generating two important vectors.

$$-\mathbf{1} = \mathbf{g_1} + \mathbf{g_2} + \cdots + \mathbf{g_{n+1}}$$
$$\mathbf{0} = (\mathbf{g_1} \vee 2 \cdot \mathbf{g_1}) + (\mathbf{g_2} \vee 2 \cdot \mathbf{g_2}) + \cdots + (\mathbf{g_{n+1}} \vee 2 \cdot \mathbf{g_{n+1}})$$

We will finish the proof by generating all the canonical vectors $\mathbf{e_{ni+j}}$ (for $i \in \{0, \ldots, n\}$ and $j \in [n]$) and applying Observation 4.2. If $i \neq j$, we first generate the vector $\mathbf{v_{ij}}$ as follows.

$$\mathbf{v_{ij}} = \mathbf{g_i} + 3 \cdot \mathbf{g_j} + \sum_{k \notin \{i,j\}} (2 \cdot \mathbf{g_k})$$

$$= \mathbf{g_j} - \mathbf{g_i} + 2 \sum_{k=1}^{n+1} \mathbf{g_k}$$

$$= -\mathbf{2} + \mathbf{g_j} - \mathbf{g_i}$$

Observe that the vector $\mathbf{v_{ij}}$ contains $\mathbf{e_j}$ in i-th n-tuple and other n-tuples contain a non-positive vector. It follows that $\mathbf{e_{ni+j}} = \mathbf{v_{ij}} \vee \mathbf{0}$.

The approach in the case when $i = j$ is similar. We generate:

$$\mathbf{w_i} = \mathbf{g_i} + 3 \cdot \mathbf{g_{n+1}} + \sum_{k \notin \{i,n+1\}} (2 \cdot \mathbf{g_k})$$

$$\mathbf{e_{ni+i}} = \mathbf{w_i} \vee \mathbf{0}$$

and we are done. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

It can also be shown that $m(kP_2) = 3$ for any $k \in \mathbb{N}$, using the generating set of $G(Z_{2k})$ from Theorem 4.7. The proof is similar to the proof of Theorem 4.7 but slightly more technical.

5. The classification of finitely generated semifields

This chapter is devoted to study semifields that are finitely generated as a semiring (fg-semifields for brevity). Let us restate the classification of semifields (Theorem 2.18) for the case of finitely generated semifields to obtain four distinct types of them.

Theorem 5.1. *Let S be a fg-semifield. Then one of the following cases occurs:*

(1) S is a finite field.

(2) S is constructed from a fg-parasemifield P by adding an element 0 and letting $0 + s = s$ and $0s = 0$ for every $s \in S$.

(3) S is constructed from a finitely generated multiplicative abelian group $A(\cdot)$ by adding an element 0 and letting $s + t = 0$ and $0s = 0$ for every $s, t \in S$.

(4) S is constructed from a fg-parasemifield $P(+, \cdot)$ as follows. Let $P(\cdot)$ be a subgroup of a finitely generated abelian group $A(\cdot)$ and let $S = A \cup \{0\}$ and $S0 = \{0\}$. We define addition for any $x, y \in S$ as follows:

$$x + 0 = 0$$
$$x^{-1}y \notin P : x + y = 0$$
$$x^{-1}y \in P : x + y = (x^{-1}y + 1) \cdot x.$$

Proof. The statement basically follows from Theorem 2.18. It remains to show that those structures are finitely generated (and finite in the case (1)).

(1) A field that is finitely generated as a semiring is also finitely generated as a ring. It is a classical result that such field has to be finite (an elementary proof is contained in [Ježek et al., 2012, Section 2]).

(2) Let us suppose that S is generated by a finite set G. Since $0+s = s$ and $0s = 0$ for every $s \in S$, we have that T is finitely generated by the set $G \setminus \{0\}$.

(3) The proof that A is a finitely generated group is similar as in the previous case (2).

(4) It holds that semifield S of type (4) is finitely generated as a semiring if and only if P is fg-parasemifield and the factorgroup $(A/P)(\cdot)$ is finitely generated [Kala and Kepka, 2008, Lemma 4.4.5]. From Corollary 3.6, we have that $P(\cdot) \simeq \mathbb{Z}^n(+)$ is a finitely generated group. Altogether, we obtain that $A(\cdot)$ is a finitely generated group (see Observation 1.15).

$\square$

As a result, we obtain the following corollary, which might be quite surprising.

Corollary 5.2. *Let S be an ideal-simple semiring that is finitely generated. Then S is finitely generated as a multiplicative semigroup.*

Proof. From the first classification of ideal-simple semifields (Theorem 2.8), we have that S is either isomorphic to $\mathbb{Z}_p$ with zero-multiplication (which is finite and thus finitely generated as a multiplicative semigroup), or a fg-parasemifield or a fg-semifield.

Corollary 3.6 states that fg-parasemifields are finitely generated as a multiplicative semigroup, implying that fg-semifields of type (3) are also. The statement also holds for fg-semifields of three remaing types, as they are either finite (type (1)) or obtained by adding one element to a finitely generated abelian group (type (2) and type (4) from Theorem 5.1). □

The fg-semifields of types (1) and (3) are constructed from well-known structures (finite fields and finitely generated abelian groups), so they are not that interesting for further study. We are going to study the fg-semifields that arise from fg-parasemifields (type (2) and type (4)) and apply the classification of fg-parasemifields described in Chapter 3.

Let us start with an easier case, when S is a fg-semifield of type (2), $S = P \cup \{0\}$ for a fg-parasemifield P. We use Theorem 3.5 (the classification of fg-parasemifields) to find a rooted forest (F, R) on m vertices such that $P \simeq G(F, R)$. The element 0 has to satisfy that, for every $\mathbf{v} \in \mathbb{Z}^m$, we have that $0 \vee \mathbf{v} = \mathbf{v}$ and $0 + \mathbf{v} = 0$, so 0 plays the role of the vector $(-\infty, \ldots, -\infty)$.

5.1 Finitely-generated semifields of type (4)

We turn our attention to fg-semifields of type (4) that have more complicated structure. Recall that fg-semifield $S(+, \cdot)$ of type (4) is constructed from a finitely generated abelian group $A(\cdot)$ that has fg-parasemifield $P(+, \cdot)$ as a multiplicative subgroup.

Our goal will be to modify the structure of $A(\cdot)$ to have the better understanding of what is going on. From the classification of finitely generated abelian groups (Theorem 1.17), we may without loss of generality assume that $A = \mathbb{Z}^n \oplus T$, where $T = \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_k}$ is the torsion part and $q_1, \ldots, q_k$ are prime powers.

We again use Theorem 3.5 to find a rooted forest (F, R) on m vertices such that $P \simeq G(F, R)$. It follows that $P(\cdot) \simeq \mathbb{Z}^m(+)$ is a free group of rank m that is also a multiplicative subgroup of $A(\cdot)$. Thus, we can, for each $i \in [m]$, find $\mathbf{b_i} \in \mathbb{Z}^n$ and $\mathbf{t_i} \in T$ such that $P = \langle \mathbf{p_1}, \ldots, \mathbf{p_m} \rangle$ for $\mathbf{p_i} = (\mathbf{b_i} \mid \mathbf{t_i})$ and that $\mathbf{p_i} \in P$ corresponds to $\mathbf{e_i} \in G(F, R)$. Let us present a useful observation.

Observation 5.3. *If* $(\mathbf{b} \mid \mathbf{t}), (\mathbf{b} \mid \mathbf{u}) \in P$, *then* $\mathbf{t} = \mathbf{u}$.

Proof. For contradiction, suppose that $\mathbf{t} \neq \mathbf{u}$ and let $\mathbf{v} = \mathbf{t} - \mathbf{u}$. Since both $(\mathbf{b} \mid \mathbf{t})$ and $(\mathbf{b} \mid \mathbf{u})$ lie in P, their difference $(\mathbf{0} \mid \mathbf{v})$ has to lie in P as well. Since P is generated by the set $\{\mathbf{p_1} \ldots, \mathbf{p_m}\}$, we can find integers $k_1, \ldots, k_m$ such that:

$$\sum_{i=1}^{m} k_i \cdot \mathbf{p_i} = (\mathbf{0} \mid \mathbf{v}). \tag{5.1}$$

We have that $T = \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_k}$. Let $q = q_1 \cdot \cdots \cdot q_k$ and observe that $q \cdot \mathbf{v} = \mathbf{0}$ for every $\mathbf{v} \in T$. Multiplying Equation 5.1 by q, we obtain a non-trivial combination

of the zero vector:

$$\sum_{i=1}^{m} q k_i \cdot \mathbf{p_i} = (\mathbf{0} \mid q \cdot \mathbf{v}) = \mathbf{0} \tag{5.2}$$

which is a contradiction with the fact that P is a free group and the expression of its elements from the basis should be unique. $\qquad \square$

Let $B \stackrel{\text{def}}{=} \{\mathbf{b} \in \mathbb{Z}^n \mid \exists \mathbf{t} \in T : (\mathbf{b} \mid \mathbf{t}) \in P\}$ be a subgroup of $\mathbb{Z}^n$.

Claim 5.4. *We claim that $B = \langle \mathbf{b_1}, \ldots, \mathbf{b_m} \rangle$.*

Proof. Since $P = \langle (\mathbf{b_1} \mid \mathbf{t_1}), \ldots, (\mathbf{b_m} \mid \mathbf{t_m}) \rangle$, it is clear that B is a subgroup of $\mathbb{Z}^n$ generated by $\{\mathbf{b_1}, \ldots, \mathbf{b_m}\}$.

For contradiction, suppose $\mathbf{b} \in B$ is not uniquely expressed, i.e., we can find $\mathbf{k} \neq \mathbf{l} \in \mathbb{Z}^m$ such that $\mathbf{b} = \sum_{i=1}^{m} k_i \cdot \mathbf{b_i} = \sum_{i=1}^{m} l_i \cdot \mathbf{b_i}$. Let $(\mathbf{b} \mid \mathbf{t}) = \sum_{i=1}^{m} k_i \cdot \mathbf{p_i}$ and $(\mathbf{b} \mid \mathbf{u}) = \sum_{i=1}^{m} l_i \cdot \mathbf{p_i}$ be two elements in P. Observation 5.3 gives us that $\mathbf{t} = \mathbf{u}$. Therefore, $\sum_{i=1}^{m} k_i \cdot \mathbf{p_i}$ and $\sum_{i=1}^{m} l_i \cdot \mathbf{p_i}$ are two expressions of the same element $(\mathbf{b} \mid \mathbf{t})$ in the free group P, implying that $\mathbf{k} = \mathbf{l}$, contradiction. $\qquad \square$

We have shown that B is a free group of rank m and moreover, B is a subgroup of $\mathbb{Z}^n$. We can now apply Theorem 1.19 to find a basis $\{\mathbf{a_1}, \ldots, \mathbf{a_n}\}$ of $\mathbb{Z}^n$ and natural numbers $d_1 \mid d_2 \mid \cdots \mid d_m$ such that $B = \langle d_1 \cdot \mathbf{a_1}, \ldots, d_m \cdot \mathbf{a_m} \rangle$.

5.1.1 Simpler case

First, let us consider the case, when $d_1, \ldots, d_m = 1$, which implies that $B = \langle \mathbf{b_1}, \ldots, \mathbf{b_m} \rangle = \langle \mathbf{a_1}, \ldots, \mathbf{a_m} \rangle$ and that $\mathbb{Z}^n = \langle \mathbf{a_1}, \ldots, \mathbf{a_n} \rangle$. We obtain that $\mathbb{Z}^n$ has the basis $\{\mathbf{b_1}, \ldots, \mathbf{b_m}, \mathbf{a_{m+1}}, \ldots, \mathbf{a_n}\}$ and we can let $\mathbf{b_i} = \mathbf{a_i}$ for $i \in \{m+1, \ldots, n\}$.

Since $\{\mathbf{b_1}, \ldots, \mathbf{b_n}\}$ is the basis of $\mathbb{Z}^n$, we can apply the following change of coordinates $h : A \to A$ defined as $h(\mathbf{b} \mid \mathbf{t}) = h(\sum_{i=1}^{m} k_i \cdot \mathbf{b_i} \mid \mathbf{t}) = (k_1, \ldots, k_n \mid \mathbf{t})$. It is easy to observe (from the definition of a basis) that h is a well-defined isomorphism of groups. Furthermore, note that $h(\mathbf{p_i}) = h(\mathbf{b_i} \mid \mathbf{t_i}) = (\mathbf{e_i} \mid \mathbf{t_i})$. Thus, we will without loss of generality assume that $P = \langle \mathbf{p_1}, \ldots, \mathbf{p_m} \rangle$ for $\mathbf{p_i} = (\mathbf{e_i} \mid \mathbf{t_i})$.

We apply one more change of coordinates $j : A \to A$, which is defined as follows. We view A as $\mathbb{Z}^m \oplus \mathbb{Z}^{(n-m)} \oplus T$ and let $j(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}) = (\mathbf{x} \mid \mathbf{y} \mid \mathbf{z} - t(\mathbf{x}))$, where $t : \mathbb{Z}^m \to T$ is the following homomorphism: $t(\mathbf{x}) = \sum_{i=1}^{m} x_i \cdot \mathbf{t_i}$.

Observation 5.5. *The map $j : A \to A$ defined above is a group isomorphism.*

Proof. Since t is a group homomorphism, j is as well. For the injectivity of j, let us assume that $j(\mathbf{u} \mid \mathbf{v} \mid \mathbf{w}) = j(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z})$. Componentwise, we obtain that:

$$\mathbf{u} = \mathbf{x} \tag{5.3}$$
$$\mathbf{v} = \mathbf{y} \tag{5.4}$$
$$\mathbf{w} - t(\mathbf{u}) = \mathbf{z} - t(\mathbf{x}). \tag{5.5}$$

From Equation 5.3 we have that $t(\mathbf{u}) = t(\mathbf{x})$. Adding that to Equation 5.5, we have $\mathbf{w} = \mathbf{z}$, the injectivity follows.

Let $(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z})$ be an arbitrary element from A. The surjectivity follows from the following equation: $j(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z} + t(\mathbf{x})) = (\mathbf{x} \mid \mathbf{y} \mid \mathbf{z})$. $\qquad \square$

We see that $j(\mathbf{p_i}) = j(\mathbf{e_i} \mid \mathbf{0} \mid \mathbf{t_i}) = (\mathbf{e_i} \mid \mathbf{0} \mid \mathbf{0})$, so we can without loss of generality assume that $\mathbf{p_i} = (\mathbf{e_i} \mid \mathbf{0} \mid \mathbf{0})$. Therefore, we have that $A = P \oplus \mathbb{Z}^{(n-m)} \oplus T$ and that A is formed by a direct product of P and a finitely generated abelian group G, in this case $G = \mathbb{Z}^{(n-m)} \oplus T$. Combining that with the definition of semifields of type (4) from Theorem 5.1, we obtain the following classification.

Theorem 5.6. *Let S be a fg-semifield of type (4) and moreover suppose that $d_1, \ldots, d_m = 1$. Then we can find a fg-parasemifield $P \simeq G(F, R)$ and a finitely generated abelian group $G(+)$ such that $S \simeq P \oplus G \cup \infty$. We set $s + \infty = \infty$ and $s \cdot \infty = \infty$. The binary operations on two arbitrary elements $(\mathbf{u} \mid g)$ and $(\mathbf{v} \mid h)$ from $G(F, R) \oplus G$ are defined as follows:*

$$g \neq h : (\mathbf{u} \mid g) + (\mathbf{v} \mid h) = \infty$$
$$(\mathbf{u} \mid g) + (\mathbf{v} \mid g) = (\mathbf{u} \vee \mathbf{v} \mid g)$$
$$(\mathbf{u} \mid g) \cdot (\mathbf{v} \mid h) = (\mathbf{u} + \mathbf{v} \mid g + h).$$

5.1.2 General case

We assume that $(d_1, \ldots, d_m) \neq \mathbf{1}$. Recall that $B = \langle \mathbf{b_1}, \ldots, \mathbf{b_m} \rangle = \langle d_1 \cdot \mathbf{a_1}, \ldots, d_m \cdot \mathbf{a_m} \rangle$ and that $\mathbb{Z}^n = \langle \mathbf{a_1}, \ldots, \mathbf{a_n} \rangle$.

Unfortunately, we are not able to classify semifields of type (4) completely. We are going to present a partial result concerning semifields of type (4) that satisfy the following assumption.

Assumption 5.7. *Let us assume that we can find natural numbers $d_1, \ldots, d_m$ and a basis $\{\mathbf{a_1}, \ldots, \mathbf{a_n}\}$ of $\mathbb{Z}^n$ such that $\mathbf{b_i} = d_i \cdot \mathbf{a_i}$ for every $i \in [m]$.*

Note that Assumption 5.7 does not have not be satisfied in general. For example, let $\mathbf{b_1} = (2, 1), \mathbf{b_2} = (4, 3)$. Since coordinates of vectors $\mathbf{b_1}, \mathbf{b_2}$ are co-prime, it holds that $d_1 = d_2 = 1$. But $\{\mathbf{a_1}, \mathbf{a_2}\} = \{\mathbf{b_1}, \mathbf{b_2}\}$ is not a basis of $\mathbb{Z}^2$, as the first coordinate is even for all generated vectors.

Similarly as in the simpler case (when $d_1, \ldots, d_m = 1$), we can apply a change of coordinates $h : A \to A$ defined as $h(\mathbf{b} \mid \mathbf{t}) = h(\sum_{i=1}^m k_i \cdot \mathbf{a_i} \mid \mathbf{t}) = (k_1, \ldots, k_n \mid \mathbf{t})$ and we can without generality assume that $P = \langle d_i \cdot \mathbf{e_i} \mid \mathbf{t_i} \rangle$.

We are able to view a semifield S of type (4) as an abelian group $A \simeq \mathbb{Z}^m \oplus \mathbb{Z}^{(n-m)} \oplus T$ with an added element ∞ (that corresponds to the zero semifield element). The multiplication in semifields of type (4) is inherited from the group operation in A which is a coordinate-wise addition on A (denoted by $+$). Moreover, we insist that $\infty + s = \infty$.

The addition in semifields of type (4) will be denoted by $\vee$ and looks as follows (see Theorem 5.1): for $\mathbf{g} = (\mathbf{u} \mid \mathbf{v} \mid \mathbf{w}) \in A$ and $\mathbf{h} = (\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}) \in A$, we should set $\mathbf{g} \vee \mathbf{h} = ((\mathbf{h} - \mathbf{g}) \vee \mathbf{0}) + \mathbf{g}$ if $\mathbf{h} - \mathbf{g} \in P$ and we set $\mathbf{g} \vee \mathbf{h} = \infty$ otherwise. Note that $(\mathbf{h} - \mathbf{g}) \vee \mathbf{0}$ is computed in the parasemifield $P \simeq G(F, R)$.

For every $i \in [m]$, let us take unique integers k_i, l_i, r_i, s_i such that $0 \leq r_i, s_i \leq d_i - 1$ and that the following equations are satisfied:

$$u_i = k_i d_i + r_i$$
$$x_i = l_i d_i + s_i.$$

We are now going to find the conditions for $\mathbf{h} - \mathbf{g}$ to belong in $P = \langle (d_i \cdot \mathbf{e_i} \mid \mathbf{0} \mid \mathbf{t_i}), i \in [m] \rangle$. That is indeed equivalent to finding $\mathbf{j} \in \mathbb{Z}^m$ such that $\mathbf{h} - \mathbf{g} = (j_1 d_1, \ldots, j_m d_m \mid \mathbf{0} \mid \sum_{i=1}^m j_i \cdot \mathbf{t_i})$. Note that $\mathbf{h} - \mathbf{g} = (\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}) - (\mathbf{u} \mid \mathbf{v} \mid \mathbf{w}) = ((d_1(l_1 - k_1) + r_1 - s_1), \ldots, (d_m(l_m - k_m) + r_m - s_m) \mid \mathbf{y} - \mathbf{v} \mid \mathbf{z} - \mathbf{w})$.

Comparing the coordinates of $(j_1 d_1, \ldots, j_m d_m \mid \mathbf{0} \mid \sum_{i=1}^m j_i \cdot \mathbf{t_i})$ and $(d_1(l_1 - k_1) + r_1 - s_1, \ldots, d_m(l_m - k_m) + r_m - s_m \mid \mathbf{y} - \mathbf{v} \mid \mathbf{z} - \mathbf{w})$, we demand that:

$$\forall i \in [m] : d_i j_i = d_i(l_i - k_i) + r_i - s_i \Rightarrow j_i = k_i - l_i, r_i = s_i$$

$$\mathbf{y} - \mathbf{v} = \mathbf{0} \Rightarrow \mathbf{y} = \mathbf{v}.$$

Let us define the function $t : \mathbb{Z}^m \to T$ as $t(x_1, \ldots, x_m) = \sum_{i=1}^m \lfloor \frac{x_i}{d_i} \rfloor \cdot \mathbf{t_i}$. Finally, comparing the torsion parts and applying the definition of the map t gives us that:

$$\mathbf{z} - \mathbf{w} = \sum_{i=1}^m j_i \cdot \mathbf{t_i} = \sum_{i=1}^m (l_i - k_i) \cdot \mathbf{t_i} = \sum_{i=1}^m l_i \cdot \mathbf{t_i} - \sum_{i=1}^m k_i \cdot \mathbf{t_i} = t(\mathbf{x}) - t(\mathbf{u})$$

which holds if and only if we can find $\mathbf{t} \in T$ such that

$$\mathbf{w} = t(\mathbf{u}) + \mathbf{t}, \mathbf{z} = t(\mathbf{x}) + \mathbf{t}.$$

Assume that the conditions above are met, i.e., $\mathbf{s} = \mathbf{r}$, $\mathbf{y} = \mathbf{v}$ and $\mathbf{w} = t(\mathbf{x}) + \mathbf{t}, \mathbf{z} = t(\mathbf{u}) + \mathbf{t}$. We shall look at the element $(\mathbf{h} - \mathbf{g}) \vee \mathbf{0}$. We have that $\mathbf{h} - \mathbf{g} = ((l_1 - k_1)d_1, \ldots, (l_m - k_m)d_m \mid \mathbf{0} \mid \sum_{i=1}^m (l_i - k_i) \cdot \mathbf{t_i}) = \sum_{i=1}^m (l_i - k_i) \cdot \mathbf{p_i}$, which corresponds to the vector $\mathbf{l} - \mathbf{k} \in G(F, R)$ (recall that $\mathbf{p_i} \in P$ was defined to correspond to $\mathbf{e_i} \in G(F, R)$).

We use structure of the rooted forest (F, R) to compute $\mathbf{m} = (\mathbf{l} - \mathbf{k}) \vee \mathbf{0}$ that corresponds to $(\mathbf{h} - \mathbf{g}) \vee \mathbf{0} = (m_1 d_1, \ldots m_m d_m \mid \mathbf{0} \mid \sum_{i=1}^m m_i \cdot \mathbf{t_i})$ in A.

From the definition of $\vee$ in $G(F, R)$, we have either $m_i = l_i - k_i$ or $m_i = 0$, for each $i \in [m]$. We can thus decompose $[m]$ into two subsets I and J such that $I = \{i \in [m] \mid m_i = 0\}$ and $J = \{i \in [m] \mid m_i = l_i - k_i\}$.

We obtain $\mathbf{g} \vee \mathbf{h}$ by adding $\mathbf{g}$ to $((\mathbf{h} - \mathbf{g}) \vee \mathbf{0})$. We have observed that:

$$\mathbf{g} = \left(k_1 d_1 + r_1, \ldots, k_m d_m + r_m \mid \mathbf{v} \mid \mathbf{t} + \sum_{i=1}^m k_i \cdot \mathbf{t_i} \right)$$

$$(\mathbf{h} - \mathbf{g}) \vee \mathbf{0} = \left(m_1 d_1, \ldots, m_m d_m \mid \mathbf{0} \mid \sum_{i=1}^m m_i \cdot \mathbf{t_i} \right).$$

Summing these equations up, we obtain that:

$$\mathbf{g} \vee \mathbf{h} = (\mathbf{n} \mid \mathbf{v} \mid \mathbf{t} + t(\mathbf{n})),$$

where $\mathbf{n}$ is the following vector: $n_i = u_i$ for $i \in I$ and $n_i = x_i$ for $i \in J$.

Finally, let us observe that for every $i \in [m]$ we have that:

$$u_i \geq x_i \Leftrightarrow d_i k_i + r_i \geq d_i l_i + r_i \Leftrightarrow k_i \geq l_i$$

which implies that $\mathbf{n} = \mathbf{u} \vee \mathbf{w}$, when we inherit the structure of rooted forest from $P \simeq G(F, R)$. Consequently:

$$\mathbf{g} \vee \mathbf{h} = (\mathbf{u} \mid \mathbf{v} \mid \mathbf{t} + t(\mathbf{u})) \vee (\mathbf{x} \mid \mathbf{v} \mid \mathbf{t} + t(\mathbf{x})) = (\mathbf{u} \vee \mathbf{x} \mid \mathbf{v} \mid \mathbf{t} + t(\mathbf{u} \vee \mathbf{x})).$$

To sum up, we have just proven the following theorem.

Theorem 5.8. *Let S be a fg-semifield of type (4) and let Assumption 5.7 be satisfied. Then, we can find a fg-abelian group $G = \mathbb{Z}^n \oplus T$ such that $T = \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_k}$, where $q_1, \ldots, q_k$ are prime powers. Moreover, we can find a rooted forest (F, R) consisting of m vertices, natural numbers $d_1, \ldots, d_m$ and $\mathbf{t_1}, \ldots, \mathbf{t_m} \in T$ such that $S \simeq G(F, R) \times G \cup \{\infty\}$.*

We set $s + \infty = \infty$ and $s \cdot \infty = \infty$ for every $s \in S$. The binary operations on two arbitrary elements $\mathbf{g} = (\mathbf{u} \mid \mathbf{v} \mid \mathbf{w})$ and $\mathbf{h} = (\mathbf{x} \mid \mathbf{y} \mid \mathbf{z})$ from $G(F, R) \oplus \mathbb{Z}^n \oplus T$ are defined as follows:

$$\mathbf{g} \cdot \mathbf{h} = (\mathbf{u} + \mathbf{x} \mid \mathbf{v} + \mathbf{y} \mid \mathbf{w} + \mathbf{z}).$$

If the following three conditions

(1) d_i divides $x_i - u_i$ for each $i \in [m]$

(2) $\mathbf{v} = \mathbf{y}$

(3) we can find $\mathbf{t} \in T$ such that $\mathbf{w} = \mathbf{t} + t(\mathbf{u})$ and $\mathbf{z} = \mathbf{t} + t(\mathbf{x})$, where $t(\mathbf{x}) = \sum_{i=1}^{m} \lfloor \frac{x_i}{d_i} \rfloor \cdot \mathbf{t_i}$

are met, then we let

$$\mathbf{g} + \mathbf{h} = (\mathbf{u} \vee \mathbf{x} \mid \mathbf{v} \mid \mathbf{t} + t(\mathbf{u} \vee \mathbf{x}))$$

and we set $\mathbf{g} + \mathbf{h} = \infty$ otherwise.

The theorem above classifies another interesting subclass of semifields of type (4). The general case remains open for further studies. However, we think that the resulting classification will be similar to Theorem 5.8.

Bibliography

Robert Bashir, Jan Hurt, Antonín Jančařík, and Tomáš Kepka. Simple commutative semirings. *Journal of Algebra*, 236(1):277–306, 2001.

David Dummit and Richard Foote. *Abstract algebra (2nd edition)*. John Wiley, 1999.

Jaroslav Ježek, Vítězslav Kala, and Tomáš Kepka. Finitely generated algebraic structures with various divisibility conditions. *Forum Mathematicum*, 24(2): 379–397, 2012.

Vítězslav Kala. Lattice-ordered abelian groups finitely generated as semirings. *Journal of Commutative Algebra*, 9(3):387–412, 2017.

Vítězslav Kala and Tomáš Kepka. A note on finitely generated ideal-simple commutative semirings. *Commentationes Mathematicae Universitatis Carolinae*, 49(1):1–9, 2008.

Vítězslav Kala and Miroslav Korbelář. Idempotence of finitely generated commutative semifields. *Forum Mathematicum*, 30(6):1461–1474, 2018.

Joseph Rotman. *An Introduction to the Theory of Groups*. Springer New York, 1999.