Idempotency in commutative semirings

Miroslav Korbelář
(a joint work with V. Kala)

Masaryk University in Brno, Czech Republic

miroslav.korbelar@gmail.com

SSAOS 2014
Stará Lesná, September 2014

This work was supported by the Grant Agency of Czech Republic

by the grant GP13-29835P.

All structures in this talk are assumed to be commutative.

Basic definitions

A (commutative) *semiring* $(S, +, \cdot)$ is an algebraic structure with two binary operations " $+$ " and " $\cdot$ " such that

- $(S, +)$ is a commutative semigroup
- $(S, \cdot)$ is a commutative semigroup
- $a(b + c) = ab + ac$ for every $a, b, c \in S$.

S is called a *parasemifield* iff (moreover) $(S, \cdot)$ is a group.

Let $\emptyset \neq M \subseteq \mathbb{N}$ be a set. An element $a \in S$ is called

- *M-divisible (in S)* $\Leftrightarrow (\forall n \in M)(\exists b \in S)\ a = \underbrace{b + \cdots + b}_{n-times}$.

  (If $M = \mathbb{N}$ we call it *divisible (in S)*.)
- *torsion* $\Leftrightarrow$ the semigroup $(\mathbb{N} \cdot a, +)$ is finite.
- *idempotent* $\Leftrightarrow a + a = a$.

S is *divisible* (*idempotent*, resp.) iff every element of S is so.

Conjectures

Let S be a finitely generated semiring. Then S is additively idempotent if:

(1) S is a parasemifield. ('08)

(2) S has a unit and is additively divisible. ('10)

(3) S is additively divisible. ('10)

Confirmed cases (n is the number of generator of S):

- (1): $n = 1$ (Kala, Kepka, K. '09), $n = 2$ (Ježek, Kala, Kepka '12), $n = 3, \ldots$ (Kala, K. '14)
- (2) & (3): $n = 1$ (K., Landsmann '13)

Equivalent versions of conjectures

Let S be a finitely generated semiring.

(1) S does not contain $(\mathbb{Q}^+, +, \cdot)$, if it is a parasemifield.

(2) S does not contain $(\mathbb{Q}^+, +, \cdot)$.

Conjectures - computational versions

(2) Let $k \in \mathbb{N}$ and $\{f_n|\ n \in \mathbb{N}\} \subseteq \mathbb{N}[x_1, \ldots, x_k]$ be a set of polynomials. The system of relations

$$1 \equiv n \cdot f_n(x_1, \ldots, x_k) \text{ where } n \in \mathbb{N}$$

implies relation $1 \equiv 2$ by using only addition and multiplication in $\mathbb{N}[x_1, \ldots, x_k]$.

(3) Let $k \in \mathbb{N}$ and $\{f_{i,n}|\ n \in \mathbb{N}\ \&\ i = 1, \ldots, k\} \subseteq \mathbb{N}[x_1, \ldots, x_k]$ be a set of polynomials that have zero constant terms. The system of relations

$$x_i \equiv n \cdot f_{i,n}(x_1, \ldots, x_k) \text{ where } n \in \mathbb{N},\ \ i = 1, \ldots, k$$

implies relations $x_i \equiv 2 \cdot x_i$ for all $i = 1, \ldots, k$ by using only addition and multiplication in $\mathbb{N}[x_1, \ldots, x_k]$.

One more conjecture:

Theorem (folklore)

Let A be a finitely generated semigroup.
If the semigroup A is divisible, then A is idempotent.

Conjecture (4)

Let M be a finitely generated S-semimodule over a finitely generated semiring S.
If the semigroup M is divisible, then M is idempotent.

Confirmed for both M and S having one generator. (Landsmann, K. '13)

Conjecture (4) symbolically

The system of relations (within $\mathbb{N}_0[m_1, \ldots, m_p, x_1, \ldots, x_k]$):

$$m_i \equiv n \cdot \Big(f_{i,n,1}(x_1, \ldots, x_k) \cdot m_1 + \cdots + f_{i,n,p}(x_1, \ldots, x_k) \cdot m_p \Big),$$

$$m_i \cdot m_j \equiv 0$$

where

- $n \in \mathbb{N}$
- $i, j = 1, \ldots, p$ and
- $f_{i,n,j} \in \mathbb{N}[x_1, \ldots, x_k]$

shall always imply the relations

$$m_i \equiv 2 \cdot m_i$$

for every $i = 1, \ldots, p$.

Ideas and further questions

Symbolical approach

Questions - rewriting systems

Let $\equiv$ be a semiring congruence $\equiv$ on $F = \mathbb{N}[x_1, \dots, x_n]$ generated by some subset $\emptyset \neq U \subseteq F \times F$.

- Let $\emptyset \neq M \subseteq F$ and $U = \{1\} \times M$. Is there a rewriting system that decides, whether $f \equiv 1$ for given $f \in F$?
- Is there a rewriting system that decides whether $f \equiv g$ for given polynomials $f, g \in F$?

Related results:

- Otto, Sokratova: *Reduction relations for monoid semirings* (2004)
- Bokut, Chen, Mo: *Gröbner-Shirshov bases for semirings* (2012)

The following are equivalent for $\emptyset \neq M \subseteq F$:

(i) There is a semiring congruence $\equiv$ on F such that $M = \{f \in F \mid f \equiv 1\}$.

(ii) $1 \in M$ and $(\forall f_1, f_2 \in F \cup \{0\})(\forall g \in M)\ f_1 + f_2 \in M \iff f_1 g + f_2 \in M$.

Topological approach

Theorem (Karvellas '74)

Let S be a compact topological semiring. The set D of additively divisible elements of S is non-empty and topologically closed. Moreover, the ideal $S \cdot A$ is additively idempotent and, if S has a multiplicative identity, then A is additively idempotent.

Examples of compact topological semirings

- possibilistic semiring: $([0,1], \max, \cdot)$
- Lukasiewicz semiring: $([0,1], \min, \max\{a+b-1, 0\})$
- lattice: $([0,1], \max, \min)$

Questions - topological semirings

Let S be a finitely gen. (add. div.) semiring.

- Is it possible into turn S to a compact topological semiring?
- Is it possible to embed S (on the algebraic level only) into a compact topological semiring?

Grothendieck ring approach

Definition

For a semiring S set the (opposite) Rees pre-order $\leq_S$ on S as follows

$$a \leq_S b \;\Leftrightarrow\; (\exists\, c \in S)\; a + c = b.$$

Proposition

For a semiring S with a unit 1_S the set

$$Q_S = \{a \in S|\ (\exists n \in \mathbb{N})\ \ a \leq_S n \cdot 1_S\}$$

is a subsemiring.
Moreover, if S additively divisible, then Q_S is so.

Example: For $S = \mathbb{Z}^2$ with $a \oplus b := \min_{\leq_{lex}}\{a, b\}$ and $a \odot b := a + b$, Q_S is NOT finitely generated as a semiring.

The Grothendieck ring construction

For the inclusion functor $\iota : ComRng \longrightarrow ComSemirng$ of the categories of commutative rings to commutative semirings there is a left adjoint $G : ComSemirng \longrightarrow ComRng$ of ι.

For a commutative semiring S is $G(S)$ (called the *Grothendieck ring*) constructed as follows:

- $a \equiv b \Leftrightarrow (\exists x \in S)\ a + x = b + x$ (a semiring congruence)
- $\tilde{S} := S_{/\equiv}$ (an additively cancellative semiring)
- $G(S) := \tilde{S} - \tilde{S}$ (a difference ring of $\tilde{S}$)

Proposition

For an additively divisible semiring S with a unit 1_S the following are equivalent:

(i) *S is additively idempotent.*

(ii) $G(Q_S) = 0$.

(iii) *$G(Q_S)$ is torsion.*

Let us call a ring R *torsion-friendly* iff
$(\forall P \subseteq \mathbb{P})(\forall a \in S)$ P is infinite & a is P-divisible $\Rightarrow$ a is torsion.

Observation: S is fin.gen. and add. divisible & $G(Q_S)$ is torsion-friendly $\Rightarrow$ $G(Q_S)$ is add. divisible and torsion-friendly $\Rightarrow$ $G(Q_S)$ is torsion $\Rightarrow$ S is add. idempotent

Question

Is $G(Q_S)$ always torsion-friendly for a fin. generated semiring S with a unit 1_S (possibly when S is add. divisible)?

Geometrical approach

Proposition

For a semiring S with a unit 1_S generated by $\{w_1, \ldots, w_n\} \subseteq S$ is the set

$$\mathcal{C} = \{(i_1, \ldots, i_n) \in \mathbb{N}_0^n | \ w_1^{i_1} \ldots w_n^{i_n} \in Q\} =$$

$$= \{(i_1, \ldots, i_n) \in \mathbb{N}_0^n | \ (\exists n \in \mathbb{N}) \ \ w_1^{i_1} \ldots w_n^{i_n} \leq_S n \cdot 1_S\}$$

a submonoid of the free commutative monoid $(\mathbb{N}_0^n, +)$.

For a subsemigroup A of $(\mathbb{N}_0^n, +)$ define closure $\overline{A}^{\mathbb{N}_0^n} := \mathbb{N}_0^n \cap \overline{A}^{\mathbb{R}^n}$, where $\overline{A}^{\mathbb{R}^n}$ is the usual top. closure of the convex hull of A in $\mathbb{R}^n$.

If S is a parasemifield then

- $\mathcal{C}$ is a pure semigroup. $(a \in \mathbb{N}_0^n,\ k \in \mathbb{N},\ ka \in \mathcal{C} \Rightarrow a \in \mathcal{C})$
- For every vector subspace V of $\mathbb{R}^n$, the semigroup $\overline{\mathcal{C} \cap V}^{\mathbb{N}_0^n}$ is finitely generated.

Unfortunately this approach seems to be less efficient for the other conjectures since:

Proposition

Every subsemigroup of $(\mathbb{N}_0^n, +)$ *can be obtained from some additively idempotent n-generated semiring.*

Thank you for your attention!