EMBEDDING GENERAL ALGEBRAS INTO MODULES

MICHAŁ M. STRONKOWSKI AND DAVID STANOVSKÝ

ABSTRACT. The problem of embedding general algebras into modules is revisited. We provide a new method of embedding, based on Ježek's embedding into semimodules. We obtain several interesting consequences: a simpler syntactic characterization of quasi-affine algebras, a proof that quasi-affine algebras without nullary operations are actually quasi-linear, and several facts regarding the "abelian iff quasi-affine" problem.

1. INTRODUCTION

Embedding one class of structures into a better understood one may widen a knowledge about the former class. We are interested in embedding (general) algebras into modules. Two similar types of representations appear in the literature:

- *Quasi-linear algebras* are subreducts of modules; their operations can be expressed as module terms, i.e. $r_1 x_1 + \cdots + r_n x_n$.
- *Quasi-affine algebras* are subreducts of modules with additional nullary operations; their operations can be expressed as module polynomials, i.e. $r_1 x_1 + \cdots + r_n x_n + c$ with a constant c.

Quasi-linear algebras are quasi-affine, and, somewhat surprisingly, one of our main results (Theorem 2.1) establishes the converse for all algebras without nullary basic operations (indeed, nullary operations are unlikely to have a linear representation).

Quasi-affine algebras were characterized syntactically by R.W. Quackenbush in [21]: obviously, in a fixed signature, quasi-affine algebras form a quasivariety, and Quackenbush found an infinite scheme of quasi-identities axiomatizing this class (for details, see [29]). His method for finding the conditions is based on the following two facts about affine algebras (i.e., polynomially equivalent to modules), discovered earlier by J.D.H. Smith and H.P. Gumm.

- An algebra is affine, if and only if it is abelian and has a polynomial Mal'cev operation.
- A Mal'cev algebra is abelian, if and only if the Mal'cev term is central.

(For all undefined notions, see Section 1.2.) Hence, Quackenbush's task was, to determine, under which conditions an algebra **A** embeds into an algebra **B** such that there is a Mal'cev central polynomial on **B**.

Here we follow a different path. We use J. Ježek's embedding of algebras into semimodules [11], and a folklore embedding of additively cancellative semimodules into modules. We determine, under which conditions the composition of the two

embeddings yields a quasi-linear representation, and obtain a set of quasi-identities, which turn out to extend Quackenbush's ones (see Theorem 2.1(3)). However, quasi-affine algebras satisfy also our larger set, hence every quasi-affine algebra without nullary basic operations is quasi-linear. Our approach seems to have several advantages over the Quackenbush's one: firstly, we obtain a linear (not only affine) representation, secondly, our proof is shorter, and finally, despite the fact that our axiomatizing scheme is larger, it has an easier-to-handle description.

Our result has some appeal to the "abelian iff quasi-affine" problem. Quasi-affine algebras are always *abelian*, in the sense of commutator theory [3], meaning that the diagonal is a block of a congruence of the square $\mathbf{A} \times \mathbf{A}$, or equivalently that the quasi-identity

$$(TC) \qquad t(x, u_1, \ldots, u_k) \approx t(x, v_1, \ldots, v_k) \rightarrow t(y, u_1, \ldots, u_k) \approx t(y, v_1, \ldots, v_k)$$

is satisfied for every term t. Modules and unary algebras are prototypical examples.

Not all abelian algebras are quasi-affine [21], although these two notions are known to be equivalent under many additional assumptions (see Section 1.1). One of the results of K.A. Kearnes [12] says that if an abelian algebra has a central cancellative binary polynomial, then it is quasi-affine. We prove a stronger theorem. It is sufficient to assume existence of a commutative cancellative binary polynomial (Theorem 3.1 and Corollary 3.7). Every abelian algebra with a weak near-unanimity polynomial is also shown to have such a polynomial (Corollary 3.8).

1.1. **A little history.** Linear and affine representations of algebras have a long history. For instance, one of the basic results in quasigroup theory is the classical Toyoda-Bruck-Murdoch theorem [1, 19, 30], saying that every medial (or entropic) quasigroup is affine over a commutative ring. P. Němec and T. Kepka studied affine quasigroups over general rings already in [20] under the name *T-quasigroups* (nowadays, affine quasigroups are usually called *central*, see [25] for recent developments). In this context, Smith [24] was probably the first to realize the connection between affine representability and the abstract condition that is now called abelianess.

However, things work in much greater generality. Smith [24], and independently Gumm [5] showed that abelian Mal'cev algebras are affine (note that quasigroups are Mal'cev algebras). This fact was used essentially to build a commutator theory for congruence-permutable varieties in [24]. C. Herrmann in [9] extended this result significantly: abelian algebras in congruence-modular varieties are affine. This fact was used essentially to build a commutator theory for congruence-modular varieties [3, 6, 7, 18]. Highlights of this theory include solution of the RS and Park's conjectures for congruence-modular varieties [2, 16].

The "abelian iff affine" theorem can be pushed a bit further. Tame congruence theory [10, Theorem 9.6(6)] yields that, if a locally finite variety $\mathcal{V}$ satisfies a nontrivial idempotent Mal'cev condition (i.e., if $\mathcal{V}$ omits type $\mathbf{1}$), then abelian algebras in $\mathcal{V}$ are affine. For non-locally finite varieties, a stronger condition was proven to be sufficient by Kearnes and Szendrei [14]: if $\mathcal{V}$ satisfies an idempotent Mal'cev condition which fails in semilattices (in locally finite case, it corresponds to omitting types $\mathbf{1}, \mathbf{5}$), then abelian algebras in $\mathcal{V}$ are affine. The algebra $(\mathbb{R}, \frac{x+y}{2})$ shows that the assumption cannot be weakened to a non-trivial idempotent Mal'cev condition.

A weaker "abelian iff quasi-affine" theorem has been proved in several cases. For example, an abelian algebra $\mathbf{A}$ is quasi-affine, if

(1) **A** is finite and simple (or more generally tame) (Hobby, McKenzie, Pálfy [10, Theorems 13.3 and 13.5]);
(2) **A** is simple idempotent (Kearnes [13, Theorem 3.8]);
(3) **A** has a central cancellative binary polynomial operation (Kearnes [12, Corollary 1.2]);
(4) $\eta_1 \cap \Delta = 0_{A^2}$, where η_1 is the kernel of the first projection $\mathbf{A}^2 \to \mathbf{A}$ and Δ is the largest congruence on $\mathbf{A}^2$ admitting the diagonal as a block. Note that abelian algebras with a Taylor term satisfy this condition (Kearnes, Szendrei [14, Corollary 3.6]).

Regarding item (3), according to [27], we do not actually need to assume that **A** is abelian; and in the present paper, we weaken the assumption of centrality to commutativity (see Theorem 3.1).

Finally, let us note that our interest in the topic originated in the theory of modes (idempotent entropic algebras). A.B. Romanowska and others were interested in embeddability of modes into modules. She and Smith [22][23, Chapter 7] proved that every cancellative mode is a subreduct of a module over a commutative ring. This fact was extended by the first author to entropic algebras in [26, 28]. The problem, whether all abelian modes have the property, remains unsettled.

Our historical exposition was partly based on the survey paper [29], where the reader can find more details about the methods and results.

1.2. **Notation and terminology.** The notation and terminology of universal algebra we use is rather standard and follows the book [17]. We quickly recall basic definitions.

An operation σ is called *idempotent*, if the identity $\sigma(x, x, \ldots, x) \approx x$ is valid.

A binary operation $x * y$ is *commutative* if $x * y \approx y * x$ is satisfied.

A ternary operation p is called *Mal'cev*, if $p(y, x, x) \approx p(x, x, y) \approx y$ hold. A *Mal'cev algebra* is an algebra possessing a Mal'cev term operation.

An n-ary operation w, $n \geqslant 2$, is called *weak near-unanimity*, if it is idempotent and

$$w(y, x, \ldots, x) \approx w(x, y, x, \ldots, x) \approx \ldots \approx w(x, \ldots, x, y)$$

are valid.

An n-ary operation ($n \geqslant 2$) is called *Taylor*, if it is idempotent and for every $i \leqslant n$ there are $x_j, y_j \in \{x, y\}$, $j \neq i$, such that the identity

$$t(x_1, \ldots, x_i, x, x_{i+1}, \ldots, x_n) \approx t(y_1, \ldots, y_i, y, y_{i+1}, \ldots, y_n)$$

holds. For instance, Mal'cev operation or weak near-unanimity operation are Taylor. A binary operation is Taylor iff it is idempotent and commutative.

An operation is called *central* if it commutes with all basic operations, i.e., if it is a homomorphism. Algebras, where all basic operations are central are called *entropic* (or, in the case of groupoids, *medial*).

An operation σ is *cancellative*, if the quasi-identity

$$\sigma(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n) \approx \sigma(x_1, \ldots, x_{i-1}, z, x_{i+1}, \ldots, x_n) \to y \approx z$$

is satisfied for every $i \leqslant n$.

A term is *linear* if each variable occurs in it at most once.

An algebra **A** is called a *reduct* of an algebra **B**, if $A = B$ and all basic operations of **A** are term operations of **B**. It is called a *subreduct*, if it is a subalgebra of a reduct of **B**. (Sometimes we also say that **A** *embeds* into **B**.)

A *polynomial* of an algebra $\mathbf{A}$ is an operation of the form $p(x_1, \ldots, x_n) = t(x_1, \ldots, x_n, a_1, \ldots, a_m)$, where t is a term and $(a_1, \ldots, a_m)$ is a tuple of elements of A. Two algebras are *polynomially equivalent* if they have the same universes and the same sets of polynomial operations. Algebras polynomially equivalent to modules are called *affine*. Subreducts of affine algebras are called *quasi-affine*. Note that the definition of quasi-affiness given here is consistent with the one given at the beginning of Introduction. Indeed, it follows from the fact that all polynomials of modules are of the form $r_1 x_1 + \cdots + r_n x_n + c$.

By a *semiring* we mean an "unitary ring without subtraction", that means an algebra $\mathbf{R} = (R, +, \cdot, 0, 1)$ such that both binary operations are associative, addition is commutative, multiplication distributes over addition, and the usual laws for $0, 1$, i.e. $1r \approx r \approx r1$ and $0r \approx 0 \approx r0$, hold. A *semimodule* over a semiring $\mathbf{R}$, or an $\mathbf{R}$-*semimodule*, is a "module without subtraction", it means an algebra $\mathbf{M} = (M, +, 0, r \cdot : r \in R)$ such that $(M, +, 0)$ is a commutative monoid, $r \cdot$ are unary operations of multiplication by elements of $\mathbf{R}$ acting homomorphically on $(M, +, 0)$, and the identities $1x \approx x$, $0x \approx 0$, $(r \cdot s)x \approx r(sx)$, $(r + s)x \approx rx + sx$ are valid for all $r, s \in \mathbf{R}$. (All semimodules and modules in this article are supposed to be left.) A semimodule is *additively cancellative* if its addition is cancellative. It is a folklore fact that every additively cancellative semimodule is a subreduct of a module. For more information about semirings and semimodules, see [4, 8].

In the present paper, we will use the notion of a *multiset* in a slightly generalized setting: not only elements are allowed to have multiple presence, but also fractional. Formally, a multiset on X is a function from X into the set of non-negative rational numbers, usually denoted as a set of pairs (x, q), omitting the pairs with $q = 0$ and writing $(x, 1)$ as x. Note also that multisets on X may be identified with elements of the semimodule freely generated by X over the semiring of non-negative rational numbers. The multiset union will be denoted by $\uplus$.

2. Quasi-identities for quasi-linearity

Let us fix a signature Σ without nullary basic operations. We will denote by $\mathbb{N}\langle S \rangle$ the semiring of polynomials over natural numbers (including 0) with the set of non-commuting variables $S = \{\sigma_{(1)}, \ldots, \sigma_{(n)} \mid \sigma \in \Sigma \text{ and } n \text{ is the arity of } \sigma\}$. Note that $\mathbb{N}\langle S \rangle$ is a subreduct of the ring $\mathbb{Z}\langle S \rangle$ of polynomials over integers with the set of non-commuting variables S.

Let $\mathbf{F}(X)$ be the free $\mathbb{N}\langle S \rangle$-semimodule over a set X. Every element of $\mathbf{F}(X)$ can be written (uniquely) as $\sum_{x \in X} r_x x$ for some $r_x \in \mathbb{N}\langle S \rangle$, or equivalently, after redistributing polynomial terms, as $\sum_{i=1}^n e_i x_i$ for some n, $e_i \in S^*$ and $x_i \in X$. Here S^* denotes the set of words with letters in S. Terms of the latter sum will be called *branches*. The multiset of all branches of $u \in F(X)$ will be denoted by $\mathrm{B}(u)$. The *complexity* of $\sum_{i=1}^n e_i x_i$, where $e_i \in S^*$, $x_i \in X$ is the length of the word $e_1 \cdots e_n$.

In our considerations, Σ-terms over X will be identified with certain elements of $\mathbf{F}(X)$. Let $\mathbf{F}^\Sigma(X)$ be the Σ-reduct of $\mathbf{F}(X)$, where

$$\sigma(u_1, \ldots, u_n) = \sigma_{(1)} u_1 + \cdots + \sigma_{(n)} u_n$$

for every $\sigma \in \Sigma$ of arity n and all $u_1, \ldots, u_n \in F(X)$. Then the subalgebra $\mathbf{T}(X)$ of $\mathbf{F}^\Sigma(X)$ generated by X is absolutely free over X. Thus we may identify a term with its evaluation in $\mathbf{T}(X)$ where each variable is assigned to itself. With this

identification we may shortly and formally say what does it mean that a term s is a *subterm* of a term t at the address $e \in S^*$, that is $t = u + es$ for some u. For a tuple of terms $(t_0, \ldots, t_n)$ we will use the symbol $\mathrm{B}(t_0, \ldots, t_n)$ to denote $\mathrm{B}(t_0 + \cdots + t_n)$. The idea of the linear representation of terms is due to Ježek [11].
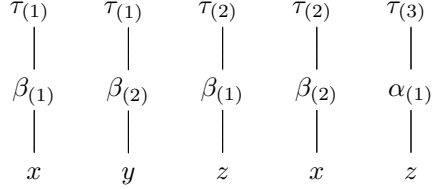
Example. Let Σ consist of a ternary operation τ, binary β and unary α. Then, e.g., the term $t = \tau(\beta(x, y), \beta(z, x), \alpha(z))$, with a parsing tree
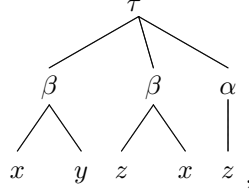
is represented in $\mathbf{F}(\{x, y, z\})$ as

$$\tau_{(1)}\beta_{(1)}x + \tau_{(1)}\beta_{(2)}y + \tau_{(2)}\beta_{(1)}z + \tau_{(2)}\beta_{(2)}x + \tau_{(3)}\alpha_{(1)}z$$

and the (multi)set of branches $\mathrm{B}(t)$ can be depicted as

Example. Let σ be a ternary operation. Then we have

$$\mathrm{B}(\sigma(x, x, z), \sigma(y, y, z)) = \mathrm{B}(\sigma(x, y, z), \sigma(y, x, z)).$$

Theorem 2.1. *For an algebra $\mathbf{A}$ without nullary basic operations, the following are equivalent:*

(1) $\mathbf{A}$ *is quasi-affine (i.e., $\mathbf{A}$ is a subreduct of an affine algebra);*
(2) $\mathbf{A}$ *is quasi-linear (i.e., $\mathbf{A}$ is a subreduct of a module);*
(3) $\mathbf{A}$ *models the quasi-identity*

$$t_1 \approx s_1 \wedge \cdots \wedge t_m \approx s_m \;\rightarrow\; t_0 \approx s_0$$

for each positive integer m and each pair of tuples of terms satisfying $\mathrm{B}(t_0, \ldots, t_m) = \mathrm{B}(s_0, \ldots, s_m)$.

In the rest of the section, we prove the theorem. To show the relevance of the quasi-identities, we will start with the implication $(3) \Rightarrow (2)$. The implication $(2) \Rightarrow (1)$ is trivial and we finish with the proof that quasi-affine algebras satisfy the quasi-identities of (3).

As noted in Introduction, the reasoning will be based on Ježek's embedding of algebras into semimodules, though the proof is self-contained. Given an algebra $\mathbf{A}$ over the signature Σ, we take the free $\mathbb{N}\langle S \rangle$-semimodule $\mathbf{F}(A)$ and generate a congruence θ by all pairs

$$(a, \sigma_{(1)}a_1 + \cdots + \sigma_{(n)}a_n)$$

such that $a, a_1, \ldots, a_n \in A$ and $a = \sigma(a_1, \ldots, a_n)$ in $\mathbf{A}$. Then $a \mapsto a/\theta$ is an embedding of $\mathbf{A}$ into the Σ-reduct of $\mathbf{F}(A)/\theta$. For details, see [11, Section 3].

Let θ_+ be the least congruence expansion of θ such that the semimodule $\mathbf{F}(A)/\theta_+$ is additively cancellative. Then $\mathbf{F}(A)/\theta_+$ is a subreduct of a $\mathbb{Z}\langle S\rangle$-module, and we are left with the following question: does $\mathbf{A}$ also embed into $\mathbf{F}(A)/\theta_+$? That means, is $\theta_+|_A$ the identity relation?

Lemma 2.2. $u\,\theta_+\,v$ iff there is $w \in F(A)$ such that $u + w\,\theta\,v + w$.

Proof. Note that θ_+ has to contain all such pairs (u, v). On the other hand, the binary relation thus defined is a congruence whose factor is additively cancellative. $\square$

Lemma 2.3. $u\,\theta_+\,v$ iff there are a natural number m and $a_1, \ldots, a_m \in A$ such that
$$u + a_1 + \cdots + a_m\,\theta\,v + a_1 + \cdots + a_m.$$

Proof. Note that for every $w \in F(A)$ there is $w' \in F(A)$ such that $w + w'$ is a sum of terms. Indeed, to each branch $u \in \mathrm{B}(w)$ we associate a term $t_u \in T(A)$ containing u, and let u' be such that $t_u = u + u'$. Then we may take $w' = \sum\{u' \mid u \in \mathrm{B}(w)\}$. However, for every $t \in T(A)$ there is $a \in A$ such that $t\,\theta\,a$. Now, use Lemma 2.2. $\square$

Let us introduce some notation. For a term t with variables in A, let $^{\mathbf{A}}t$ be its evaluation in $\mathbf{A}$ where each variable is assigned to itself. For $a \in A$ we will write $a \searrow t$ if $a = {}^{\mathbf{A}}t$, and $\nearrow$ will be the converse relation. Observe that
$$^{\mathbf{A}}t = {}^{\mathbf{A}}s \quad \text{iff} \quad t\,(\nearrow \circ \searrow)\,s.$$
For tuples of terms, we will write $(a_1, \ldots, a_m) \searrow (t_1, \ldots, t_m)$ if $a_i \searrow t_i$ for all i.

We define a relation $\sim_m$, or simply $\sim$, on the set $T(X)^m$ by
$$(t_1, \ldots, t_m) \sim (s_1, \ldots, s_m) \quad \text{iff} \quad t_1 + \cdots + t_m = s_1 + \cdots + s_m \text{ in } \mathbf{F}(X).$$
In other words, iff the multisets of branches satisfy $\mathrm{B}(t_1, \ldots, t_m) = \mathrm{B}(s_1, \ldots, s_m)$.

For $a, b \in A$, let $a\,\rho_m^k\,b$ if there are $c_1, \ldots, c_m \in A$ such that
$$(a, c_1, \ldots, c_m)\,(\searrow \circ \sim \circ \nearrow)^k\,(b, c_1, \ldots, c_m).$$

Lemma 2.4. For $a, b \in A$, $a\,\theta_+\,b$ iff $a\,\rho_m^k\,b$ for some k and m.

Proof. For $u, v \in F(A)$ let

(L) $u\,\lambda\,v \quad \text{if} \quad u = w + e(\sigma_{(1)}a_1 + \cdots + \sigma_{(n)}a_n) \quad \text{and} \quad v = w + ea$

for some $w \in F(A)$, $e \in S^*$, an n-ary operation $\sigma \in \Sigma$, and $a, a_1, \ldots, a_n \in A$ such that $\sigma(a_1, \ldots, a_n) = a$ in $\mathbf{A}$. Then θ is the transitive and reflexive closure of $\lambda \cup \lambda^{-1}$, where λ^{-1} is the inverse of λ.

Claim. Let $(u, v) \in \lambda \cup \lambda^{-1}$. If $u = t_0 + \cdots + t_m$, where all $t_i \in T(A)$, then there are $t_i', t_i'' \in T(A)$ such that $(t_0, \ldots, t_m) \sim (t_0', \ldots, t_m')$, $v = t_0'' + \cdots + t_m''$ and $(t_0', \ldots, t_m')\,(\nearrow \circ \searrow)\,(t_0'', \ldots, t_m'')$.

Proof of Claim. The statement in the case when $(u, v) \in \lambda^{-1}$ follows easily. Let $v = w + e(\sigma_{(1)}a_1 + \cdots + \sigma_{(n)}a_n)$ and $u = w + ea = t_0 + \ldots + t_m$. Let $l \leqslant m$ be such that $ea \in \mathrm{B}(t_l)$. Put $t_l' = t_l$ and let t_l'' be the term obtained from t_l by substituting $\sigma(a_1, \ldots, a_n)$ for a at the address e in t_l, i.e. if $t_l' = p + ea$, then $t_l'' = p + e(\sigma_{(1)}a_1 + \cdots + \sigma_{(n)}a_n)$. For $k \neq l$ we may put $t_k'' = t_k' = t_k$.

Let us assume that $(u, v) \in \lambda$ and u, v are as in (L). Let $l_i \leqslant m$ be such that $e\sigma_{(i)}a_i \in \mathrm{B}(t_{l_i})$. Then, in particular, t_{l_1} has a subterm $\sigma(a_1, r_2, \ldots, r_n)$, where

$r_i \in T(A)$, at the address e. Define t'_{l_1} as the term obtained from t_{l_1} by substituting a_i for r_i at the address $e\sigma_{(i)}$ for all $i \in \{2, \dots, n\}$. Let t'_{l_i}, $2 \leqslant i \leqslant n$, be the term obtained from t_{l_i} by substituting r_i for a_i at the address $e\sigma_{(i)}$. (Note that it may happen that some $a_i = r_i$, which means the respective changes are void.) Note that $t_{l_1} + \cdots + t_{l_n} = t'_{l_1} + \cdots + t'_{l_n}$. If $k \neq l_i$ for all i, let $t'_k = t_k$. Then $u = t'_0 + \cdots + t'_m$. Now let t''_{l_1} be the term obtained from t'_{l_1} by substituting a for $\sigma(a_1 \dots, a_n)$ at the address e, i.e. if $t'_{l_1} = p + e(\sigma_{(1)}a_1 + \cdots + \sigma_{(n)}a_n)$, then $t''_{l_1} = p + ea$. For other $k \neq l_1$, let $t''_k = t'_k$. Then $v = t''_0 + \cdots + t''_m$, and since ${}^{\mathbf{A}}t'_k = {}^{\mathbf{A}}t''_k$ for all k, we obtain $(t'_0, \dots, t'_m)\,(\nearrow \circ \searrow)\,(t''_0, \dots, t''_m)$. $\qquad\square$

Assume $a\,\theta_+\,b$. By Lemma 2.3, there are $c_1, \dots, c_m \in A$ such that
$$u := a + c_1 + \cdots + c_m \; \theta \; b + c_1 + \cdots + c_m =: v.$$
Thus there is a sequence $u_0, \dots, u_k \in T(A)$ such that $u_0 = u$, $u_k = v$ and $(u_j, u_{j+1}) \in \lambda \cup \lambda^{-1}$ for all j. By the Claim, there are terms $t_{j,l}$, $t'_{j,l}$, $j = 0, \dots, k$, $l = 0, \dots, m$, such that $u_j = t_{j,0} + \cdots + t_{j,m} = t'_{j,0} + \cdots + t'_{j,m}$ and $t'_{j,i}\,(\nearrow \circ \searrow)\,t_{j+1,i}$.

The converse implication in the statement is evident. $\qquad\square$

Lemma 2.5. *For $a, b \in A$, if $a\,\rho_m^k\,b$, then $a\,\rho_{m'}^1\,b$ for some m'.*

Proof. Let
$$(a_0, \underline{c}_0) \searrow \underline{u}_0 \sim \underline{v}_1 \nearrow (a_1, \underline{c}_1) \searrow \underline{u}_1 \sim \underline{v}_2 \nearrow (a_2, \underline{c}_2) \searrow \cdots \nearrow (a_k, \underline{c}_k),$$
where $a_0 = a$, $a_k = b$, $\underline{c}_0 = \underline{c}_k$. Then
$$(a_0, \underline{c}_0, a_1, \underline{c}_1,, \dots, a_{k-1}, \underline{c}_{k-1}) \searrow (\underline{u}_0, \dots, \underline{u}_{k-1}) \sim (\underline{v}_1, \dots, \underline{v}_k)$$
$$\sim (\underline{v}_k, \underline{v}_1, \dots, \underline{v}_{k-1}) \nearrow (a_k, \underline{c}_k, a_1, \underline{c}_1,, \dots, a_{k-1}, \underline{c}_{k-1}).$$
(We get $m' = (m+1)k - 1$.) $\qquad\square$

Proof of Theorem 2.1, (3) $\Rightarrow$ (2). Let $a, b \in A$ and assume that $a\,\theta_+\,b$. It follows from Lemmas 2.4 and 2.5 that there are $c_1, \dots, c_m \in A$ and terms $t_0, \dots, t_m$, $s_0, \dots, s_m$ such that
$$(a, c_1, \dots, c_m) \searrow (t_0, \dots, t_m) \sim (s_0, \dots, s_m) \nearrow (b, c_1, \dots, c_m).$$
By assumption, $\mathbf{A}$ satisfies the quasi-identity
$$t_1 \approx s_1 \wedge \cdots \wedge t_m \approx s_m \;\to\; t_0 \approx s_0.$$
Note that in this quasi-identity, variables are elements of A. And since
$$ {}^{\mathbf{A}}t_i = c_i = {}^{\mathbf{A}}s_i$$
for every $1 \leqslant i \leqslant m$,
$$a = {}^{\mathbf{A}}t_0 = {}^{\mathbf{A}}s_0 = b.$$
Hence $a \mapsto a/\theta_+$ is an embedding of $\mathbf{A}$ into a reduct of the additively cancellative semimodule $\mathbf{F}(A)/\theta_+$, and thus $\mathbf{A}$ is quasi-linear. $\qquad\square$

In order to prove the remaining implication, we start with some auxiliary definitions. First, to capture the affine representation of operations, let us introduce new symbols c_σ for each $\sigma \in \Sigma$, and put $C_\Sigma = \{c_\sigma \mid \sigma \in \Sigma\}$. Let $\mathbf{G}(X)$ be the $\mathbb{N}\langle S \rangle$-semimodule $\mathbf{F}(X \cup C_\Sigma)$ extended by C_Σ as the set of nullary basic operations. Let $\mathbf{G}^\Sigma(X)$ be the Σ-reduct of $\mathbf{G}(X)$, where

(AFF) $$\sigma(u_1, \dots, u_n) = \sigma_{(1)}u_1 + \cdots + \sigma_{(n)}u_n + c_\sigma$$

for every $\sigma \in \Sigma$ with arity n and all $u_1, \ldots, u_n \in G(X)$.

For a multiset of branches B from $G(X)$ and $e \in S^*$, $\sigma \in \Sigma$ let $N_{e,\sigma}$ be the cardinality (counted with multiplicities) of the multiset

$$\{(e\sigma_{(i)}x, q) \in B \mid 1 \leqslant i \leqslant \text{arity of } \sigma, \ x \in X \cup C_\Sigma\}$$

and let

$$B' = \left\{ \left(ec_\sigma, \frac{N_{e,\sigma}}{\text{arity of } \sigma} \right) \ \middle| \ e \in S^* \text{ and } \sigma \in \Sigma \right\}$$

We set $B^* = B' \uplus B'' \uplus B''' \uplus \cdots$.

Example. Let σ, τ be binary operations, $t_1 = \sigma(\tau(x, \sigma(x, y)), z)$, $t_2 = \sigma(x, z)$. Then one may compute

$$\mathrm{B}(t_1, t_2) = \{\sigma_{(1)}x, (\sigma_{(2)}z, 2), \sigma_{(1)}\tau_{(1)}x, \sigma_{(1)}\tau_{(2)}\sigma_{(1)}x, \sigma_{(1)}\tau_{(2)}\sigma_{(2)}y\},$$
$$\mathrm{B}'(t_1, t_2) = \{(c_\sigma, 3/2), (\sigma_{(1)}c_\tau, 1/2), \sigma_{(1)}\tau_{(2)}c_\sigma\},$$
$$\mathrm{B}''(t_1, t_2) = \{(c_\sigma, 1/4), (\sigma_{(1)}c_\tau, 1/2)\},$$
$$\mathrm{B}'''(t_1, t_2) = \{(c_\sigma, 1/4)\},$$
$$\mathrm{B}^*(t_1, t_2) = \{(c_\sigma, 2), \sigma_{(1)}c_\tau, \sigma_{(1)}\tau_{(2)}c_\sigma\}.$$

In the above example all multiplicities in $\mathrm{B}^*(t_1, t_2)$ are natural numbers. If u is a sum of terms, then $\mathrm{B}^*(u)$ always has natural multiplicities. This fact will be important in the following proof.

Proof of Theorem 2.1, $(1) \Rightarrow (3)$. First note that if a Σ-algebra is quasi-affine, then it is a subreduct of some $\mathbb{Z}\langle S \rangle$-module $\mathbf{M}$ extended by nullary operations corresponding to the symbols from C_Σ. Let $\mathbf{M}^\Sigma$ be the Σ-reduct of $\mathbf{M}$, where the basic operations are given by (AFF). Let t_i, s_i be terms from $T(M)$ such that $\mathrm{B}(t_0, \ldots, t_m) = \mathrm{B}(s_0, \ldots, s_m)$. We just need to check that

(Q)   if $\ {}^{\mathbf{M}^\Sigma}t_1 = {}^{\mathbf{M}^\Sigma}s_1, \ldots, {}^{\mathbf{M}^\Sigma}t_m = {}^{\mathbf{M}^\Sigma}s_m,$ then ${}^{\mathbf{M}^\Sigma}t_0 = {}^{\mathbf{M}^\Sigma}s_0.$

Let $\boxed{} : G(M) \to M$ be the $\mathbb{N}\langle S \rangle$-semimodule homomorphism such that its restriction to M is the identity mapping and $\boxed{c_\sigma} = c_\sigma$ for $\sigma \in \Sigma$.

Claim. *For $t \in T(M)$ we have* ${}^{\mathbf{M}^\Sigma}t = \boxed{t} + \sum \boxed{\mathrm{B}^*(t)}$.

Proof of Claim. This follows inductively from the observation that

$$\mathrm{B}^*(\sigma(t_1, \ldots, t_n)) = \mathrm{B}^*(\sigma_{(1)}t_1 + \cdots + \sigma_{(n)}t_n) = \{c_\sigma\} \uplus \biguplus_{i=1}^{n} \sigma_{(i)} \mathrm{B}^*(t_i).$$

$\square$

Because $\mathrm{B}(t_0, \ldots, t_m) = \mathrm{B}(s_0, \ldots, s_m)$ we have $\mathrm{B}^*(t_0, \ldots, t_m) = \mathrm{B}^*(s_0, \ldots, s_m)$, and by the Claim

$$
\begin{aligned}
{}^{\mathbf{M}^\Sigma}t_0 + \cdots + {}^{\mathbf{M}^\Sigma}t_m &= \boxed{t_0 + \cdots + t_m} + \sum \boxed{\mathrm{B}^*(t_0, \ldots, t_m)} \\
&= \boxed{s_0 + \cdots + s_m} + \sum \boxed{\mathrm{B}^*(s_0, \ldots, s_m)} \\
&= {}^{\mathbf{M}^\Sigma}s_0 + \cdots + {}^{\mathbf{M}^\Sigma}s_m.
\end{aligned}
$$

This, together with the cancellativity of the addition in $\mathbf{M}$, yields the satisfaction of (Q).

$\square$

Let us note that the set of quasi-identities from the condition (3) of Theorem 2.1 properly contains the original Quackenbush's scheme. However, we found our description much easier to handle, in particular in view of the results in Section 3.

3. APPLICATION

Theorem 3.1. *Let $\mathbf{A}$ be an algebra without nullary basic operations and possessing a commutative cancellative polynomial $x * y$. Then $\mathbf{A}$ is quasi-linear if and only if it is abelian.*

In this section we will prove Theorem 3.1 and derive some consequences.

Lemma 3.2. *An abelian commutative groupoid $\mathbf{A} = (A, *)$ is entropic.*

Proof. By the commutativity we have the validity of $(x*y)*(z*x) \approx (x*z)*(y*x)$, and by (TC) the validity of $(x * y) * (z * t) \approx (x * z) * (y * t)$. $\square$

An operation $q(x_0, \ldots, x_m)$ is *commutative* if $q(x_0, \ldots, x_m) \approx q(x_{\pi(0)}, \ldots, x_{\pi(m)})$ is satisfied for every permutation π of $\{0, \ldots, m\}$.

Lemma 3.3. *An abelian algebra $\mathbf{A}$ possessing a commutative cancellative binary polynomial $x * y$ has a commutative cancellative polynomial $q(x_0, \ldots, x_m)$ for arbitrary m.*

Proof. For the sake of simplicity, we may assume that the operation $x * y$ is basic, i.e. $* \in \Sigma$. Let l be a natural number. Let $t_l(x_0, \ldots, x_{2^l-1})$ be a linear $\{*\}$-term, where addresses of all variables have length l. The cancellativity of t_l is evident. We will prove inductively the commutativity of t_l. Term t_0 equals x_0, and the statement for it is trivial. For $t_1(x_0, x_1) = x_0 * x_1$ the assertion is just a part of the assumption of the lemma. So let $t_l = (t_{00} * t_{01}) * (t_{10} * t_{11})$, and assume that all t_k, $k < l$, are commutative. Assume that x_0 is the leftmost variable occurring in t_l. It is enough to prove that

$$t_l(x_0, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{2^l-1}) \approx t_l(x_i, \ldots, x_{i-1}, x_0, x_{i+1}, \ldots, x_{2^l-1})$$

holds for every $i \in \{1, \ldots, 2^l-1\}$. If x_i occurs in $t_{00} * t_{01}$, then the assertion follows from the commutativity of this term. If x_i occurs in t_{10}, then the assertion follows from the validity of $(t_{00} * t_{01}) * (t_{10} * t_{11}) \approx (t_{00} * t_{10}) * (t_{01} * t_{11})$, proved in Lemma 3.2, and the commutativity of $t_{00} * t_{10}$. Finally, if x_i occurs in t_{11}, then the assertion follows from the commutativity of $t_{10} * t_{11}$ and the latter case.

Now choose l such that $m + 1 \leqslant 2^l$, and define

$$q(x_0, \ldots, x_m) = t_l(x_0, \ldots, x_m, d, \ldots, d),$$

where d is an arbitrary element of A. $\square$

Lemma 3.4. *Let $t(x, y_1, \ldots, y_n)$ and $s(x, z_1, \ldots, z_m)$ be linear terms having the same branch containing x, i.e. x is at the same address in t and s. Then an abelian algebra satisfies the quasi-identity*

$$t(x_1, y_1, \ldots, y_n) \approx s(x_1, z_1, \ldots, z_m) \rightarrow t(x_2, y_1, \ldots, y_n) \approx s(x_2, z_1, \ldots, z_m).$$

Lemma 3.5. *Let $\mathbf{A}$ be an abelian algebra possessing a commutative polynomial $q(x_0, \ldots, x_m)$. If $\mathrm{B}(t_0, \ldots, t_m) = \mathrm{B}(s_0, \ldots, s_m)$, where $s_i, t_i \in T(\{y\})$, then $\mathbf{A}$ satisfies*

$$q(t_0, \ldots, t_m) \approx q(s_0, \ldots, s_m).$$

Proof. We proceed by induction on the complexity of $t_0 + \cdots + t_m$. If all terms t_i equal y, then also all s_i equal y, and the assertion is trivially satisfied. Let us assume that the above trivial case does not hold. Let us also assume that the assertion is valid for each pair of $(m + 1)$-tuples of terms of a smaller complexity than of $t_0 + \cdots + t_m$. Observe that there are $e \in S^*$, $\sigma \in \Sigma$ and $i, j \in \{1, \ldots, m\}$ such that $\sigma(y, \ldots, y)$ is a subterm of t_i and s_j at the address e. By the commutativity of q we may assume that $i = j = 0$. Let t_0' be the term obtained from t_0 by substituting y for $\sigma(y, \ldots, y)$ at the address e, and let s_0' be obtained from s_0 in the same way. Let $t_l' = t_l$ and $s_l' = s_l$ for $l \geqslant 1$. We have $\mathrm{B}(t_0', \ldots, t_m') = \mathrm{B}(s_0', \ldots, s_m')$, and by the inductive assumption

$$q(t_0', \ldots, t_m') \approx q(s_0', \ldots, s_m').$$

Now the assertion follows from Lemma 3.4. $\qquad\square$

Lemma 3.6. *Let $\mathbf{A}$ be an abelian algebra possessing a commutative polynomial $q(x_0, \ldots, x_m)$. If $\mathrm{B}(t_0, \ldots, t_m) = \mathrm{B}(s_0, \ldots, s_m)$, where $s_i, t_i \in T(X)$, then $\mathbf{A}$ satisfies*

$$q(t_0, \ldots, t_m) \approx q(s_0, \ldots, s_m).$$

Proof. Let y be a variable not belonging to X. We will define the sequence of multisets of branches B_j with natural multiplicities and the sequences of terms $t_{l,j}, s_{l,j} \in T(X \cup \{y\})$ satisfying

$$B_j = \{ex \in \mathrm{B}(t_{0,j}, \ldots, t_{m,j}) \mid e \in S^* \text{ and } x \in X - \{y\}\}$$

and

$$\mathrm{B}(t_{0,j}, \ldots, t_{m,j}) = \mathrm{B}(s_{0,j}, \ldots, s_{m,j}),$$

in the following way. Let $B_0 = \mathrm{B}(t_0, \ldots, t_m)$, $t_{l,0} = t_l$ and $s_{l,0} = s_l$. Assume that B_j and $t_{l,j}$, $s_{l,j}$ are already defined. If $B_j \neq \emptyset$, then take an arbitrary branch $ex \in B_j$, where $e \in S^*$, $x \in X$. There are l, k such that $ex \in \mathrm{B}(t_{l,j})$ and $ex \in \mathrm{B}(s_{k,j})$. Let $B_{j+1} = B_j - \{ex\}$ and let $t_{l,j+1}$ be the term obtained form $t_{l,j}$ by substituting y for x at the address e (in other words by substituting the branch ey for ex), $s_{k,j+1}$ be obtained from $s_{k,j}$ in the same way, and $t_{l',j+1} = t_{l',j}$, $s_{k',j+1} = s_{k',j}$ for $l' \neq l$ and $k' \neq k$. Finally, let J be such that $B_J = \emptyset$. Then $t_{l,J} = t_l(y, \ldots, y)$, $s_{l,J} = s_l(y, \ldots, y)$, for $l \leqslant m$, and, by Lemma 3.5, $\mathbf{A}$ satisfies

$$q(t_{0,J}, \ldots, t_{m,J}) \approx q(s_{0,J}, \ldots, s_{m,J}).$$

Lemma 3.4, together with the commutativity of q, yields the validity of

$$q(t_{0,j}, \ldots, t_{m,j}) \approx q(s_{0,j}, \ldots, s_{m,j}) \leftrightarrow q(t_{0,j+1}, \ldots, t_{m,j+1}) \approx q(s_{0,j+1}, \ldots, s_{m,j+1}),$$

for all j. Thus $q(t_0, \ldots, t_m) \approx q(s_0, \ldots, s_m)$ holds in $\mathbf{A}$. $\qquad\square$

Proof of Theorem 3.1. Use Lemmas 3.3 and 3.6 together with Theorem 2.1. $\qquad\square$

Now we may easily derive a strengthening of Kearnes' theorem mentioned on page 2.

Corollary 3.7. *Let* **A** *be an abelian algebra without nullary basic operations and possessing a cancellative polynomial* $x \bullet y$ *such that* $(A, \bullet)$ *is entropic. Then* **A** *is quasi-linear.*

Proof. Define a binary cancellative commutative polynomial as $x*y = (d\bullet x)\bullet(y\bullet d)$, where $d \in A$, and use Theorem 3.1. $\square$

Our last contribution is a new proof that an abelian algebra having a weak near-unanimity polynomial is quasi-affine. It is a special case of Kearnes' and Szendrei's theorem mentioned on page 3. The importance of such operation follows from the fact, proved by M. Maróti and R. McKenzie in [15], that possessing a weak near-unanimity term is equivalent to having a Taylor term for locally finite varieties.

Corollary 3.8. *Let* **A** *be an abelian algebra without nullary basic operations and having a weak near-unanimity polynomial* $w(x_1, \ldots, x_n)$. *Then* **A** *is quasi-linear.*

Proof. Let $x * y = w(x, y, d, \ldots, d)$, where d is an arbitrary element of A. In order to use Theorem 3.1 we will show that $x * y$ is commutative and cancellative.

Because w is a weak near-unanimity operation, for $a, b \in A$

$$w(a, \ldots, a, b, a, a, \ldots, a) = w(a, \ldots, a, a, b, a, \ldots, a),$$

where b appears on the ith position on the left side and on the $(i + 1)$th position on the right side, $i < n$. By (TC) we obtain the equality

(C) $\qquad w(c_1, \ldots, c_{i-1}, b, a, c_{i+2}, \ldots, c_n) = w(c_1, \ldots, c_{i-1}, a, b, c_{i+2}, \ldots, c_n)$

for every $c_j \in A$. For $i = 1$ and $c_j = d$ this yields $a * b = b * a$. Now assume that $a * c = b * c$. By (TC) and (C), this implies

$$a = w(a, \ldots, a) = w(b, a, \ldots) = w(a, b, a, \ldots, a).$$

Applying again (TC) and (C),

$$a = w(b, a, \ldots, a) = w(b, b, a, \ldots, a) = w(a, b, b, a, \ldots, a).$$

We may proceed in this way obtaining finally

$$a = w(a, b \ldots, b) = w(b, b \ldots, b) = b.$$

$\square$

We do not know the answer to the following question posed by the referee.

Problem. For finite algebras with finite signature without nullary basic operations, is the property of being quasi-linear decidable?

Note however that abelianess is decidable, as we may check whether the diagonal is a block of a congruence of the square of a given finite algebra with finite signature. Thus, if an algebra **A** satisfies any of known conditions guaranteeing that abelian algebras are quasi-linear, then in fact we may decide whether it is quasi-linear. Note also that the properties in the conditions (1)-(4) in Subsection 1.1 and in Theorem 3.1 are decidable.

References

[1] Richard H. Bruck. Some results in the theory of quasigroups. *Trans. Amer. Math. Soc.*, 55:19–52, 1944.

[2] Ralph Freese and Ralph N. McKenzie. Residually small varieties with modular congruence lattices. *Trans. Amer. Math. Soc.*, 264(2):419–430, 1981.

[3] Ralph Freese and Ralph N. McKenzie. *Commutator theory for congruence modular varieties*, volume 125 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1987.

[4] Jonathan S. Golan. *Semirings and affine equations over them: theory and applications*, volume 556 of *Mathematics and its Applications*. Kluwer Academic Publishers Group, Dordrecht, 2003.

[5] H. Peter Gumm. Algebras in permutable varieties: geometrical properties of affine algebras. *Algebra Universalis*, 9(1):8–34, 1979.

[6] H. Peter Gumm. Geometrical methods in congruence modular algebras. *Mem. Amer. Math. Soc.*, 45(286):viii+79, 1983.

[7] Joachim Hagemann and Christian Herrmann. A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity. *Arch. Math. (Basel)*, 32(3):234–245, 1979.

[8] Udo Hebisch and Hanns J. Weinert. *Semirings: algebraic theory and applications in computer science*, volume 5 of *Series in Algebra*. World Scientific Publishing Co. Inc., River Edge, NJ, 1998. Translated from the 1993 German original.

[9] Christian Herrmann. Affine algebras in congruence modular varieties. *Acta Sci. Math. (Szeged)*, 41(1-2):119–125, 1979.

[10] David Hobby and Ralph N. McKenzie. *The structure of finite algebras*, volume 76 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1988.

[11] Jaroslav Ježek. Terms and semiterms. *Comment. Math. Univ. Carolin.*, 20(3):447–460, 1979.

[12] Keith A. Kearnes. A quasi-affine representation. *Internat. J. Algebra Comput.*, 5(6):673–702, 1995.

[13] Keith A. Kearnes. Idempotent simple algebras. In *Logic and algebra (Pontignano, 1994)*, volume 180 of *Lecture Notes in Pure and Appl. Math.*, pages 529–572. Dekker, New York, 1996.

[14] Keith A. Kearnes and Ágnes Szendrei. The relationship between two commutators. *Internat. J. Algebra Comput.*, 8(4):497–531, 1998.

[15] Miklós Maróti and Ralph N. McKenzie. Existence theorems for weakly symmetric operations. *Algebra Universalis*, 59(3-4):463–489, 2008.

[16] Ralph N. McKenzie. Finite equational bases for congruence modular varieties. *Algebra Universalis*, 24(3):224–250, 1987.

[17] Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor. *Algebras, lattices, varieties. Vol. I*. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1987.

[18] Ralph N. McKenzie and John Snow. Congruence modular varieties: commutator theory and its uses. In *Structural theory of automata, semigroups, and universal algebra*, volume 207 of *NATO Sci. Ser. II Math. Phys. Chem.*, pages 273–329. Springer, Dordrecht, 2005.

[19] David C. Murdoch. Structure of abelian quasi-groups. *Trans. Amer. Math. Soc.*, 49:392–409, 1941.

[20] Petr Němec and Tomáš Kepka. *T*-quasigroups. I, II. *Acta Univ. Carolin. Math. Phys.*, 12(1):39–49 (1972); ibid. 12 (1971), no. 2, 31–49 (1972), 1971.

[21] Robert W. Quackenbush. Quasi-affine algebras. *Algebra Universalis*, 20(3):318–327, 1985.

[22] Anna B. Romanowska and Jonathan D. H. Smith. Embedding sums of cancellative modes into functorial sums of affine spaces. In *Unsolved problems on mathematics for the 21st century*, pages 127–139. IOS, Amsterdam, 2001.

[23] Anna B. Romanowska and Jonathan D. H. Smith. *Modes*. World Scientific Publishing Co. Inc., River Edge, NJ, 2002.

[24] Jonathan D. H. Smith. *Mal'cev varieties*. Lecture Notes in Mathematics, Vol. 554. Springer-Verlag, Berlin, 1976.

[25] Jonathan D. H. Smith. *An introduction to quasigroups and their representations*. Studies in Advanced Mathematics. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[26] Michał M. Stronkowski. *On embeddings of entropic algebras*. PhD thesis, Warsaw University of Technology, Warsaw, 2006.

[27] Michał M. Stronkowski. Cancellation in entropic algebras. *Algebra Universalis*, 60(4):439–468, 2009.

[28] Michał M. Stronkowski. Embedding entropic algebras into semimodules and modules. Internat. J. Algebra Comput. to appear.

[29] Ágnes Szendrei. Modules in general algebra. In *Contributions to general algebra, 10 (Klagenfurt, 1997)*, pages 41–53. Heyn, Klagenfurt, 1998.

[30] Kôshichi Toyoda. On axioms of linear functions. *Proc. Imp. Acad. Tokyo*, 17:221–227, 1941.

FACULTY OF MATHEMATICS AND INFORMATION SCIENCES, WARSAW UNIVERSITY OF TECHNOLOGY, WARSAW, POLAND

EDUARD ČECH CENTER, CHARLES UNIVERSITY, PRAGUE, CZECH REPUBLIC
E-mail address: `m.stronkowski@mini.pw.edu.pl`

DEPARTMENT OF ALGEBRA, FACULTY OF MATHEMATICS AND PHYSICS, CHARLES UNIVERSITY, PRAGUE, CZECH REPUBLIC
E-mail address: `stanovsk@karlin.mff.cuni.cz`