SIXTH INTERNATIONAL CONFERENCE
on Discrete Mathematics and Applications
31.08.2001 - 02.09.2001, Bansko, Bulgaria

APPROACHES TO THE PROBLEM OF CONSTRUCTING FREE ALGEBRAS

SMILE MARKOVSKI, LIDIJA GORAČINOVA ILIEVA

Abstract. Free algebras are very important for studying classes of algebras, especially varieties of algebras, since they express the essential properties of the algebras of a whole class. They are significant not only for the universal algebra itself, but also for the topology, computer science, the research connected with process algebras etc. Therefore, finding convenient constructions of free algebras is an important task. There is no general method to resolve the problem of describing free algebras efficiently enough in each particular case. In this paper we distinguish several approaches to this problem for varieties of algebras, which turn out to be useful in many cases.

Given a variety $\mathcal{V}$ of algebras of some type, an algebra $\mathbf{A} \in \mathcal{V}$ is said to be free in $\mathcal{V}$ with free base B if $\mathbf{A}$ is generated by B and any mapping $\alpha : B \to C$, where $\mathbf{C} \in \mathcal{V}$, can be extended to a homomorphism $\beta : \mathbf{A} \to \mathbf{C}$, such that $\alpha(b) = \beta(b)$, for each $b \in B$. Free algebras in $\mathcal{V}$ can be obtained as quotients of the so-called term algebras by using a suitable congruence. Namely, for given type of algebras Ω and for given set B, the term algebra $\mathbf{T}_B(\Omega) = \mathbf{T}_B$ over B is build in such a way that the value of an n-ary operation f^T in $\mathbf{T}_B(\Omega)$ on the Ω-terms $t_1, \ldots, t_n$ is just the term $f(t_1, \ldots, t_n)$, i.e. $f^T(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$. The algebra $\mathbf{T}_B$ is free in the class of all Ω-algebras with free base B.
Denote by $\Theta_{\mathcal{V}}(B)$ the congruence $\bigcap\{\Theta \in Con\mathbf{T}_B \mid \mathbf{T}_B/\Theta \in \mathcal{V}\}$. Then the quotient algebra $\mathbf{F}_{\mathcal{V}}(B) = \mathbf{T}_B/\Theta$ is (isomorphic to) a free algebra in $\mathcal{V}$ with free base B. From this construction of free algebras it follows that we usually do not have clear picture how the free algebras look like. That is the reason why we need to give more convenient descriptions of free algebras in varieties of algebras. In fact, the problem of finding an effective description of free algebras in a variety $\mathcal{V} = Mod(\Sigma)$ is equivalent to the problem of giving an effective description of a congruence on the absolutely free algebra $\mathbf{T}_B$ of the corresponding type, generated by the identities Σ satisfied in $\mathcal{V}$ (i.e. $\Theta_{\mathcal{V}}(B)$). In the subsequent sections we present several ideas used for suitable

1991 *Mathematics Subject Classification.* Primary 08B20.

constructions of free algebras. Of course, they can not be used in general, but we find out that they can be helpful in attacking the problem of constructing free algebras in many varieties. To each of the given approaches we associate an example of variety where that idea works well.

1. Construction of the congruence $\Theta_{\mathcal{V}}(B)$

There are only a few varieties in which we can use directly the congruence $\Theta_{\mathcal{V}}(B)$. For instance, $\Theta_{\mathcal{V}}(B)$ is $\Delta_B \cup \nabla_{T_B \setminus B}$ for the variety of groupoids defined by the identity $xy = uv$. In most of the cases, the description of the congruence $\Theta_{\mathcal{V}}(B)$ is not that simple, since the defining identities induce new ones which can not always be perceived easily. On the other hand, dealing with classes and checking whether two elements of T_B are representatives of the same class or not, create additional difficulties. Therefore, we usually turn to some other ways that might give the same result.

2. Term reduction

Closely connected to the previous approach is a determination of a procedure for choosing a subset R of the set T_B of all terms, with the following properties:

(i) for every term $t \in T_B$ there exists exactly one term $r(t) \in R$ and $t = r(t)$ is an identity in $\mathcal{V}$;
(ii) if $t \in R$ then every subterm of t belongs to R.

We call this set R a set of representatives or reduced terms. The existence of an algorithm, such that for each term this algorithm determines the corresponding reduced term, also leads to the definition of the operations on R, thus resulting in a free algebra in $\mathcal{V}$.

A Steiner loop, or a sloop, is an algebra $(L, \cdot, 1)$, where $\cdot$ is a binary operation and 1 is a constant, that satisfies the following identities:

$$1 \cdot x = x$$
$$x \cdot y = y \cdot x$$
$$x \cdot (x \cdot y) = y$$

Denote by $\mathcal{V}_{sl}$ the variety of sloops and let $\mathbf{T}_B = (T_B, \cdot, 1)$ be the term algebra of the corresponding type over a set of free generators B. Let us assume that the set B is well ordered. Then we can extend it to well ordering on T_B by induction on the length of terms ($|1| = 1, |t| = 1$, for $t \in B$, $|t_1 \cdot t_2| = |t_1| + |t_2|$), choosing the element 1 to be the smallest in T_B.

The reduction is defined inductively:

$r(t) = t$, for $t \in B \cup \{1\}$, and

$$r(t_1 \cdot t_2) = \begin{cases} 1: & r(t_1) = r(t_2) \\ r(t_1): & r(t_2) = 1 \\ r(t_2): & r(t_1) = 1 \\ t_3: & r(t_2) \in \{r(t_1) \cdot t_3, t_3 \cdot r(t_1)\} \\ t_3: & r(t_1) \in \{r(t_2) \cdot t_3, t_3 \cdot r(t_2)\} \\ r(t_2) \cdot r(t_1): & r(t_2) < r(t_1) \textit{ and none of the previous holds} \\ r(t_1) \cdot r(t_2): & \textit{in the rest of the cases.} \end{cases}$$

Define an operation $*$ on $R = r(T_B)$ by $t_1 * t_2 = r(t_1 \cdot t_2)$.

Theorem ([5]) The algebra $(R, *, 1)$ is free in $\mathcal{V}_{sl}$ with free base B.

3. Direct approach: construction by choosing a free algebra - model

In some cases, when the structure of the free algebra is recognizable, the free algebra can be defined in some way directly, by choosing an algebra - model. That is the case of well known free monoid - the set of all words over a given alphabet with the operation concatenation. Instead of the congruence, it is much easier to define a groupoid with some special structure, and then prove that it is a free monoid. Here we state another example which fully expresses the significance of the identities, i.e. that the discovering of all the relevant identities solves the problem of the construction.

Let $\mathcal{V}_i$ be the variety of all groupoids with the identities:

$$x \cdot xy = y$$
$$xy \cdot y = yx$$

Besides the defining identities, the following ones hold in $\mathcal{V}_i$:

$xy \cdot x = x \cdot yx$	$x(yx \cdot y) = yx$
$xx = x$	$yx \cdot y = x \cdot yx$
$xy \cdot yx = y$	$xy \cdot (x \cdot yx) = x$
$(xy \cdot x)x = y$	$(xy \cdot x) \cdot xy = yx$
$(xy \cdot x)y = x$	$(xy \cdot x) \cdot yx = xy$

as well as the cancellation laws and the anticommutativity.

As a consequence, we get that the groupoids in $\mathcal{V}_i$ are quasigroups. Also note that in any $\mathcal{V}_i$-quasigroup we have $x \cdot yx = xy \cdot x = yx \cdot y = y \cdot xy$. Let α be the congruence generated by the preceeding identities. In what follows, we denote by uvu the class $u(vu)/\alpha$ and use the notations "term" and "subterm" for the elements of T_B/α, too.

Let $F_i \subseteq T_B/\alpha$ be the set of all terms that do not contain as a subterm a left-hand side of $(i) - (viii)$:

$(i)\ ss = s$	$(v)\ s \cdot sts = ts$
$(ii)\ s \cdot st = t$	$(vi)\ st \cdot sts = s$
$(iii)\ st \cdot t = ts$	$(vii)\ sts \cdot s = t$
$(iv)\ st \cdot ts = t$	$(viii)\ sts \cdot st = ts$

Define an operation $*$ on F_i in the following way. For $u, v \in F_i$, if $uv \in F_i$ then $u * v = uv$. Otherwise, if uv has the form of a left-hand side of some of $(i) - (viii)$, define $u * v$ to be the corresponding right-hand side of the identity, except in the case of (iii), i.e. when $u = wv$, then we put $u * v = v * w$. It can be shown, by induction on length of terms, that $*$ is well defined. Moreover, we have the following statement.

Theorem([1]) The groupoid $(F_i, *)$ is free in $\mathcal{V}_i$ with free base B.

4. Term rewriting

Sometimes it is convenient to describe free algebras by using term rewriting systems (TRS). In general, a TRS is a set R of rewrite rules $l_i \to r_i$, where $l_i, r_i \in T_B$ $(i \in I)$. It generates a relation $\to_R$ on T_B in the following way: $u \to_R v$ iff there exists a rewrite rule $l \to r$ and a substitution σ, such that $l\sigma$ is the subterm of u in some position p in u, and v is the term which is obtained by its replacement by $r\sigma$. The transitive and reflexive closure of $\to_R$ is called a rewrite relation and is denoted by $\to_R^*$. For our purpose, we require two additional properties:

$confluence:$

$$(\forall u, v, w \in T_B)(\exists z \in T_B)(u \to_R^* v \wedge u \to_R^* w \Longrightarrow v \to_R^* z \wedge w \to_R^* z)$$

$termination:$

$$there\ is\ no\ infinite\ sequence\ u_0 \to u_1 \to u_2 \to \ldots,\ such\ that\ u_i \neq u_{i-1}.$$

In this case we say that the TRS is complete. Such a system ensures functionality, that is, the existence of an algorithm for transformation of each term into its unique reduced one.

One implementation of TRS for obtaining free algebras is given in the next example.

Let $\mathcal{V}_s$ denote the variety of semigroups with the identity $xxy = y$. As a consequence of the identity $xyz = yxz$ that holds in $\mathcal{V}_s$, the free semigroup over $B = \{b_1, b_2, b_3, \dots\}$ can be described by the following TRS:

$$b_ib_ib_j \to b_j, \text{ for all } i, j$$
$$b_jb_ib_k \to b_ib_jb_k, \text{ for all } i, j, k, \text{ such that } i < j.$$

(For other, rather direct, descriptions of the free $\mathcal{V}_s$-semigroups, see [4].)

5. Construction by a chain of partial groupoids

When we are not able to determine the needed identities, it is sometimes convenient to "build" the free algebra step by step, as an union of partial algebras, moving from terms with smaller length to terms with greater length. This approach can be useful in the case when the number of the identities which should be taken into consideration is not finite. We illustrate this method with the variety of groupoids $\mathcal{V}_{st} = Mod(xy \cdot y = yx)$, determined by one of the Stein's identities.

Let $B \neq \emptyset$ be an arbitrary set, $R_1 = B_1 = B$, $*_1 = \emptyset$ and let B_i, R_i, and partial operation $*_i$ on R_i be defined for $i \in \{1, 2, \dots, n\}$. We also define the following subsets of T_B:

$$C_{n+1} = \{uv \mid u \in B_i,\ v \in B_j,\ i \geq j,\ i + j = n + 1,\ u *_n v \text{ is defined}\},$$

$$D_{n+1} = \Big(\bigcup_{\substack{i \geq j, \\ i+j=n+1}} B_iB_j\Big) \setminus C_{n+1}, \qquad D'_{n+1} = \{uv \mid vu \in D_{n+1}\},$$

$$B_{n+1} = D_{n+1} \cup D'_{n+1}, \qquad R_{n+1} = R_n \cup B_{n+1}.$$

Define partial operation $*_{n+1}$ on R_{n+1} by $*_{n+1} = *_n \cup \bar{*}_{n+1}$, where for $u, v \in R_{n+1}$ and $u *_n v$ not defined, $\bar{*}_{n+1}$ is determined by the following mutually exclusive rules:

(1) if $uv \in B_{n+1}$, then $u \bar{*}_{n+1} v = uv$;
(2) if $u = v = w^2 \in B_{n+1}$, then $u \bar{*}_{n+1} v = w^2$;
(3) if $u = wv \in B_{n+1}$, then $u \bar{*}_{n+1} v = vw$;
(4) if $u = pq \in B_{n+1}$, $|u| > |v| > |q|$, $|v| \geq |p|$ and $v *_n q = p$, then $u \bar{*}_{n+1} v = p$;
(5) if $v = u^2 \in B_{n+1}$, then $u \bar{*}_{n+1} v = u^2$;
(6) if $v = wu, u \neq w$ and $uw \cdot u \in B_{n+1}$, then $u \bar{*}_{n+1} v = uw \cdot u$;

(7) if $v = pq$, $|v| > |u| > |q|$, $|u| \geq |p|$, $u *_n q = p$ and $pu \in B_{n+1}$, then $u \bar{*}_{n+1} v = pu$.

Note that in any $\mathcal{V}_{st}$-groupoid $(G, *)$, $(x*y)*x = x*(y*x)$ and $(x*x)*(x*x) = (x*x)$ hold. These identities and the defining one justify the rules (2), (3), (5) and (6). The motivation for including (4) and (7) is the following: if $u = p*q$ and $v*q = p$, for some $p, q \in G$, then $u*v = (p*q)*v = ((v*q)*q)*v = (q*v)*v = v*q = p$, and after that $v*u = (u*v)*v = p*v$.
Partial operations are well defined and partial groupoids $(R_n, *_n)$, $n \geq 1$, satisfy the following properties:

The groupoid $(R_n, *_n)$ is a partial subgroupoid of $(R_{n+1}, *_{n+1})$, for each $n \geq 1$.

The product $u *_{2n} v$ is defined for all $u, v \in R_n$ and every $n \geq 1$.

If $u, v \in R_n$ and both $(u *_n v) *_n v$ and $v *_n u$ are defined, then these products are equal.

Let $R = \bigcup_{n\geq 1} R_n$ and $* = \bigcup_{n\geq 1} *_n$. According to the stated properties, we have the following:

$(R, *)$ is a $\mathcal{V}_{st}$-groupoid.

By induction on the length of terms, the next theorem can also be proved:

Theorem([1]) $(R, *)$ is free in $\mathcal{V}_{st}$ with free base B.

The basic reason for this approach here is the fact that at first we have observed some pattern in the way of forming the identities, but we didn't know their common shapes. But, after we had obtained this construction which could serve as an algorithm for generation of the identities, we were in a position to give another, direct description of the free groupoids, just as in the previous example ([3]).

6. Construction by a sequence of successive approachings

In some sense opposite to the preceding approach, but certainly more natural, is the construction of free algebras by a sequence of successive approachings. The attempt to construct a free algebra according to defining identities often results in some new identities which should be taken into consideration. The examination of the corrected algebra might result in some other identities, and so on. In many cases, this process must not come to an end after a finite number of steps. But if it is possible to determine the forms of the identities, one can define a sequence of algebras with the property that the universe of each algebra contains the universe of the next one in the sequence. These algebras approach to the wanted free algebra which can be defined as their intersection. In this way the free groupoid in the variety $\mathcal{V} = Mod(x \cdot (y \cdot yx) = x)$ was obtained. Its corresponding sequence of groupoids $(G_i, *_i)$ is stated as follows.

$G_1 = \{t \in T_B \mid t$ doesn't contain a subterm of the form $p(q \cdot qp)\}$

$$u *_1 v = \begin{cases} u: & v = t \cdot tu \\ uv: & otherwise, \end{cases}$$

$G_2 = \{t \in G_1 \mid t$ doesn't contain a subterm of forms $pp \cdot p,\ (p \cdot pq) \cdot qq\}$

$$u *_2 v = \begin{cases} u: & v = t \cdot tu \\ u: & u = vv \\ u: & u = p \cdot pq, v = qq \\ uv: & otherwise, \end{cases}$$

$G_3 = \{t \in G_2 \mid t$ doesn't contain a subterm of forms $p(pp \cdot pp),\ pp \cdot (q \cdot qp)(q \cdot qp)\}$

$$u *_3 v = \begin{cases} u: & v = t \cdot tu \\ u: & u = vv \\ u: & u = p \cdot pq, v = qq \\ u: & v = uu \cdot uu \\ u: & u = pp, v = (q \cdot qp)(q \cdot qp) \\ uv: & otherwise. \end{cases}$$

The above sequence of groupoids indicates the following definition to be given. For a term t, define inductively terms t^{2^n} for $n \geq 0$ by $t^1 = t$ and $t^{2^{n+1}} = t^{2^n} \cdot t^{2^n}$. Now, for $n \geq 2$, we continue by stating

$G_{2n} = \{t \in G_{2n-1} \mid t$ doesn't contain a subterm of the form $(q \cdot qp)^{2^{n-1}} \cdot p^{2^n}\}$

$$u *_{2n} v = \begin{cases} u: & u = v^2 \\ u: & v = u^4 \\ u: & u = (q \cdot qp)^{2^{m-1}},\ v = p^{2^m}, m \in \{1, 2, \ldots, n\} \\ u: & u = p^{2^{m-1}},\ v = (q \cdot qp)^{2^{m-1}}, m \in \{1, 2, \ldots, n\} \\ uv: & otherwise, \end{cases}$$

$G_{2n+1} = \{t \in G_{2n} \mid t$ doesn't contain a subterm of the form $p^{2^n} \cdot (q \cdot qp)^{2^n}\}$

and the operation $*_{2n+1}$ on G_{2n+1} is defined as $*_{2n}$ with the difference $m \in \{1, 2, \ldots, n+1\}$ instead of $m \in \{1, 2, \ldots, n\}$ in the case of $u = p^{2^{m-1}}$, $v = (q \cdot qp)^{2^{m-1}}$.

Let $G = \bigcap_{n \geq 1} G_n$ and define an operation $*$ on G by $u * v = u$ if uv is a term which is not contained in some G_k and $u * v = uv$ in the rest of the cases, i.e. when $uv \in G$.

Theorem([1]) The groupoid $(G, *)$ is free in $\mathcal{V}$ with free base B.

7. Replacement scheme

Another approach for constructing free algebras is by using a suitably chosen set of ordered pairs of terms, the so-called replacement scheme. For a given set J of ordered pairs of terms, let A_J denote the set of all terms t such that whenever $(u, v) \in J$ and σ is a substitution, then $u\sigma$ is not a subterm of t. In what follows, we state the properties needed to be satisfied by a set J of ordered pairs of terms, so that this could be a replacement scheme for a variety $\mathcal{V}$. In order to be concise, we give the definition by [2], which concerns the case of groupoids.

(1) if $(u, u'), (v, v') \in J$, σ, τ are substitutions such that $u\sigma = v\tau$ and every proper subterm of $u\sigma$ belongs to A_J, then $u'\sigma = v'\tau$;

(2) if $(u, u') \in J$, σ is a substitution and every proper subterm of $u\sigma$ belongs to A_J, then $u'\sigma \in A_J$;

(3) if $(u, u') \in J$, then u is not a variable.

If J is a replacement scheme, then we can define a mapping $J^* : T_B \to A_J$ in the following way: if $t \in B$, we put $J^*(t) = t$; if $t = t_1 t_2$ and $J^*(t_1)J^*(t_2) \in A_J$, let $J^*(t) = J^*(t_1)J^*(t_2)$; and if $t = t_1 t_2$ and $J^*(t_1)J^*(t_2) = u\sigma$ for some $(u, u') \in J$ and a substitution σ, let $J^*(t) = u'\sigma$.
If J is a replacement scheme, we define an operation $\circ$ on A_J by $a \circ b = J^*(ab)$. We say that $(A_J, \circ)$ is a groupoid connected with J.
Let $\mathcal{V}$ be a variety of groupoids. A replacement scheme J is said to be a replacement scheme for $\mathcal{V}$ if, besides (1)-(3), J satisfies the following properties:

(4) if $(u, u') \in J$, then the identity $u = u'$ is satisfied in $\mathcal{V}$;

(5) $(A_J, \circ)$ belongs to $\mathcal{V}$.

This approach facilitates the proving. For instance, by using a replacement scheme the checking of universal mapping property is avoided. Nevertheless, the main problem connected with constructions of free algebras, that is, the obtaining of all the relevant identities, still remains.
A large number of varieties with the corresponding replacement schemes are stated in the mentioned paper [2]. The author has limited himself to varieties

of groupoids defined by a single identity of the form $x = t$, where x is a variable and t is a term with length not greater than four.

References

[1] L. Goračinova Ilieva: *Free groupoids*, MSc. thesis, Skopje, 2001

[2] J. Ježek, *Free Groupoids in Varieties Determined By a Short Equation*, Acta Universitatis Carolinae - Math. et Phys. Vol.23 No1, 1982, 3-24

[3] S. Markovski, L. Goračinova Ilieva, A. Sokolova: *Free groupoids defined by the identity* $(xy)y = yx$, Proceedings of the 10th Congress of Yugoslav Mathematicians, Belgrade, 21-24.01.2001, 173-176

[4] S. Markovski, A. Sokolova, L. Goračinova Ilieva: *On semigroups with the identity* $xxy = y$, Publication de l'Inst. Math., Belgrade (in print)

[5] S. Markovski, A. Sokolova: *Free Steiner loops*, Glasnik Matematički Vol.36 (56) (2001), 85-93

(Smile Markovski) The Faculty of the Natural Sciences and Mathematics, Institute of Informatics, P.O.Box 162, Skopje, Republic of Macedonia

E-mail address: `smile@pmf.ukim.edu.mk`

(Lidija Goračinova Ilieva) Pedagogical Faculty, Štip, Republic of Macedonia

E-mail address: `fildim@mt.net.mk`

http:\\ii.pmf.ukim.edu.mk\crypto\