Description of the project: Clones on groups [1]

Peter Mayr
Institut für Algebra, Johannes Kepler Universität Linz, Austria
peter.mayr@jku.at

March 1, 2006

Abstract: For an arbitrary algebraic structure (universal algebra), polynomial functions are those that can be obtained from the constant functions and the projection operations using the operations of this algebraic structure. This concept is a true generalization of the well-known concept of polynomial functions on commutative rings (e.g., polynomial functions on the real numbers) and has been studied since the 50s of the last century. “Rings are particular algebraic structures whose operations include the operations of a group. Such algebras have a group reduct or, using a dual point of view, they are expanded groups. We will mainly focus on them.

We aim to solve open problems in universal algebra that are connected to the following: Is there a finite group that has more than countably many expansions such that their sets of polynomial functions are pairwise distinct? Our starting point is a conjecture by P. Idziak: On a fixed finite set whose size is squarefree there exist only finitely many clones containing a group operation and all constant functions. While E. Aichinger and the author already proved this conjecture to be true for sets whose order is a product of 2 distinct primes, the general case is still open.

The main problem in this kind of research is to characterize polynomial functions on specific algebraic structures. In the results existing so far, polynomial functions are determined in terms of the lattice of congruences (ideals) of the algebra together with the commutator structure of these congruences. One aspect of this research is it to determine which parameters of a certain class of algebras suffice to describe the polynomial functions. Usually it is not necessary to know the actual operations. For example, although the operations of the field of size 2 and the Boolean algebra of size 2 are totally different, their polynomial functions are the same, namely all functions on the 2-element set.

When dealing with functions on expanded groups, the group operation allows us to use powerful methods from classical algebra, like group theory and module theory, in addition to the tools from universal algebra, like the theory of commutators on congruences. We hope that this approach will provide new results for expanded groups which can then serve as a guideline for more general algebras.

[1] 2000 AMS Mathematics Subject Classification: 08A40

1. Positioning of this project

Every function from $\{0,1\}^k$ to $\{0,1\}$ can be expressed using the Boolean operations AND, OR, and NOT. Let $\mathbf{A}$ be some algebraic structure (ring, group, ...) and let $f : A^k \to A$ be a function. How can we tell whether there is a word $w = w(x_1, \ldots, x_k)$ in this algebra whose interpretation in $\mathbf{A}$ is f? If such a word (term) exists, then f is said to be a *term function* of $\mathbf{A}$ (see [**18**]). The set of all term functions on $\mathbf{A}$ is called the clone $\mathrm{Clo}(\mathbf{A})$ of $\mathbf{A}$. As for our example of the Boolean algebra $\langle \{0,1\}, \wedge, \vee, \neg \rangle$ above, every function is a term function. The clone of an algebra $\mathbf{A}$ is an important parameter determining the properties of $\mathbf{A}$ (e.g. the subalgebras of $\mathbf{A}^k$ for all $k \in \mathbb{N}$, whether $\mathbf{A}$ is abelian, ...). Algebras that have the same term functions, like the Boolean algebra $\langle \{0,1\}, \wedge, \vee, \neg \rangle$ and the Boolean ring with one $\langle \{0,1\}, +, \cdot, 1 \rangle$, are said to be *term-equivalent*.

The clone $\mathrm{Pol}(\mathbf{A})$ of polynomial functions on an algebraic structure $\mathbf{A}$ is closely related to $\mathrm{Clo}(\mathbf{A})$. A function is a *polynomial function* if it can be obtained from the constant functions and the projection operations using the operations of the algebra $\mathbf{A}$ (see [**18**, Definition 4.4]). This concept, which has been studied, e.g., in [**16, 18**], is a generalization of the concept of polynomial functions on commutative rings.

Two algebras $\mathbf{A}$ and $\mathbf{B}$ are called *polynomially equivalent* if $\mathrm{Pol}(\mathbf{A}) = \mathrm{Pol}(\mathbf{B})$. Given a finite set A, one may ask how many algebras exist on the universe A that are pairwise term inequivalent or polynomially inequivalent respectively. If $|A| \geq 3$, then one can define continuum many polynomially inequivalent algebras on A [**1**]. However in general it is not known how many algebras on a fixed set A have a *Mal'cev operation* (i.e., a ternary operation m that satisfies $m(x,x,y) = m(y,x,x) = y$ for all $x, y \in A$) or a group operation as term operation. We note that for every group $\langle G, + \rangle$ the function $m(x,y,z) = x - y + z$ is a Mal'cev operation contained in $\mathrm{Clo}(\langle G, + \rangle)$.

From Post's characterization of clones on a 2-element set [**19**], one obtains that there are only finitely many term inequivalent Mal'cev algebras of size 2. P. Idziak proved that the number of polynomially inequivalent Mal'cev algebras on a set of size k is finite if and only if $k \leq 3$ in [**10**]. In [**5**] A. Bulatov showed that the term functions on every 3-element Mal'cev algebra $\mathbf{A}$ are characterized by the subalgebras of the product $\mathbf{A} \times \mathbf{A} \times \mathbf{A} \times \mathbf{A}$. As a consequence he obtained that there are 1129 term inequivalent Mal'cev algebras of size 3. Recently, in [**13**], K. Kearnes and Á. Szendrei proved that term functions on a group $\mathbf{G}$ whose Sylow subgroups are abelian are determined by the subgroups of $\mathbf{G} \times \mathbf{G} \times \mathbf{G}$.

In this project we will mainly focus on a certain class of Mal'cev algebras that contains all groups, namely on *expanded groups*; these are algebras that have a group operation among their fundamental operations. An expanded group of prime order is necessarily simple and consequently either polynomially complete or polynomially equivalent to the cyclic group. A. Bulatov proved in [**6**] that the number of polynomially inequivalent expansions of groups of order p^2 is countably infinite for every prime p.

We hope that our research will contribute to the solution of the following open problems:

(1) (R. McKenzie) On a finite set A, determine the number of clones containing a Mal'cev operation.

(2) Is there a finite group $\langle G, +\rangle$ such that there are more than countably many polynomially inequivalent expansions of $\langle G, +\rangle$?

Studying polynomial functions on general algebraic structures has a long tradition in Austria starting with Nöbauer's work (cf. [**16**]). Currently there are 3 Austrian centers of research in universal algebra: a group led by M. Goldstern at the TU Vienna which is mainly concerned with set theory and clone theory, the University of Klagenfurt, and the author's home institution led by G. Pilz at the University of Linz. The topics of the present proposal are in the mainstream of Austrian algebraic research. Currently the author also carries out some ongoing joint work on polynomial functions on infinite groups with Josef Schicho (Radon Institute for Computational and Applied Mathematics at Linz) and Günter Landsmann (RISC, Hagenberg) [**14, 15**].

2. Goals of this project

CONJECTURE 1 (P. M. Idziak, Conjecture 9 in [**10**]). *Let n be a squarefree natural number, and let $\mathbf{A}$ be an expansion of the group $\langle \mathbb{Z}_n, +\rangle$. Then $\operatorname{Pol}(\mathbf{A})$ is completely determined by the lattice of congruences of A, denoted by $\mathbf{Con\,A}$, and the commutator operation (in the sense of [**18**]) on the congruences. In particular the number of polynomially inequivalent expansions of $\langle \mathbb{Z}_n, +\rangle$ is finite.*

In 2005 E. Aichinger and I verified Conjecture 1 for the case of expansions of groups whose order is a product of 2 distinct primes p and q. In fact we obtained that there are 17 polynomially inequivalent expansions of $\langle \mathbb{Z}_{pq}, +\rangle$ (see [**4**], the result was presented at the conference on universal algebra and lattice theory, Szeged, July 2005). The proof makes use of universal algebra, module theory, and representation theory of finite groups – with the last one prominently closing the final gap. The following lemma is central for our solution.

LEMMA 2 (cf. [**4**]). *Let $\mathbf{V}$ be an expansion of the group $\langle \mathbb{Z}_{pq}, +\rangle$ for distinct primes p and q with a unique nontrivial proper ideal M. Let $k \in \mathbb{N}$, and let $f : V^k \to M$. If f is constant on the cosets of M^k in V^k, then $f \in \operatorname{Pol}(\mathbf{V})$.*

For a nonabelian monolith M, Lemma 2 is obvious from [**9**]. If M is abelian but not central in $\mathbf{V}$, then the result follows using the techniques developed in [**7**] or [**11**]. Only the remaining case that the monolith is central in $\mathbf{V}$ cannot be dealt with by using known results in universal algebra. It is here that representation theory of groups can be applied successfully. The assertion of the lemma follows from an analysis of the set of functions

$$\{f : V^k \mapsto M \mid f(x+m) = f(x) \text{ for all } x \in V, m \in M\} \tag{2.1}$$

considered as module over some appropriately chosen group algebra.

The result for expansions of $\langle \mathbb{Z}_{pq}, +\rangle$ has since been crucial in my proof of Idziak's conjecture for expansions of groups of squarefree order whose congruences are linearly ordered. I have already presented this result at the 71st Workshop on General Algebra (AAA71) at Bedlewo in February 2006. The problem has increasingly received interest in the scientific community. In one of the main talks at the Novi Sad Algebraic Conference in July 2005, Ágnes Szendrei mentioned an alternative approach to our solutions in [**4**]. In this collaborative project we want to combine the different techniques to obtain a better understanding of Idziak's conjecture and its implications. Presently there is neither proof nor falsification of Conjecture 1 in its full generality available.

The following problem is a variation of the implicit questions in Conjecture 1.

PROBLEM 3. *Determine* Clo($\mathbf{V}$) *for finite expanded groups* $\mathbf{V}$ *of squarefree order.*

In [**13**] Keith Kearnes and Ágnes Szendrei proved that term functions on a group $\mathbf{G}$ whose Sylow subgroups are abelian are determined by the subgroups of $\mathbf{G} \times \mathbf{G} \times \mathbf{G}$. They further examined the connections between term functions and subgroup lattices of powers of groups in [**12**]. Obviously expanded groups of squarefree order have cyclic Sylow subgroups. It remains to be investigated what insight the techniques in [**13**] (possibly in combination with our methods in [**4**]) can provide for Problem 3.

Polynomial clones on finite simple congruence permutable algebras are fully determined in [**9**]. We propose a natural follow-up question whose importance for understanding clones on more complex algebras became apparent again when studying Conjecture 1 (cf. Lemma 2).

PROBLEM 4. *Determine polynomial functions on Mal'cev algebras with* 3 *congruences.*

In a specialized version of Problem 4, I want to consider expanded groups $\mathbf{V}$ with a unique non-trivial proper ideal M such that

1. M is central in $\mathbf{V}$,
2. $\mathbf{V}/M$ is abelian, and
3. $|M|$ and $|V : M|$ are relatively prime.

It is expected that for this "nilpotent" case Pol($\mathbf{V}$) is determined by the congruences of $\mathbf{V}$ and their commutators. It has yet to be studied whether the techniques from representation theory can be applied to obtain a version of Lemma 2 for this case. With Problem 4 as a first step, I then want to generalize the setting of Conjecture 1 as follows.

PROBLEM 5. *Determine the polynomial (term) functions on expanded groups* $\mathbf{V}$ *whose ideal lattice has the following property: for all ideals* I_1, I_2, J_1, J_2 *such that* I_2 *covers* I_1 *and* J_2 *covers* J_1*, either* $|I_2 : I_1|$ *and* $|J_2 : J_1|$ *are relatively prime or* $I_1 = J_1$ *and* $I_2 = J_2$*.*

The assumption that distinct minimal sections in the congruence lattice of $\mathbf{V}$ have relatively prime orders is certainly satisfied on expanded groups of squarefree order. This condition implies in particular that $\mathrm{Pol}(\mathbf{V})$ operates in a distinct way on 2 distinct minimal sections of $\mathbf{Con}\,(\mathbf{V})$.

The problems proposed in this section are actually instances of more general questions on algebras with Mal'cev operations. The final goal is to provide answers in the more general setting (cf. McKenzie's problem (1) stated in the previous section). However, a preliminary restriction to algebras with group operation seems reasonable as long as this case is wide open. Eventually we want to generalize our results to Mal'cev algebras.

Bibliography

[1] I. Ágoston, J. Demetrovics, and L. Hannák. On the number of clones containing all constants (a problem of R. McKenzie). In *Lectures in universal algebra (Szeged, 1983)*, volume 43 of *Colloq. Math. Soc. János Bolyai*, pages 21–25. North-Holland, Amsterdam, 1986.

[2] E. Aichinger, F. Binder, J. Ecker, P. Mayr, and C. Nöbauer. *SONATA - system of near-rings and their applications, GAP package, Version 2*, 2003. (`http://www.algebra.uni-linz.ac.at/Sonata/`).

[3] E. Aichinger and P. Mayr. Polynomial functions and endomorphism near-rings on certain linear groups. *Communications in Algebra*, 31(11):5627–5651, 2003.

[4] E. Aichinger and P. Mayr. Polynomial clones on groups of order pq, 2005. Submitted.

[5] A. A. Bulatov. Three-element mal'tsev algebras. *Acta Sci. Math. (Szeged)*, XX:519–550, 2005.

[6] Andrei A. Bulatov. Polynomial clones containing the Mal′tsev operation of the groups $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$. *Mult.-Valued Log.*, 8(2):193–221, 2002. Multiple-valued logic in Eastern Europe.

[7] Y. Fong and K. Kaarli. Unary polynomials on a class of groups. *Acta Sci. Math. (Szeged)*, 61(1-4):139–154, 1995.

[8] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002. (`http://www.gap-system.org`).

[9] J. Hagemann and C. Herrmann. Arithmetical locally equational classes and representation of partial functions. In *Universal Algebra, Esztergom (Hungary)*, volume 29, pages 345–360. Colloq. Math. Soc. János Bolyai, 1982.

[10] P. M. Idziak. Clones containing Mal'tsev operations. *Internat. J. Algebra Comput.*, 9(2):213–226, 1999.

[11] P. M. Idziak and K. Słomczyńska. Polynomially rich algebras. *J. Pure Appl. Algebra*, 156(1):33–68, 2001.

[12] Keith A. Kearnes and Ágnes Szendrei. Groups with identical subgroup lattices in all powers. *J. Group Theory*, 7(3):385–402, 2004.

[13] Keith A. Kearnes and Ágnes Szendrei. Clones of finite groups. *Algebra Univers.*, 54(1):23–52, 2005.

[14] G. Landsmann, P. Mayr, and Schicho J. A topological criterion for polynomiality. In *Dolzmann, Seidl, Sturm (Eds.) Algorithmic Algebra and Logic. Proceedings of the A3L 2005*, pages 41–54. BOD Norderstedt, Germany, 2005.

[15] G. Landsmann, P. Mayr, and Schicho J. A topological property of polynomial functions on $\mathrm{GL}(2, \mathbb{R})$, 2005. Submitted.

[16] H. Lausch and W. Nöbauer. *Algebra of polynomials.* North-Holland, Amsterdam, London; American Elsevier Publishing Company, New York, 1973.

[17] P. Mayr. The polynomial functions on Frobenius complements, 2006. To appear in Acta Sci. Math. (Szeged).

[18] R. N. McKenzie, G. F. McNulty, and W. F. Taylor. *Algebras, lattices, varieties, Volume I.* Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987.

[19] Emil L. Post. *The Two-Valued Iterative Systems of Mathematical Logic.* Annals of Mathematics Studies, no. 5. Princeton University Press, Princeton, N. J., 1941.

[20] Ágnes Szendrei. *Clones in universal algebra*, volume 99 of *Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics].* Presses de l'Université de Montréal, Montreal, QC, 1986.