An instance of the subnear-ring membership problem

Erhard Aichinger

Department of Algebra
Johannes Kepler University Linz, Austria

Near-rings 2009, Vorau, Austria

Outline

Polynomials obtained from squaring

Which polynomials in $\mathbb{Z}[x]$ can be obtained from $1, x, x^2$ using $+$, $-$, $\circ$?

Examples

1. $x^8 = x^2 \circ x^2 \circ x^2$.
2. $2x^5 = (x + x^4)^2 - x^2 - x^8$.
3. $4x^{19} = 2x^4 + 2x^8 - 2(x^2 + x^4)^2 + \left(x^{16} + (x + x^2)^2 - x^4 - x^2\right)^2 - x^{32}$.

The problem in near-ring language

The membership problem for $\langle 1, x, x^2 \rangle$

Given A polynomial $f \in \mathbb{Z}[x]$.

Asked Does f lie in the subnear-ring of $\langle \mathbb{Z}[x], +, \circ \rangle$ that is generated by $\{1, x, x^2\}$?

Here, $\circ$ denotes functional composition. Example:
$(x^3 + x) \circ (2x^2 + 1) = (2x^2 + 1)^3 + (2x^2 + 1) = 8\,x^6 + 12\,x^4 + 8\,x^2 + 2.$

Let S be the subnear-ring of $\langle \mathbb{Z}[x], +, \circ \rangle$ generated by $1, x, x^2$.
Mathematica: The group $\langle \{f \in S \mid \deg f \leq 32\}, + \rangle$ is generated by

$$
\begin{gathered}
1, \\
x, \\
x^2, \\
2x^3, x^4, \\
2x^5, 2x^6, 4x^7, x^8, \\
2x^9, 2x^{10}, 4x^{11}, 2x^{12}, 4x^{13}, 4x^{14}, 8x^{15}, x^{16}, \\
2x^{17}, 2x^{18}, 4x^{19}, 2x^{20}, 4x^{21}, 4x^{22}, 8x^{23}, 2x^{24}, \\
4x^{25}, 4x^{26}, 8x^{27}, 4x^{28}, 8x^{29}, 8x^{30}, 16x^{31}, x^{32}
\end{gathered}
$$

Polynomials that can be obtained from $1, x, x^2$

Conjecture

A polynomial $p = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$ lies in the subnear-ring of $\langle \mathbb{Z}[x], +, \circ \rangle$ that is generated by $\{1, x, x^2\}$ if and only if for all $i \in \mathbb{N}$, c_i is a multiple of $2^{s_2(i)-1}$. ($s_2(i)$... binary digit sum of i).

Proof of the conjecture

$$M := \{\sum_{i=0}^{n} c_i x^i \,|\, n \in \mathbb{N}, c_0 \in \mathbb{N}, \text{ and } 2^{s_2(i)-1} \mid c_i \text{ for all } i \in \{1, \ldots, n\}\}.$$

We have to prove:

1. Every $m \in M$ can be obtained from $1, x, x^2$.
2. M is closed under $\circ$.

Generating a function from $1, x, x^2$

$$F := \{1, x, x^2\}$$

We show

$$\text{For all } j \in \mathbb{N} : 2^{s_2(j)-1} x^j \in \langle F \rangle \,.$$

If j is not a power of 2, choose $k \in \mathbb{N}$ such that $2^k < j < 2^{k+1}$. By the induction hypothesis, we have

$$2^{s_2(j)-2} x^{j-2^k} \in \langle F \rangle \,.$$

Hence

$$x^2 \circ \left(x^{2^k} + 2^{s_2(j)-2} x^{j-2^k} \right) \in \langle F \rangle \,.$$

Thus

$$x^{2^{k+1}} + 2^{s_2(j)-1} x^j + 2^{2 \cdot (s_2(j)-2)} x^{2(j-2^k)} \in \langle F \rangle \,.$$

Theorem

A polynomial $p = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$ lies in the subnear-ring of $\langle \mathbb{Z}[x], +, \circ \rangle$ that is generated by $\{1, x, x^3\}$ if and only if for all $i \in \mathbb{N}$, c_i is a multiple of $3^{\lfloor \frac{s_3(i)}{2} \rfloor}$.

As a consequence, $3x^2$ and $3x^4$ both lie in the near-ring generated by $\{1, x, x^3\}$.

Theorem

A polynomial $p = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$ lies in the subnear-ring of $\langle \mathbb{Z}[x], +, \circ \rangle$ that is generated by $\{x, x^2\}$ if and only if $c_0 = 0$, and for all $i \in \mathbb{N}$, c_i is a multiple of $2^{s_2(i)-1}$.

We note that neither $3x^2$ nor $3x^4$ lie in the near-ring generated by $\{x, x^3\}$ because all polynomials in this near-ring satisfy $p \circ (-x) = -(p \circ x)$.

The subnear-ring membership problem for integer polynomials

Given A finite subset F of $\mathbb{Z}[x]$, and a polynomial $f \in \mathbb{Z}[x]$.

Asked Does f lie in the subnear-ring of $\langle \mathbb{Z}[x], +, \circ \rangle$ that is generated by F?

At this moment, we do not know whether there exists an algorithm that would solve this problem.
A special case:

The completetness problem for integer polynomials

Given A finite subset F of $\mathbb{Z}[x]$.

Asked Is the subnear-ring of $\langle \mathbb{Z}[x], +, \circ \rangle$ that is generated by F equal to $\mathbb{Z}[x]$?

Given a set A and a collection F of finitary functions on A, one may ask which functions can be obtained as compositions of the functions in F. Using the terminology of universal algebra [McKenzie et al., 1987], one can state this problem as follows:

The clone membership problem

Given A set A, a subset F of $\bigcup\{A^{A^n} \mid n \in \mathbb{N}\}$, a natural number $m \in \mathbb{N}$, and a function $f : A^m \to A$.

Asked Is f a term operation of the algebra $\mathbf{A} = \langle A, F \rangle$?

If both A and F are finite, then there is an obvious way to enumerate all m-ary term operations of $\mathbf{A} = \langle A, F \rangle$. Thus there is an algorithm that solves the problem above. [Bergman et al., 1999] and [Kozik, 2008] discuss the computational complexity of the clone membership problem.

Bergman, C., Juedes, D., and Slutzki, G. (1999).
Computational complexity of term-equivalence.
Internat. J. Algebra Comput., 9(1):113–128.

Kozik, M. (2008).
A finite set of functions with an EXPTIME-complete composition problem.
Theoret. Comput. Sci., 407(1-3):330–341.

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