Algorithms for Near-rings of Non-linear Transformations *

Franz Binder, Erhard Aichinger, Jürgen Ecker, Christof Nöbauer, Peter Mayr
Department of Algebra
Johannes Kepler University Linz, Austria
Franz.Binder@algebra.uni-linz.ac.at

ABSTRACT

In this note we present some algorithms to deal with near-rings, the appropriate algebraic structure to study non-linear functions. This is similar the role of rings in the theory of linear functions or that of groups for permutations. In particular, we give efficient algorithms that deal with big near-rings that are given by a small set of generators. In this context, generating involves composition as well as pointwise addition. In the extreme case, one transformation of a group of order n can generate a set of up to n^n transformations.

Categories and Subject Descriptors

F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems—*computations on discrete structures*; I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*algebraic algorithms*; G.2 [**Mathematics and Computing**]: Discrete Mathematics

General Terms

Algorithms

Keywords

Near-rings, Non-linear transformations, Groups

1. INTRODUCTION

Important examples of *rings* are matrix-rings; these arise as linear mappings on vector spaces. In the present note, we compute with algebraic structures appropriate for dealing with non-linear mappings, namely *near-rings* [7, 6, 5].

Definition 1. A set N together with two binary operations $+$ and $\cdot$ is called a *near-ring* if

1. $(N, +)$ is a (not necessarily abelian) group.
2. $(N, \cdot)$ is a semigroup.
3. $\cdot$ is right distributive over $+$, i.e.,
   $\forall\, a, b, c \in N\colon (a + b) \cdot c = a \cdot c + b \cdot c$.

Let Γ be a group, and let $\mathrm{M}(\Gamma)$ be the set of all mappings (*transformations*) from Γ into Γ. We define $+$ and $\cdot$ on $\mathrm{M}(\Gamma)$ by $(f + g)(\gamma) := f(\gamma) + g(\gamma)$ and $(f \cdot g)(\gamma) := f(g(\gamma))$. Then $(\mathrm{M}(\Gamma), +, \cdot)$ is a near-ring, the *full transformation near-ring.* A subset N of $\mathrm{M}(\Gamma)$ is a sub-near-ring of $(\mathrm{M}(\Gamma), +, \cdot)$ if it is closed under $+$, $-$, and functional composition. We then write $N \leq \mathrm{M}(\Gamma)$ and call it a *transformation near-ring.* In fact, every near-ring can be represented as a transformation near-ring on some group Γ, but we are primarily interested in the case where Γ is small and N (very) big.

If we are given transformations $f_1, \dots, f_r$ on Γ, we would like to know how big the generated near-ring $F = \langle f_1, \dots, f_r \rangle$ is and whether a given transformation $g\colon \Gamma \to \Gamma$ lies in F. We notice that $g \in F$ whenever it can be "built up" from $f_1, \dots, f_r$. Of course, because N is intended to be big, no straightforward enumeration is applicable. In fact, near-ring theory tells us that a single transformation might on a group of size n might generate a near-ring as large as n^n ([8] contains many impressive examples). We note that a corresponding problem in group theory is solved via Sim's stabilizing chains [10]. We have no comparable tool yet, but we can solve the membership problem in important special cases, thereby extending the cases solved by [3]. And we can solve satisfactorily a variety of related problems.

Definition 2. Let N be a near-ring. Then Γ together with an endomorphism $\Phi : N \to \mathrm{M}(\Gamma)$ is called an *N-group.* N operates on Γ by $n\gamma := \Phi(n)(\gamma)$. It operates *faithfully* if the endomorphism is injective.

Thus, N-groups correspond to modules in ring theory. Of course, if N operates faithfully on Γ, it can be identified with a sub-near-ring of $\mathrm{M}(\Gamma)$ and, conversely, every sub-near-ring of $\mathrm{M}(\Gamma)$ operates faithfully on Γ by function application.

A main endeavor of this note is to find methods to establish properties of near-rings just from a small set E of generators and to avoid the usually unfeasible task of enumerating all near-ring elements. Concretely this means that a near-ring N operating on Γ might be very large, (up to $|\Gamma|^{|\Gamma|}$)

*This work has been supported by the Austrian National Science Foundation (Fonds zur Förderung der wiss. Forschung) under Grant P12911-INF. See `www.algebra.uni-linz.ac.at` for details.

but is given by a small set of generators E. We are looking for algorithms polynomial in $|\Gamma|$ and $|E|$.

We can also interpret this situation in the language of systems theory: If we are given a set $E \subseteq \Gamma^\Gamma$ of some building blocks, we consider all systems N that can be built from these using serial (composition) and parallel (addition) connections, i.e., $N = \langle E \rangle$. Typical questions in this context are:

Membership Can f be built from the blocks in E, i.e., is $f \in N$?

Realizability Can we realize all transformations using these building blocks, i.e., is $\langle E \rangle = \mathrm{M}(\Gamma)$? If so, how can we do this?

Reachability Which states can be reached using such systems, i.e., what is $N\gamma$, for any $\gamma \in \Gamma$?

Linearity Does the system happen to be linear, i.e., is N a ring?

The last two questions will turn out to be quite easy to answer the second one gets a satisfactory solution using results from near-ring theory, whereas the first question, which at first might seem to be easier, turns out to be the hardest, and we can give only a partial solution for it.

In very contrast to ring theory, no attempt on an algorithmic treatment of near-ring theory has been done so far. Therefore, in a project funded by the Austrian Science Fonds, the share package SONATA for GAP 4 has been developed (`www.algebra.uni-linz.ac.at`). This article contains a selection of those algorithms developed as part of that project that are most interesting for transformation near-rings on finite groups.

2. ORBITS AND INTERPOLATION

First, let us attack the reachability problem. Its solution, though rather simple, is the basis of all other problems solved in this note.

Problem 1. (Reachability) Let N be a near-ring given by a set E of generators, Γ an N-group, and $\gamma \in \Gamma$.

1. Compute the *orbit* $N\gamma := \{\, n\gamma \mid n \in N \,\}$.
2. For each $\eta \in N\gamma$, find $f \in N$ such that $\eta = f\gamma$.

The key result for an efficient solution of this basic problem is easy to establish. Note that a subgroup H of Γ is an N-subgroup via the restriction of the operation of N on Γ iff $NH \subseteq H$.

THEOREM 1. *Let N be a near-ring generated by a set E and operating on a group Γ. Then a subgroup H of Γ is an N-subgroup iff $EH \subseteq H$.*

PROOF. Because $E \subseteq N$, necessity is trivial. To prove sufficiency, call $f \in N$ *good* iff $fH \subseteq H$. By the assumption, all elements in E are good. If f, g are good, then $(f-g)\gamma = f\gamma - g\gamma \in H$ for all $\gamma \in \Gamma$, because H was assumed to be a subgroup. Thus $f - g$ is also good. Similarly, fg is good, and so all elements in N are good. □

This leads to an easy completion algorithm. Note that $N\gamma$ is the smallest N-subgroup of Γ containing $E\gamma$.

Algorithm 1 Computing Orbits

Let N be a near-ring operating on the group Γ.
Require: A set E generating N; $\gamma \in \Gamma$.
Ensure: $H = N\gamma$
  $H := \langle E\gamma \rangle$
  while $EH \not\subseteq H$ **do**
    $H := \langle H \cup EH \rangle$ (generated subgroup)
  end while

PROPOSITION 1. *Algorithm 1 correctly computes $N\gamma$ within $\mathrm{O}(|E|\,|N\gamma| \le \mathrm{O}(|E|\,|\Gamma|)$ operations in Γ. In particular, the size of N does not matter.*

PROOF. Correctness is immediate from the theorem. For the bound, observe that the size of H, and therefore the computing time, doubles at each step in the loop. Thus the total complexity has the same order as that for the last step, which is $O(|E|\,|N\gamma|)$. □

Note that the class of near-rings is defined by equations. Thus the whole theory for varieties applies, in particular, there are free near-rings over any set.

COROLLARY 1. *With appropriate bookkeeping, for any $\eta \in N\gamma$, Algorithm 1 can also compute $f \in N$ such that $\eta = f\gamma$. In fact, it can also construct a term in the free near-ring generated over E that represents f.*

PROOF. The necessary bookkeeping is straightforward. In the first step, each element of H has the form $e\gamma$, $e \in E$, thus has an appropriate representation by definition. If for each element $\eta \in H$ we have a representation $\eta = f_\eta\gamma$, then for each element $e\eta \in EH$, we use $f_{e\eta} := ef_\eta$. Similarly, if $\eta = \eta_1 + \ldots + \eta_m$, then we use $f_\eta = f_{\eta_1} + \ldots + f_{\eta_m}$. □

Given $\gamma, \eta \in \Gamma$, the statement $\eta \in N\gamma$ means that there is an $f \in N$ such that $f(\gamma) = \eta$. This leads us to the following problem very common in near-ring theory.

Problem 2. (k-Interpolation) Given a sequence (γ_1, η_1), $\ldots$, (γ_k, η_k) of points in $\Gamma \times \Gamma$ and a near-ring N operating on Γ, we want to know whether there is (and if so, find) a function $f \in N$ such that $f(\gamma_i) = \eta_i$ for all $i = 1, \ldots, n$.

Obviously, Algorithm 1 solves the 1-interpolation problem. In fact, the same algorithm can also be used to solve higher interpolation problems, as can be easily seen as follows. If Γ is an N-group then Γ^2 is an N group, too, in a natural way by defining the operation as $f(a,b) := (fa, fb)$. Similarly each Γ^k is an N-group. With this definition, $(c,d) \in N(a,b)$ just means that there exists $f \in N$ such that $f(a) = c$ and $f(b) = d$, which is the 2-interpolation property.

PROPOSITION 2. *The k-interpolation problem can be solved within $\mathrm{O}(|E|\,|\Gamma|^k)$ operations.*

PROOF. This follows immediately from Proposition 2.2, using the operation defined above and applying Algorithm 1 to compute $N\big((\gamma_1,\dots,\gamma_k)\big)$ and to decide whether (and find out how) $(\eta_1,\dots,\eta_k)$ is in this orbit. $\square$

Thus, the k-interpolation-problem can be solved in time polynomial in $|E|$ and in $|\Gamma|$. Unfortunately, the solution is exponential in k. In particular, for the $|\Gamma|$-interpolation problem, which just means to test whether a given transformation is in N, we only get the bound $\mathrm{O}(|E|\,|\Gamma|^{|\Gamma|})$, which essentially means to enumerate all elements of N. But see Section 8 for a different approach that works in many important cases.

3. FINDING THE IDENTITY IN A NEAR-RING OF TRANSFORMATIONS

A near-ring need not have an identity. Thus we need a method to find out whether a near-ring contains an identity, and, in the affirmative case, how it looks like. We give a solution for near-rings N faithfully operating on a group Γ. Without loss of generality, we assume that $N \le \mathrm{M}(\Gamma)$. Again, think of Γ to be small, and N to be big, but generated by a small subset E.

Clearly, if the identity transformation id is an element of N, the near-ring has an identity and it is id. The converse, in general, is not true, as the following counterexample demonstrates:

Example 1. Let $\Gamma = \mathbb{Z}_2 \times \mathbb{Z}_2$ be Klein's 4-group and $N = (\{\bar{0}, \pi_1\}, +, \circ)$, where $\bar{0}$ denotes the zero mapping, and π_1 the projection onto the first component, i.e., $\pi_1(x,y) = (x,0)$. Then N is a near-ring with identity π_1, in fact it is isomorphic to the residue class field of integers modulo 2. But $\pi_1 \neq \mathrm{id}_{\mathbb{Z}_2\times\mathbb{Z}_2}$

Nevertheless, the identity in N (if it exists) cannot be too far from the identity transformation. We are going to develop some necessary conditions for a transformation i to be the identity of N.

First, we use that i is a left identity. Thus, for all $n \in N$, and all $x \in \Gamma$, we have $i(nx) = (in)x = nx$. Hence

$$i|_{N\Gamma} = \mathrm{id}|_{N\Gamma} \tag{1}$$

is a necessary condition for i to be the near ring's identity. This means that at least on $N\Gamma$ it has to behave like the identity mapping. And $N\Gamma$ can be computed efficiently by Algorithm 1.

Next, we use that i is a right identity. Thus, for all $f \in N$ and all $x \in \Gamma$, we have $f(ix) = (fi)x = fx$, or, equivalently, $ix \in f^{-1}(\{fx\})$. So $ix \in I_x := N\Gamma \cap \bigcap_{f\in N} f^{-1}(\{fx\})$.

Of course, we cannot compute such an intersection if we want to avoid computing all elements of N. Fortunately, the condition $f(ix) = fx$ only has to be tested for the set E of generators of N, because from $f(ix) = fx$ and $g(ix) = gx$, we get immediately that $fg(ix) = fgx$ and $(f+g)(ix) = (f+g)x$. Thus we just have to go through the elements of $N\Gamma$ and find out all the elements y for which $fy = fx$ for all $f \in E$.

Finally, we use that i must take some unique value for each $x \in \Gamma$. Thus, if for some $x \in \Gamma$ the set I_x is empty, N cannot have an identity. Similarly, if I_x contains more than one element for some $x \in \Gamma$, N cannot have an identity, too: Suppose, $a, b \in I_x$. Then $a, b \in N\Gamma$ and $\forall\, n \in N$: $na = nx = nb$. In particular, $ia = ib$. But a and b are from $N\Gamma$ (whereupon i acts as identity transformation, by (1)), so $a = ia = ib = b$.

Summarizing, if N is generated by E, then

$$\forall x \in \Gamma\colon\ I_x := |N\Gamma \cap \bigcap_{n\in E} n^{-1}(nx)| = 1. \tag{2}$$

and $I_x = \{i(x)\}$ is the single element. Conversely, if this condition is satisfied, we define $i(x)$ as the unique element of I_x. If this i is contained in N, it is its identity. Otherwise N has no identity.

Condition (2) uniquely determines ix at every point x (or contradicts the existence of an identity). If the candidate i computed using (2) happens to be an element of N, then it is the identity of N. This is formulated in Algorithm 2.

Algorithm 2 Identity

Let N be a near-ring of transformations on the group Γ.
Require: E a set of generators of N.
Ensure: Find an identity, if there is one.

```
for x ∈ Γ do
  I_x := ⋂_{n∈E} (NΓ ∩ n^{-1}nx);
  if |I_x| ≠ 1 then
    return (N has no identity);
  end if
  Define i(x) to be the unique element in I_x.
end for
if i ∈ N or N contains an identity then
  return (i is the identity of N);
else
  return (N has no identity);
end if
```

So, for a near ring of transformations on a group, we can find its identity (if it has one) and the decision problem of testing whether is has one has been reduced to the problem of deciding membership of a single transformation. The complexity of this reduction is the same as the complexity of computing $N\Gamma$.

4. LINEARITY

An element f of a near-ring N is called *distributive on* N iff $f(g+h) = fg + fh$ for all $f, h \in N$. A near-ring is *distributive* iff all its elements are distributive on N. It is called *abelian* iff the addition is commutative. Obviously, a near-ring is a ring iff it is abelian and distributive.

Again, we take a small group Γ and a (probably big) near-ring $N \le \mathrm{M}(\Gamma)$ generated by a small set E. Of course, if f is an endomorphism of Γ then it is distributive. But this condition is not necessary. We need a weaker one. Call f a *piecewise endomorphism on* N iff all restrictions of f to $N\gamma$, $\gamma \in \Gamma$, are endomorphisms. Note that this notion, like distributivity, depends on the near-ring N involved.

PROPOSITION 3. *Let* $f \in N \leq \mathrm{M}(\Gamma)$. *Then* $f \in N$ *is distributive iff it is a piecewise endomorphism on* N.

PROOF. Let f be distributive and $g\gamma, h\gamma \in N\gamma$. Then $f(g\gamma + h\gamma) = f(g+h)\gamma = (fg+fh)\gamma = f(g\gamma) + f(h\gamma)$. So the restriction of f is a homomorphism. Clearly $f(g\gamma) = (fg)\gamma \in N\gamma$. Conversely, if $f(g+h)\gamma = (fg+fh)\gamma$ for all $\gamma \in \Gamma$, then, using faithfulness, $f(g+h) = fg + fh$, hence f is distributive. □

Note that the $N\gamma$ can be computed efficiently by Algorithm 1.

Remark 1. To test whether a mapping f is a homomorphism on a group Γ generated (as a group) by a set F it is enough to test whether $f(\gamma+\varphi) = f(\gamma) + f(\varphi)$ for all $\gamma \in \Gamma$, $\varphi \in F$. Thus the test has complexity $\mathrm{O}(|\Gamma|\,|F|)$.

PROPOSITION 4. N *is an abelian near-ring iff all* $N\gamma$ *are abelian groups.*

PROOF. Let $f\gamma, g\gamma \in N$. Then $f\gamma + g\gamma = (f+g)\gamma = (g+f)\gamma = g\gamma + f\gamma$ if N is abelian. Conversely, for $f, g \in N$ we have to show that $(f+g)\gamma = (g+f)\gamma$, which again follows directly from $N\gamma$ being abelian. □

COROLLARY 2. *We can test whether* N *is a ring using* $\mathrm{O}(|\Gamma|\,|E|^2)$ *operations.*

PROOF. A near-ring is a ring iff it is abelian and all its generators are distributive. □

Many more properties can be tested efficiently by a reduction to the computation of some $N\gamma$ as before, e.g.:

PROPOSITION 5. $f \in N$ *is in the center of* N *(i.e., commutes with all* $g \in N$*) iff* f *is distributive and commutes with all generators.*

Our test for distributivity is generalized in Section 7.

5. DIFFERENCE OPERATOR

Computations in spaces of continuous functions are usually performed using linearization via the differential operator. In the discrete case, we can do something similar with a difference operator. We define it in the following way.

Definition 3. Let N be a near-ring and Γ an N-group. For $f \in N$, $x, a \in \Gamma$ we define

$$\Delta fxa := -fx + f(x+a)$$

and call it the *difference of* f *at* x *in direction* a.

Thus the Operator Δ is understood to map an element of N into a function that maps elements of Γ into elements of Γ^Γ. In particular, $\Delta fx \in \Gamma^\Gamma$. This operator is also useful in the case $\Gamma = N$, i.e., if N itself is considered as an N-group via the multiplication of N (just as a ring might be considered as a module over itself).

PROPOSITION 6. *With the notation of the definition we have*

$$\Delta fx(a+b) = \Delta fxa + \Delta f(x+a)b, \qquad \textit{(quasi-linearity)} \tag{3}$$

$$\Delta f(x+a)b = -\Delta fxa + \Delta fx(a+b). \qquad \textit{(translation rule)} \tag{4}$$

PROOF. Of course, both equations are equivalent. We show (4):

$$\begin{aligned} -\Delta fxa + \Delta fx(a+b) &= -f(x+a) + fx - fx + f(x+a+b) \\ &= \Delta f(x+a)b. \end{aligned}$$ □

Of course, the definition of the difference operator is to mirror that of the differential operator for functions on linear spaces. In contrast to the latter, the difference at a point, Δfx, need not be a linear function. Equation (3), however, suggests that it is not too far away. In particular, if we know the difference in directions generating G (as a group), then we know it in any direction. This is similar to partial derivatives. On the other hand, the equivalent equation (4) shows that the difference at 0, $\Delta f0$, already determines the difference at any point Δfx. This is far away from the idea that the difference at a point should describe a function locally. The following proposition again suggests a very close connection.

PROPOSITION 7. *The operator* Δ *fulfills the following chain rule:*

$$\Delta(fg)xa = \Delta f(gx)\Delta gxa. \tag{5}$$

PROOF. $\Delta(fg)xa = -fgx + fg(x+a) = -fgx + f(gx + \Delta gxa) = \Delta f(gx)\Delta gxa$. □

Some essential properties occurring in near-ring theory [9] can be expressed easily using the difference operator:

Definition 4. A faithful N-group Γ is

1. *tame* iff $\forall f \in N$, $\forall x \in \Gamma$, $\forall a \in \Gamma$ $\exists f' \in N$ such that $\Delta fxa = f'a$;
2. *k-tame* iff $\forall f \in N$, $\forall x \in \Gamma$, $\forall a_1, \ldots, a_k \in \Gamma$ $\exists f \in N'$ such that $\Delta fxa_i = f'a_i$, $\forall i = 1, \ldots, k$;
3. *compatible* iff $\forall f \in N$, $\forall x \in \Gamma$ $\exists f \in N'$ such that $\Delta fxa = f'a$, $\forall a \in \Gamma$.

Thus, compatible means that Δfx $(\in \Gamma^\Gamma)$ operates in the same way as some $f' \in N$, meaning something similar to differentiability. Similarly, k-tame means that Δfx can be interpolated at k places by some element in N. Of course, tame just means 1-tame, and can also be expressed as the reachability problem $\Delta fxa \in Na$. The following proposition reduces the tameness test to testing the generators of the near-ring.

PROPOSITION 8. *Let* E *be a set of generators of the near-ring* N. *Then a faithful abelian* N*-group* Γ *is tame iff* $\forall f \in E$, $\forall x \in \Gamma$, *and* $\forall a \in \Gamma$: $\Delta fxa \in Na$;

PROOF. Only sufficiency is non-trivial. Suppose that f and g fulfill the condition. Then $\Delta(f-g)xa = \Delta fxa - \Delta gxa \in Na - Na = Na$ and, applying (5), $\Delta(fg)xa = \Delta f(gx)\Delta gxa = f'(g'a) = (f'g')a \in Na$. □

COROLLARY 3. *We can test whether a faithful abelian N-group Γ is tame within $O(|E|^2\,|\Gamma|)$ multiplications*

PROOF. By the proposition, the property in the definition of tameness just has to be tested for all generators. □

COROLLARY 4. *We can test whether a faithful abelian N-group Γ is k-tame within $O(|E|^{k+1}\,|\Gamma|)$ multiplications.*

PROOF. Instead of the 1-interpolation problems before, we are faced with k-interpolation problems here. □

PROPOSITION 9. *Testing whether a transformation near-ring N (on Γ) generated by a set E is compatible reduces to* $\mathrm{O}(|E|\,|\Gamma|)$ *membership problems.*

PROOF. We just have to test whether $\Delta fx \in N$, for all points $x \in \Gamma$ and generators $f \in E$. □

6. COMPLETENESS AND REALIZABILITY

We continue considering a transformation near-ring $N \leq \mathrm{M}(\Gamma)$ given by a set E of generators.

It is natural to ask, whether E already generates the full transformation near-ring, i.e., whether $N = \mathrm{M}(\Gamma)$. Certainly, this will not be the case if all generators are *zero-symmetric*, i.e., if $E0 = \{0\}$, because this property is preserved by addition and composition. In this case, we better to ask whether all zero-symmetric transformations can be generated, i.e., whether $N = \mathrm{M}_0(\Gamma) := \{\, f \in M(\Gamma) \mid f(0) = 0\,\}$.

Problem 3. (Completeness) Let $N \leq \mathrm{M}(\Gamma)$ be a near-ring given by a set E of generators.

If N is zero-symmetric, decide whether $N = \mathrm{M}_0(\Gamma)$, otherwise whether $N = \mathrm{M}(\Gamma)$.

Let Γ be a group, and let N be a sub-near-ring of $\mathrm{M}(\Gamma)$. We say that N has the *k-interpolation property* iff for all finite subsets Ω of Γ with $|\Omega| \leq k$ and for all mappings $m\colon \Omega \to \Gamma$ there exists an element $f \in F$ such that $f|_\Omega = m$. It has the k-interpolation property *with respect to* $\mathrm{M}_0(\Gamma)$ if it is enough to interpolate all zero-symmetric mappings $m \in \mathrm{M}_0(\Gamma)$.

Of course, as we only consider the case that Γ is finite, the $|\Gamma|$-interpolation property means that $N = \mathrm{M}(\Gamma)$, and if N is zero-symmetric, then $N = \mathrm{M}_0(\Gamma)$ is the same as the $|\Gamma|-1$ interpolation-property with respect to $M_0(\Gamma)$.

Using our solution to the k-interpolation problem (Proposition 2.4) we can see that the k-interpolation property can be solved within $\mathrm{O}(|E|)|\Gamma|^{2k+1}|F|^2$, where F is a set of generators for the group Γ: it is enough to test all interpolation Problems of the form $f(\gamma_1) = \eta_1,\ \ldots,\ f(\gamma_k) = \eta_k$ with $\gamma_i \in \Gamma$, $\eta_i \in F$. This bound is polynomial in all variables, except in k. In particular, we cannot really solve the completeness problem this way.

At this point, classical near-ring theory can help us, as it provides the following *density theorems*:

THEOREM 2. *If N has the 2-interpolation property and $N_0 := \{f \in N \mid f0 = 0\}$ is not a ring, then N has the k-interpolation property for all $k \in \mathbb{N}$.*

Note that the 2-interpolation property can be tested efficiently. Usually, it is not difficult to establish that N_0 is not a ring. But in some cases this may be difficult to test, and we have to use a similar theorem.

THEOREM 3. *If N has the 3-interpolation property and there is an element $\gamma \in \Gamma$ with $\gamma + \gamma \neq 0$, then N has the k-interpolation property for all $k \in \mathbb{N}$.*

If this does not help either, we have to resort to interpolation on 4 places, which has no additional requirements and still provides a polynomial-time algorithm.

THEOREM 4. *If N has the 4-interpolation property, then N has the n-interpolation property for all $n \in \mathbb{N}$.*

Proofs for these classical results are contained in [2, 1].

For the 0-symmetric case, it is sometimes enough to test for the 1-interpolation property.

THEOREM 5. *Let Γ be a group with $|\Gamma| \geq 3$, and let N be a sub-near-ring of* $\mathrm{M}_0(\Gamma)$. *Then N has the k-interpolation property for all $k \in \mathbb{N}$ with respect to* $\mathrm{M}_0(\Gamma)$ *iff*

1. *N has the 1-interpolation property with respect to* $\mathrm{M}_0(\Gamma)$,
2. *N is not a ring,*
3. *There is no fixed point free group automorphism $\alpha \neq \mathrm{id}$ of $(\Gamma, +)$ of prime order such that $\forall f \in N\colon \alpha f = f\alpha$.*

An automorphism α of $(\Gamma, +)$ is called *fixed point free* iff $\alpha(\gamma) = \gamma$ implies $\gamma = 0$. The order of α is the smallest positive k with $\alpha^k = \mathrm{id}$. Theorem 6.4 can be proved using the description of 0-primitive near-rings in [4] or [1, Theorem 4.21].

If these requirements cannot be established, we can always resort to the 2-interpolation property.

THEOREM 6. *Let N be a sub-near-ring of* $\mathrm{M}_0(\Gamma)$ *that has the 2-interpolation property with respect to* $\mathrm{M}_0(\Gamma)$. *If N is not a ring, then N has the k-interpolation property with respect to* $\mathrm{M}_0(\Gamma)$ *for all $k \in \mathbb{N}$.*

Often we will not be satisfied with the information that some $f \in \mathrm{M}(\Gamma)$ happens to be in N, but rather want to know how f can be realized, i.e., how it can be obtained from the generators using addition and composition.

Problem 4. (Realizability) Suppose that $\mathrm{M}(\Gamma)$ is generated by a set E of generators and let $f \in \mathrm{M}(\Gamma)$.
Compute a term t in the free near-ring over E that realizes f.

Suppose, e.g., that completeness of the near-ring generated by E was established by Theorem 6.1. The constructive proof of this theorem by [1] can be used to solve the realizability problem in this case, as described in Algorithm 3.

For this algorithm we will need a binary term ("multiplication") K on Γ such that $K(\gamma, 0) = K(0, \gamma) = 0$ for all $\gamma \in \Gamma$, but $K(\alpha, \beta) \neq 0$ for some $\alpha, \beta \in \Gamma$. In our case, these can be found as follows. If $(\Gamma, +)$ is not abelian, then we can take α and β in Γ with $\alpha + \beta \neq \beta + \alpha$, and define $K(\gamma_1, \gamma_2) := -\gamma_1 - \gamma_2 + \gamma_1 + \gamma_2$. Otherwise, from establishing Theorem 6.1, we know how to construct (from the generators in E) a transformation $f \in \mathrm{M}_0(\Gamma)$, such that there are $\alpha, \beta \in \Gamma$ with $f(\alpha + \beta) \neq f(\alpha) + f(\beta)$. Then we can take these together with $K(\gamma_1, \gamma_2) := f(\gamma_1) + f(\gamma_2) - f(\gamma_1 + \gamma_2)$.

Algorithm 3 takes a finite subset

$$S := \{(\gamma_1, \eta_1), (\gamma_2, \eta_2), \ldots, (\gamma_k, \eta_k)\}$$

(all γ_i different) of $\Gamma \times \Gamma$, and returns a term f (built from the generators in E) such that $f(\gamma_i) = \eta_i$ for $i = 1, 2, \ldots, k$. We assume that we have an algorithm *InterpolateAtTwo* that produces this f if S has at most two elements. Proposition 2.4 (with full book-keeping, of course) can be used for this purpose.

Algorithm 3 Interpolation

Require: A set $\{ (\gamma_i, \eta_i) \mid i = 1, \ldots, k \}$ of points in $\Gamma \times \Gamma$.
Ensure: A term f satisfying $f(\gamma_i) = \eta_i$ for all $i = 1, \ldots, n$.

```
if k ≤ 2 then
  return InterpolateAtTwo(S)
else
  (* Interpolate recursively on k − 1 points *)
  s1 := Interpolation[{(γi, ηi) | i = 1, 2, ..., k − 1}]
  s2 := LagrangePoly({(γi, 0) | i = 1, 2, ..., k − 1} ∪
        {(γk, ηk − s1(γk))})
  return s2 + s1
end if
```

The following algorithm ***LagrangePoly*** solves a specific interpolation problem by a divide and conquer strategy.

Require: A set $\{ (\gamma_i, \eta_i) \mid i = 1, \ldots, k \}$ of points in $\Gamma \times \Gamma$ with $\eta_1 = \cdots = \eta_{k-1} = 0$.
Ensure: A function f satisfying $f(\gamma_i) = \eta_i$ for all $i = 1, \ldots, k$.

```
if k ≤ 2 then
  InterpolateAtTwo(S)
else
  Partition {1, ..., k − 1} into two smaller subsets X, Y
  p1 := LagrangePoly({(γi, 0) | i ∈ X} ∪ {(γk, α)})
  p2 := LagrangePoly({(γi, 0) | i ∈ Y} ∪ {(γk, β)})
  (* Multiply using K *)
  h := K(p1, p2)
  g := InterpolateAtTwo[{(0, 0), K(α, β), ηk)}]
end if
return g ∘ h
```

Note that this algorithm just needs $\mathrm{O}(k^2)$ interpolations on 2 places. Similar algorithms can be used to solve the realizability in the cases where one of the other density theorems is applicable.

THEOREM 7. *The Realizability problem can be solved in polynomial time.*

7. DEGREE

Considering real functions, we know that a polynomial has degree n iff its $(n + 1)$st derivative is the first one that vanishes.

We do something similar using the difference operator, which in fact can be iterated in the following way. The definition is motivated by the formal rule $\Delta^{n+1} f = \Delta(\Delta^n f)$.

Definition 5. Let Γ be an N-group, $f \in N$, $x, a, b \in \Gamma$, $\mathbf{a} \in \Gamma^n$. Then we define the higher order difference operators as

$$\Delta^{n+1} fxb\mathbf{a} := -\Delta^n fx\mathbf{a} + \Delta^n f(x + b)\mathbf{a}.$$

In particular,

$$\begin{aligned} \Delta^2 fxba &= \Delta(\Delta f)xba \\ &= -\Delta fxa + \Delta f(x + b)a \\ &= -f(x + a) + fx - f(x + b) + f(x + b + a). \end{aligned}$$

Remark 2. If Γ is abelian, then Δ^n is symmetric in the last n arguments.

Remark 3. By the translation rule, $\Delta f = 0$ iff $\Delta^n f0 = 0$ iff $\Delta^n fx = 0$ for some x.

Remark 4. An element f in a near-ring is constant (i.e., satisfies $fg = f$ for all g) iff $\Delta f = 0$. It is *affine* (i.e., $f - f0$ is distributive) iff $\Delta^2 f0 = 0$. Here, we have considered N to operate over itself.

Definition 6. An element f in a near-ring N has *degree n* iff $\Delta^{n+1} f0 \underbrace{N \ldots N}_{n+1} = 0$ but $\Delta^n f0 \underbrace{N \ldots N}_{n} \neq 0$.

Example 2. Let R be an integral domain. Then the notion of degree in the near-ring $(R[x], +, \circ)$, according to the above definition, coincides with the usual definition.

THEOREM 8. *If a near-ring N operates faithfully on a group Γ, then each $f \in N$ has degree at most n iff it operates on Γ piecewisely like a function of degree at most n, i.e, iff $\Delta^{n+1} a0(N\gamma)...(N\gamma) = \{0\}$, for each $\gamma \in \Gamma$.*

PROOF. We proceed exactly as in the test for distributivity. Suppose f has degree at most n. Let $f_1\gamma, \ldots, f_n\gamma \in N\gamma$. Then, using the distribute law, $\Delta^{n+1} a0(f_1\gamma, \ldots, f_n\gamma) = \Delta^{n+1} a0(f_1, \ldots, f_n)\gamma = 0\gamma = 0$. Conversely, to prove that $\Delta^{n+1} a0(f_1, \ldots, f_n) = 0$ (this is an equation over N) disappears we have to show that how that $\Delta^{n+1} a0(f_1, \ldots, f_n)\gamma$ for all $\gamma \in \Gamma$, which is true by the same equality as above. □

Remark 5. Again, instead of testing $\Delta^{n+1} a0(N\gamma)...(N\gamma) = \{0\}$, it is enough to test $\Delta^{n+1} a0(M\gamma)F...F = \{0\}$, if F generates $N\gamma$. Thus the complexity of this test is in $\mathrm{O}(|\Gamma|\,|F|^n)$.

8. MEMBERSHIP

One of the most natural problems arising in the context of transformation near-rings is the following.

Problem 5. (Membership) Let $N \leq \mathrm{M}(\Gamma)$ be given by a set of generators E. For any $f \in M(\Gamma)$ test whether $f \in N$.

This turns out to be the hardest of our problems and we cannot give a completely satisfactory answer, but one that is acceptable in many important cases.

The idea is to compute a set A of *additive generators for* N, i.e., ones that generate N as a group. Then we can use all the method's known from computational group theory to solve problems about N, e.g., computing its size and solving the membership problem.

Translated to the language of systems theory, additive generators correspond to building blocks from which all transformations in N can be built using only parallel connections.

Things are particularly easy if all generators of the near-ring are distributive. Then additive generators can be computed successively by an easy closure algorithm: $E_0 := E$, $E_1 := E_0 \cup EE_1$, $E_2 := E_1 \cup EE_2$, ..., until this process becomes stable. Essentially the same method works if the generators turn out to have degree 1. The basic idea here is that we need not compute $E(E+E)$, $E(E+E+E)$, ... because from $\Delta^2 e0fg = 0$, i.e., $-eg + e0 - ef + e(f+g) = 0$, we know that $e(f+g) = eg - e0 + ef$, and thus $e(f+g)$ happens to be in the additive closure of ef, eg, and $e0$.

There is a generalization for near-rings generated by elements of small degree:

THEOREM 9. *Let E be a set of near-ring generators of N of degree at most n. Define $E_0 = E$, $E_{i+1} := E_i \cup E(E_i + ... + E_i)$ (n-fold sum). If $E_k = E_{k+1}$, for some k, then E_k generates N additively.*

PROOF. The case $n = 1$ has been shown above. We show the important case $n = 2$ ("quadratic functions"). We have $0 = \Delta^3 e0fgh = -\Delta^2 e0gh + \Delta^2 efgh = -e(g+h) + eg - e0 + eh - e(f+h) + ef - e(f+g) + e(f+g+h)$ and again see that $e(f+g+h)$ can be isolated and thus is already contained in the group generated by $E0 \cup E^2 \cup (E+E)$. We omit the general induction proof. □

Thus we need $\mathrm{O}(|E|\,|A|^n)$ steps to compute a set A of additive generators for N. Of course, this solution by far does not have the efficiency of all the other algorithms presented in this note, in particular there is no good bound for $|A|$. Nevertheless, even in its most simple version, for $n = 1$, this method has already solved some problems previously open [3].

Some optimizations are possible, e.g., if the elements in $E = \{e_1, ..., e_m\}$ have different degrees, say $n_1, ..., n_m$, then it is enough to compute all the $e_\nu(E_i + ... + E_i)$ (where the sum is only n_ν-fold) instead of $E(E_i + ... + E_i)$ with the n-fold sum.

9. CONCLUSION

Various problems for computing with transformation near-rings have been considered. Most of them have got very satisfactory solutions, as everything can be done with the near-ring generators and we are able to compute with near-ring of a size where group theoretic algorithms could not be applied any more. The membership problem turned out to be much harder and we had to resort to the computation of additive generators, thus reducing the problem to computations with the additive group structure. On the other hand, we can decide whether the full transformation near-ring is generated and how we can realize arbitrary functions also in this case.

10. REFERENCES

[1] E. Aichinger. Interpolation with near-rings of polynomial functions. Master's thesis, University of Linz, 1994.

[2] E. Aichinger. Local interpolation near-rings as a frame-work for the density theorems. In *Contributions to General Algebra*, volume 9, pages 27 – 36. Verlag Hölder-Pichler-Tempsky, Wien - Verlag B.G. Teubner, Stuttgart, 1995.

[3] E. Aichinger and C. Nöbauer. The cardinalities of the endomorphism near-rings $I(G)$, $A(G)$, and $E(G)$ for all groups G with $|G| \leq 31$. In G. Saad and M. J. Thomsen, editors, *Near-rings, near-fields and K-loops*, pages 175–178. Kluwer Acad. Publisher, 1997.

[4] G. Betsch. Primitive near-rings. *Math.Z.*, 130:351–361, 1973.

[5] J. Clay. *Nearrings: Geneses and Applications.* Oxford University Press – Oxford, New York, Tokyo, 1992.

[6] J. D. P. Meldrum. *Near-rings and their links with groups*, volume 134 of *Research Notes in Mathematics.* Pitman Publishing Ltd., 1985.

[7] G. F. Pilz. *Near-Rings. The Theory and its Applications*, volume 23 of *North-Holland Mathematics Studies.* North-Holland Publishing Company, Amsterdam, New York, Oxford, revised edition, 1983.

[8] S. D. Scott. Involution near-rings. *Proc. Edinburgh Math. Soc. (2)*, 22(3):241–245, 1979.

[9] S. D. Scott. Tame near-rings and N-groups. *Proc. Edinburgh Math. Soc. (2)*, 23(3):275–296, 1980.

[10] C. Sims. Computational methods in the study of permutation groups. In J. Leech, editor, *Computational problems in abstract algebra, Conf. Oxford*, pages 169–183, 1970.